INTERNAL AUDIT · COMPLIANCE · INFORMATION TECHNOLOGY · CYBERSECURITY · RISK CONSULTING

AuditOne

COMPLIANCE ADVISORY

November 2026 Regulatory Developments

AUDITONE COMPLIANCE ADVISORY	
COVERAGE	Third-party risk, stablecoins, examination cycles, MRAs, CRA, FDIC signage, NCUA deregulation, CCPA/CPRA, and other developments
PUBLISHED	November 2026
PREPARED FOR	Banks, credit unions, fintechs, sponsor banks, and payments organizations
PREPARED BY	Celeste Burton, CIA, Practice Director, Compliance and Director, Credit Union Engagement Services, AuditOne

Prepared for general informational purposes and not intended as legal advice. May be shared with colleagues responsible for the areas discussed. © 2026 AuditOne OH LLC. Confidential and Proprietary.

Q3 2026 COMPLIANCE ADVISORY

CONTENTS

IN THIS ISSUE

01 **Overview: Key Regulatory Developments Institutions Need to Know**

02 **At a Glance**

03 **Agencies Propose New Interagency Third-Party Risk Management Guidance**

04 **OCC Finalizes GENIUS Act Rule for Payment Stablecoins**

05 **More Banks Qualify for the 18-Month Examination Cycle**

06 **FDIC and OCC Redefine "Unsafe or Unsound Practice" and Establish Uniform MRA Standards**

07 **OCC and FDIC Propose Targeted Changes to Community Reinvestment Act Rules**

08 **FDIC Finalizes Revised Official Signs Requirements for Digital Channels and ATMs**

09 **NCUA Advances Deregulation Project Through 11 Final Rules**

10 **CCPA and CPRA Implementation: 2026 Requirements and Next Milestones**

11 **Other Noteworthy Compliance News and Developments**
OCC Cybersecurity Supervision Work Program · CRA data through Reporting Central · FDIC Consumer Compliance Examination Manual · Mobile driver's licenses under the CIP rule · SAR confidentiality · CFPB Section 1033

12 **Key Dates to Watch**

13 **About AuditOne**

OVERVIEW: KEY REGULATORY DEVELOPMENTS INSTITUTIONS NEED TO KNOW

EXECUTIVE SUMMARY

Supervisory focus is shifting toward material financial risk, risk-based oversight, and regulatory relief. Accountability for effective controls is not.

Now in effect: the FDIC and OCC unsafe or unsound practice and MRA standards (Nov. 2, 2026) and the expanded 18-month examination cycle (Sept. 14, 2026).

Coming next: CCPA/CPRA automated decision-making requirements (Jan. 1, 2027), the OCC GENIUS Act rule (Jan. 18, 2027), and FDIC official signs compliance (Apr. 1, 2027).

Still evolving: proposed third-party risk management guidance, proposed CRA amendments, NCUA deregulation, and the CFPB Section 1033 rule.

Regulatory developments in the third and early fourth quarters of 2026 reflect a continued shift toward risk-based supervision, stronger governance, and expanded oversight of emerging products and technologies. This Advisory covers eight principal developments, summarized in the At a Glance table that follows, and six additional items in Other Noteworthy Compliance News and Developments.

WHAT THIS MEANS FOR YOUR INSTITUTION

The developments discussed below reinforce several consistent expectations for financial institutions:

- Regulatory change management should identify effective dates, accountable owners, affected systems, and evidence of implementation.
- Longer examination cycles, narrower supervisory definitions, and deregulation do not reduce the need for internal monitoring, testing, and audit coverage. Management remains responsible for demonstrating that controls are designed and operating effectively.
- New products and technologies require governance that is proportionate to legal, operational, cybersecurity, consumer, and third-party risk.

This Compliance Advisory was prepared by Celeste Burton, CIA, Practice Director, Compliance and Director Credit Union Engagement Services, at AuditOne. The information is intended to support informed decision-making and may be shared with colleagues responsible for the areas discussed.

AT A GLANCE

The table below summarizes the principal developments in this Advisory, who they apply to, and the next date to watch.

TOPIC	APPLIES TO	KEY DATE	ACTION TO CONSIDER
Third-party risk management guidance (proposed)	Banks, credit unions, fintechs partnering with banks	**Comments due Dec. 16, 2026 (extended)**	Compare current vendor and fintech oversight to the proposal; consider commenting
OCC GENIUS Act final rule	Banks, fintechs, prospective stablecoin issuers	**Effective Jan. 18, 2027**	Assess direct and indirect stablecoin exposure
18-month examination cycle	Banks with less than $6 billion in assets	**Effective Sept. 14, 2026**	Confirm eligibility and document the basis
Unsafe or unsound practice and MRA rule	FDIC- and OCC-supervised banks	**Effective Nov. 2, 2026**	Review open findings and issue tracking
CRA proposed rule (OCC and FDIC)	Banks subject to the CRA	**Comments closed Oct. 13, 2026**	Model proposed size thresholds and reporting changes
FDIC official signs rule	FDIC-insured banks	**Compliance Apr. 1, 2027**	Validate website, app, and ATM signage
NCUA deregulation final rules	Federally insured credit unions	**Effective Sept. 8, 2026**	Complete a rule-by-rule applicability assessment
CCPA and CPRA regulations	Covered businesses, including non-GLBA data at institutions and fintechs	**Jan. 1, 2027; Dec. 31, 2027; Apr. 1, 2028**	Inventory ADMT and schedule risk assessments and audits
SAR confidentiality joint statement	Banks and credit unions	**Issued Sept. 2, 2026**	Update fraud and account-closure communication procedures
CRA data through Reporting Central	Banks reporting CRA data	**2027 reporting year; data due Mar. 1, 2028**	Confirm vendor file capability and access

AGENCIES PROPOSE NEW INTERAGENCY THIRD-PARTY RISK MANAGEMENT GUIDANCE

APPLIES TO | *Banks, credit unions, and fintechs that partner with them*

On September 11, 2026, the OCC, Federal Reserve, FDIC, and NCUA proposed interagency guidance to revise and replace existing third-party risk management guidance. The proposal would encourage institutions to align their third-party risk management practices with the assessed risk of each third-party relationship, tailored to the institution's size, complexity, and risk profile and to the nature of the relationship, and to avoid overly process-driven approaches that treat all third-party relationships as inherently higher risk. The agencies state that replacing the existing guidance is intended to promote consistency and prudent innovation in the banking industry. On November 13, 2026, the agencies extended the comment period from November 16 to December 16, 2026.

The proposal is principles-based supervisory guidance. It would not set enforceable standards or prescriptive requirements, and non-compliance with the guidance would not by itself result in supervisory action. When finalized, it would apply to banking organizations of all sizes, including community banks. The Federal Reserve also proposed a companion guide for the community banks it supervises, and the federal bank regulatory agencies issued a separate statement on community banks' engagement with core service providers, which discusses factors the agencies will consider in supervisory and enforcement decisions related to those providers.

Institutions should compare the proposal with their current programs, including vendor risk tiering, due diligence, contract provisions, ongoing monitoring, and termination planning. Sponsor banks and fintechs involved in bank-fintech and Banking-as-a-Service arrangements should confirm that oversight of each relationship reflects its actual risk. Institutions may wish to submit comments before the extended December 16, 2026, deadline and should avoid dismantling existing controls until final guidance is issued.

> **HOW AUDITONE CAN HELP**
>
> Third-party risk management program reviews, including sponsor-bank and Banking-as-a-Service oversight, vendor risk tiering, and testing of due diligence, contract, and monitoring controls.

SOURCES

OCC Bulletin 2026-46 - Third-Party Risk Management: Proposed Guidance and Request for Comment

OCC News Release 2026-100 - Agencies Extend Comment Period for Proposed Third-Party Risk Management Guidance (November 13, 2026)

Federal Reserve Board - Agencies seek comment on proposed third-party risk management guidance (September 11, 2026)

OCC FINALIZES GENIUS ACT RULE FOR PAYMENT STABLECOINS

APPLIES TO | *Banks, fintechs, and other prospective stablecoin issuers; institutions with indirect stablecoin exposure*

On October 21, 2026, the OCC finalized a rule implementing portions of the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act). The rule establishes a federal framework for OCC-supervised payment stablecoin issuers and addresses licensing,

reserve assets, redemption, custody, risk management, reporting, and supervisory expectations. It takes effect January 18, 2027, the same day the GENIUS Act takes effect.

The rule is relevant beyond institutions planning to issue stablecoins. Banks and credit unions may encounter stablecoin exposure through custody, payments, settlement, third-party relationships, deposit products, treasury services, technology vendors, or customers operating in the digital-asset sector. Risk assessments should identify direct and indirect exposure and consider liquidity, operational resilience, cybersecurity, fraud, sanctions, BSA/AML, consumer protection, legal, and concentration risk.

Institutions evaluating a stablecoin strategy should establish Board-approved risk appetite, identify permissible activities, complete legal and compliance reviews, assess reserve and redemption mechanics, evaluate third parties, and determine whether existing monitoring and incident-response capabilities are sufficient. Product approval should also define the conditions under which the institution would pause or exit the activity.

The OCC indicated that it will separately announce when it will begin accepting applications and waiver requests, and that regulations addressing BSA/AML and OFAC sanctions requirements will be finalized in a separate rulemaking coordinated with the Department of the Treasury; the OCC proposed those requirements in June 2026. Treasury has also proposed GENIUS Act regulations governing the issuance, offering, and sale of payment stablecoins, for which comments closed October 19, 2026. In addition, beginning July 18, 2028, three years after the GENIUS Act's enactment, digital asset service providers generally may not offer or sell a payment stablecoin to a person in the United States unless it is issued by a permitted payment stablecoin issuer, a change that will affect custody, exchange, and payments relationships. Institutions should monitor subsequent OCC and Treasury communications and avoid treating the final rule as the end of the implementation process.

> **HOW AUDITONE CAN HELP**
>
> Risk assessments of direct and indirect stablecoin and digital-asset exposure, payments and third-party risk reviews, and BSA/AML program testing.

SOURCES

OCC Bulletin 2026-50 - GENIUS Act Regulations: Final Rule

Federal Register - U.S. Department of the Treasury, GENIUS Act Regulations on Payment Stablecoin Issuance, Offer, and Sale (Proposed Rule, August 18, 2026)

MORE BANKS QUALIFY FOR THE 18-MONTH EXAMINATION CYCLE

APPLIES TO | *Banks with less than $6 billion in total assets (OCC-, Federal Reserve-, and FDIC-supervised)*

The OCC, Federal Reserve, and FDIC issued an interagency interim final rule, effective September 14, 2026, that implements the 21st Century ROAD to Housing Act by raising the total asset threshold for the 18-month on-site examination cycle from $3 billion to $6 billion. To qualify, a bank must be rated 1 or 2, well capitalized, and well managed; not be subject to a formal enforcement proceeding or order; and not have undergone a change in control during the preceding 12 months. The agencies retain authority to examine more frequently and will continue off-site monitoring between scheduled examinations.

As the interval between examinations lengthens, institutions will rely more heavily on their own monitoring to identify emerging risk, resolve findings promptly, and report reliably to the Board. Internal audit plans, compliance monitoring, and issue tracking should be designed to provide independent assurance between examinations.

Management should confirm eligibility and document the basis for the examination schedule. Changes in condition, enforcement status, ownership, risk profile, or supervisory concern can affect eligibility. The Federal Reserve confirmed the same criteria for state member banks in SR 26-8, issued October 14, 2026.

> **HOW AUDITONE CAN HELP**
>
> Risk-based internal audit planning that maintains independent assurance coverage regardless of the examination calendar.

SOURCES

OCC Bulletin 2026-45 - Expanded Examination Cycle Eligibility: Interim Final Rule

Federal Reserve - SR 26-8: Updates to the Expanded Examination Cycle for Certain State Member Banks and U.S. Branches and Agencies of Foreign Banking Organizations (October 14, 2026)

FDIC AND OCC REDEFINE "UNSAFE OR UNSOUND PRACTICE" AND ESTABLISH UNIFORM MRA STANDARDS

APPLIES TO | *FDIC- and OCC-supervised banks*

On August 27, 2026, the FDIC and the OCC issued a final rule establishing a uniform definition of the term "unsafe or unsound practice" for use in enforcement actions and supervisory activities. The rule took effect on November 2, 2026, and is consistent with the agencies' October 2025 proposal, with certain modifications. The agencies stated that the definition is designed to ensure that examiners prioritize material financial risks over policies, processes, documentation, and other nonfinancial risks.

Under the final rule, an unsafe or unsound practice is a practice, act, or failure to act, alone or together with one or more other practices, acts, or failures to act, that is contrary to generally accepted standards of prudent operation and that, if continued, is likely to materially harm the financial condition of the institution or present a material risk of loss to the Deposit Insurance Fund (DIF), or that has materially harmed the financial condition of the institution. The rule also establishes uniform standards for when and how the agencies may issue Matters Requiring Attention (MRAs) and communicate supervisory observations and other violations of laws and regulations. The agencies will tailor their use of the definition and the MRA standard based on risk factors specific to each institution, and the rule is expressly limited to institutions the agencies supervise.

A narrower supervisory definition should not be interpreted as reducing expectations for compliance with consumer protection, BSA/AML, or other banking laws and regulations. Violations of laws and regulations remain subject to supervisory communication, and policies, procedures, and documentation remain the means by which management demonstrates that controls are designed and operating effectively.

In implementing the rule, the FDIC ended its use of Matters Requiring Board Attention and Supervisory Recommendations for examination findings. Outstanding items are being reviewed and will either be redesignated as MRAs or closed out. The FDIC also stated that it intends to generally limit MRAs for violations to substantive violations, with other violations communicated as "other violations" for which remediation may still be required. Separately, the OCC issued a notice of proposed rulemaking addressing Matters Requiring Attention for violations of laws and regulations and revised its policies and procedures manuals for bank enforcement actions and MRAs.

Management should review outstanding supervisory findings, understand how existing MRAs and other supervisory communications may be characterized under the new standards, and confirm that issue tracking and Board reporting continue to capture both regulatory findings and internally identified weaknesses. Risk assessments and audit plans should continue to address compliance areas where control weaknesses could result in violations, consumer harm, reputational risk, or financial loss.

> **HOW AUDITONE CAN HELP**
>
> Reviews of issue tracking, MRA remediation, and Board reporting, and independent testing of compliance controls.

SOURCE
Federal Register - Unsafe or Unsound Practices, Matters Requiring Attention (Final Rule, September 1, 2026)

OCC AND FDIC PROPOSE TARGETED CHANGES TO COMMUNITY REINVESTMENT ACT RULES

APPLIES TO | *Banks subject to the Community Reinvestment Act (proposal issued by the OCC and FDIC)*

On July 31, 2026, the OCC and FDIC proposed targeted amendments to their Community Reinvestment Act (CRA) regulations. After reviewing comments on their July 2025 proposal to rescind the 2023 CRA final rule, which a federal court enjoined before it took effect, the agencies proposed targeted reforms to the 1995 framework that remains in effect today. The proposal would:

- Raise the asset thresholds so that a small bank has less than $1 billion in assets (from $412 million), an intermediate bank has $1 billion to $10 billion (from $1.65 billion), and a large bank has more than $10 billion. Reduce data collection, maintenance, and reporting requirements for banks with $10 billion or less in assets.
- Narrow the scope of retail banking services to focus on credit services, excluding deposit services, and focus retail lending evaluations on a bank's major product lines.
- Limit consideration of community development grants to those directly used for a plan, project, or initiative with community development as a primary purpose, and require large banks to document that grant recipients' overhead costs do not exceed 15 percent of total costs.
- Codify an illustrative list of qualifying and nonqualifying community development activities and provide a process to confirm that an activity qualifies, without making significant changes to the assessment area framework.

Comments were due October 13, 2026. Because the proposal is not final, the current CRA rules remain in effect. Banks near the proposed thresholds should model how their classification, data and reporting obligations, and examination approach would change. Banks with significant deposit-service or grant-making activity should assess the potential effect on CRA consideration. The separate transition of CRA aggregate data submissions to Reporting Central is discussed below.

> **HOW AUDITONE CAN HELP**
>
> CRA and regulatory compliance program reviews, including testing of CRA data integrity, assessment area and product-line analysis, and community development documentation.

SOURCES

OCC Bulletin 2026-35 - Community Reinvestment Act: Interagency Notice of Proposed Rulemaking

Federal Register - Community Reinvestment Act Regulations (Proposed Rule, August 12, 2026)

FDIC FINALIZES REVISED OFFICIAL SIGNS REQUIREMENTS FOR DIGITAL CHANNELS AND ATMS

APPLIES TO | *FDIC-insured banks*

On January 29, 2026, the FDIC issued a final rule amending sections 328.4 and 328.5 of its official signs and advertising rule, which governs the display of the FDIC official digital sign and related signage on bank websites, mobile applications, automated teller machines, and similar devices. The amendments took effect on March 2, 2026, and compliance is required by April 1, 2027. This compliance date replaces the January 1, 2027, date the FDIC announced in November 2025. The final rule addresses implementation issues and potential consumer confusion raised after the 2023 rule was adopted, providing banks with additional flexibility while helping consumers understand when they are dealing with an insured institution and when their funds are protected by deposit insurance. Other part 328 requirements, including restrictions against false advertising, misrepresentation of insured status, and misuse of the FDIC's name or logo, were not changed by this rule and have been in effect since May 1, 2025.

The revised compliance date provides additional time for implementation, especially when banks rely on vendors for core systems, online banking, mobile applications, websites, or ATMs to configure the required signage. Because the requirements have changed, institutions should confirm that vendor configurations and implementation plans reflect the amended rule, not the 2023 version. Institutions should complete a channel-by-channel inventory, confirm vendor release dates, document testing, and verify that signage is displayed in the correct location and manner. Deposit and non-deposit products should be clearly distinguished to avoid leading customers to believe that uninsured products are FDIC-insured.

Institutions that implemented signage under the 2023 requirements should not automatically remove it or defer validation until 2027. Instead, they should compare existing implementations with the amended requirements and adjust as needed. Management should confirm that implementations are accurate across websites and digital platforms, that changes are controlled through vendor and system updates, and that evidence is retained for compliance monitoring and examination support. Institutions still relying on vendors should document outstanding

dependencies, interim controls, escalation procedures, and a completion schedule that allows sufficient time for testing before the April 1, 2027, compliance date.

> **HOW AUDITONE CAN HELP**
>
> Regulatory compliance audits that test FDIC signage across websites, mobile applications, and ATMs, including vendor change controls.

SOURCE
Federal Register - FDIC Official Signs, Advertisement of Membership, False Advertising, Misrepresentation of Insured Status, and Misuse of the FDIC's Name or Logo (Final Rule, January 29, 2026)

NCUA ADVANCES DEREGULATION PROJECT THROUGH 11 FINAL RULES

APPLIES TO | *Federally insured credit unions*

On August 5, 2026, the NCUA Board approved 11 final rules, the first round from its Deregulation Project. The rules were published in the Federal Register on August 6 and took effect on September 8, 2026. They address surety and guarantor requirements, limits on loans to other credit unions, eligible obligations, credit union service contracts, third-party servicing of indirect vehicle loans, notice of termination of excess insurance coverage, and disclosure of share insurance for non-member shares. They also rescind four Interpretive Rulings and Policy Statements related to chartering and field of membership. The action reflects the agency's broader effort to eliminate requirements viewed as obsolete, duplicative, unnecessarily prescriptive, or better addressed through supervisory guidance. The NCUA expects a second phase addressing more complex regulations to begin in 2027. For federally insured credit unions, this development is important because regulatory relief can change formal requirements without eliminating the underlying need for safe-and-sound governance, member protection, and effective internal controls. The NCUA has since finalized additional Deregulation Project rules, including a November 16, 2026, final rule amending the associational common bond provisions of the Chartering and Field of Membership Manual.

Credit unions should complete a rule-by-rule applicability assessment rather than assuming that deregulation automatically reduces operational or compliance risk. Policies, procedures, forms, system controls, monitoring programs, and audit work programs should be revised only after the effective date and practical impact of each final rule are confirmed. State-chartered credit unions should also determine whether state law, contractual obligations, governance documents, or examiner expectations continue to require controls that are no longer expressly required under an NCUA regulation.

The change-management record should identify the former requirement, the final regulatory change, the effective date, the business owner, affected processes, and the reason for retaining, modifying, or removing each control. Controls that support fraud prevention, segregation of duties, member protection, reliable reporting, or Board oversight may remain prudent even when the related federal requirement is simplified or removed.

> **HOW AUDITONE CAN HELP**
>
> Rule-by-rule impact assessments and updates to credit union audit work programs.

SOURCE
NCUA - NCUA Board Approves 11 Final Rules for Deregulation Project (August 5, 2026)

CCPA AND CPRA IMPLEMENTATION: 2026 REQUIREMENTS AND NEXT MILESTONES

APPLIES TO | *Any covered business, including banks, credit unions, and fintechs, for information outside the GLBA exemption*

California privacy requirements continued to mature in 2026. The California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), now requires covered businesses to move beyond policy updates and demonstrate that privacy, cybersecurity, and data-use controls are embedded in operations. The January 1, 2026, rollout is particularly important for organizations that process California consumer information in ways that may pose significant privacy or security risks.

Financial institutions should not assume that the Gramm-Leach-Bliley Act exemption removes them from CCPA and CPRA requirements. The exemption generally applies to information collected, processed, sold, or disclosed pursuant to the GLBA, rather than providing a blanket institutional exemption. Employee information, business contact information, website activity, marketing data, certain prospect information, and data used outside the GLBA relationship may remain within scope.

Key implementation considerations include:

- Maintain an up-to-date data inventory that identifies California personal information, processing purposes, systems, retention periods, disclosures, and service providers.
- Complete and document risk assessments before beginning processing activities that pose significant privacy risks, and establish a plan to assess activities already underway.
- Inventory automated decision-making technology and determine whether notice, access, opt-out, or risk-assessment requirements apply.
- Confirm that cybersecurity audit readiness covers governance, access controls, incident response, vendor oversight, testing, and executive certification requirements.
- Review service-provider and contractor agreements for required restrictions on the use, retention, disclosure, and combination of personal information.
- Align consumer-request procedures with actual system capabilities so that access, deletion, correction, and opt-out requests can be completed and documented within required timeframes.

Upcoming milestones include: (1) businesses that use automated decision-making technology to make significant decisions before January 1, 2027, must comply with the ADMT requirements by that date; (2) risk assessments for processing activities that began before January 1, 2026, and continue after that date must be completed and documented by December 31, 2027, with initial submission of risk assessment information to the California Privacy Protection Agency due by April 1, 2028; and (3) first cybersecurity audit certifications are due on a phased schedule based on annual gross revenue: April 1, 2028, for businesses with revenue above $100 million; April 1, 2029, for businesses with revenue between $50 million and $100 million; and April 1, 2030, for businesses with revenue below $50 million.

A defensible program should link the legal applicability analysis to specific data populations and controls. Internal audit and compliance testing should therefore include data flows and operating evidence, not only the privacy notice and written policy.

> **HOW AUDITONE CAN HELP**
>
> Privacy and cybersecurity control testing and audit-readiness assessments.

SOURCE
California Privacy Protection Agency - California Finalizes Regulations to Strengthen Consumers' Privacy (September 23, 2025)

OTHER NOTEWORTHY COMPLIANCE NEWS AND DEVELOPMENTS

OCC Updates Cybersecurity Supervision Work Program

In September 2026, the OCC updated the structure and references of its Cybersecurity Supervision Work Program (CSW) to align with the updated NIST Cybersecurity Framework categories and subcategories. The OCC did not add or change any examination procedures, and the CSW does not establish new regulatory expectations. Banks are not expected to use it to assess their own cybersecurity preparedness. Even so, the structure provides useful insight into how examiners may organize questions and evidence requests.

Institutions may find it useful to map cybersecurity policies, risk assessments, control testing, incident-response exercises, vulnerability management, access administration, vendor oversight, and Board reporting to the updated structure. Gaps in evidence, ownership, testing frequency, or escalation should be addressed before the next examination.

SOURCE
OCC Bulletin 2026-48 - Cybersecurity: Cybersecurity Supervision Work Program

CRA Aggregate Data Can Be Submitted Through Federal Reserve Reporting Central

Beginning with the 2027 reporting year (data due by March 1, 2028), banks required to report CRA aggregate data, or choosing to do so, will have the option to submit it through the Federal Reserve's Reporting Central portal. Existing submission methods, including email, will remain available, and the current process will continue for reporting years 2026 and earlier. Institutions that choose Reporting Central will need to coordinate among CRA, compliance, information technology, data governance, and third-party software providers.

Preparations should include confirming registration and user entitlements, verifying that vendor software can generate the required XML file, assigning submission and attestation responsibilities, retaining reconciliation evidence, and completing trial runs before the first Reporting Central submission. Vendor reliance does not transfer accountability for data completeness or accuracy.

SOURCE
FFIEC - Transition to Reporting Central

FDIC Revises Consumer Compliance Examination Manual

Following the August 2026 issuance of the new unsafe or unsound practice rule, the FDIC revised five chapters of its Consumer Compliance Examination Manual: Documenting the Examination (II-7), Investigations and Visitations (II-8), Appeals (II-11), Home Mortgage Disclosure Act (V-9), and Small-Dollar Lending (V-17). The FDIC also removed the "Bank of Anytown (III-2) Examination

Template" from its website. The FDIC has indicated it is conducting a broader review of the manual to incorporate recent rule changes, including Regulation B and the unsafe or unsound practice rule, so additional revisions should be expected.

FDIC-supervised institutions should review the revised chapters to understand how examiners will document findings, conduct investigations and visitations, and process appeals. Compliance monitoring and HMDA and small-dollar lending audit work programs should be updated where the revised procedures affect testing approaches or evidence expectations.

SOURCE

FDIC FIL-53-2026 - Implementation of the Final Rule on Unsafe or Unsound Practices; Matters Requiring Attention (August 27, 2026)

Interagency FAQs Address Mobile Driver's Licenses Under the CIP Rule

On September 8, 2026, FinCEN and the staffs of the federal financial institution regulators jointly issued two new FAQs and amended a previously issued FAQ addressing the use of state-issued mobile driver's licenses (mDLs) and other government-issued verifiable digital credentials (VDCs) to verify customer identity under the BSA/AML Customer Identification Program (CIP) rule. The FAQs do not alter existing BSA requirements or establish new supervisory expectations. The CIP rule neither requires nor prohibits reliance on government-issued VDCs. An unexpired, government-issued VDC, such as an mDL, qualifies as "government-issued identification" if it also evidences nationality or residence and bears a photograph or similar safeguard. A bank or credit union may use a VDC to the extent permitted by its CIP, so long as it maintains the appropriate technology or systems to extract the relevant information from the credential. If a government-issued VDC shows indications of fraud, the institution must consider that factor when determining whether it can form a reasonable belief that it knows the customer's true identity. For credentials issued and maintained by a non-government third party, the institution is responsible for ensuring that the third party uses the same level of authentication the institution itself would use.

Institutions considering acceptance of mDLs should confirm that the CIP expressly permits their use and that procedures address verification, exception handling, recordkeeping, and fraud monitoring. Vendor-supported identity verification solutions should be evaluated through third-party risk management, and BSA/AML independent testing should confirm that digital credentials are accepted only as permitted by the institution's CIP.

SOURCE

FinCEN - FinCEN Issues Frequently Asked Questions Regarding Treatment of Verifiable Digital Credentials Under the Customer Identification Program Rule (September 8, 2026)

Joint Statement Clarifies SAR Confidentiality When Communicating With Customers

On September 2, 2026, the Federal Reserve, FDIC, NCUA, OCC, and FinCEN issued a joint statement clarifying the confidentiality requirements for Suspicious Activity Reports (SARs) when banks and credit unions communicate with customers about potentially fraudulent transactions, other suspicious activity such as payment or check fraud, or account closures. The statement does not alter existing BSA requirements or establish new supervisory expectations. The BSA continues to prohibit disclosing a SAR or information that would reveal its existence. It does not prohibit discussing the underlying facts, transactions, and documents on which a SAR is based, or notifying a customer of an intention to close an account for potentially fraudulent or other suspicious activity, as long as the communication does not reveal the existence of a SAR.

Institutions should confirm that fraud, BSA/AML, and customer-service procedures and scripts distinguish between permitted discussion of transaction facts and prohibited disclosure of a SAR's existence, that customer communications are evaluated on a case-by-case basis, and that staff are trained accordingly. BSA/AML independent testing should include a review of how fraud-investigation and account-closure communications are handled.

SOURCE

FinCEN - FinCEN, Agencies, Issue Joint Statement on Suspicious Activity Report Confidentiality Considerations Regarding Communications with Customers (September 2, 2026)

CFPB Personal Financial Data Rights (Section 1033) Rule Remains on Hold

The CFPB's Personal Financial Data Rights rule implements Section 1033 of the Dodd-Frank Act and would require data providers to make covered data available to consumers and authorized third parties. In August 2025, the CFPB issued an advance notice of proposed rulemaking to reconsider key aspects of the rule, including who may act as a consumer's representative, fees for data access, data security, and data privacy. A federal court subsequently enjoined the CFPB from enforcing the rule pending reconsideration, so the original April 1, 2026, first compliance date did not become a binding enforcement trigger. Banks, credit unions, and fintechs that rely on data aggregation or data access should monitor the reconsideration and any revised compliance dates before finalizing implementation plans.

SOURCE

Federal Register - CFPB Personal Financial Data Rights Reconsideration, Advance Notice of Proposed Rulemaking (August 22, 2025)

KEY DATES TO WATCH

The timeline below lists upcoming compliance dates discussed in this Advisory, in date order, to support regulatory change management and audit planning.

DATE	DEVELOPMENT	WHAT TO DO
Dec. 16, 2026	Comments due on proposed interagency third-party risk management guidance (extended from Nov. 16)	Banks, credit unions, and fintech partners: finalize any comment letter
Jan. 1, 2027	CCPA/CPRA automated decision-making technology (ADMT) requirements apply to existing significant-decision uses	Covered businesses: complete ADMT inventory, notices, opt-out, and access processes
Jan. 18, 2027	GENIUS Act and OCC final rule take effect; payment stablecoin issuance generally requires approval	Banks and fintechs: confirm direct and indirect stablecoin exposure and approvals
Mar. 1, 2027	2026 CRA data due through the existing submission process	Banks reporting CRA data: complete data validation and submission
Apr. 1, 2027	FDIC official signs compliance date for websites, mobile apps, and ATMs	FDIC-insured banks: complete vendor changes, testing, and evidence retention

DATE	DEVELOPMENT	WHAT TO DO
Dec. 31, 2027	CCPA risk assessments due for processing that began before Jan. 1, 2026	Covered businesses: complete and document risk assessments
Mar. 1, 2028	First CRA aggregate data submissions eligible for Federal Reserve Reporting Central (2027 data)	Banks reporting CRA data: confirm credentials and vendor XML capability
Apr. 1, 2028	CCPA risk assessment attestations due; first cybersecurity audit certifications due for businesses with revenue above $100 million	Covered businesses: finalize audits, attestations, and executive certifications
July 18, 2028	GENIUS Act: digital asset service providers generally may not offer or sell payment stablecoins to persons in the United States unless issued by a permitted payment stablecoin issuer	Banks, fintechs, and custodians: inventory supported stablecoins and confirm issuer status

Dates reflect the regulator sources cited in each section as of November 25, 2026, and may change through subsequent agency action.

ABOUT AUDITONE

Established in 2003, AuditOne is an independent internal audit, compliance, and risk advisory firm specializing in regulated financial services. We serve banks, credit unions, fintechs, sponsor banks, Banking-as-a-Service programs, and payments organizations nationwide. Our senior-led, multidisciplinary teams deliver appropriately scaled, risk-based, and exam-ready assurance across internal audit, regulatory compliance, BSA/AML and financial crime, credit and lending, technology and cybersecurity, payments, operations, and enterprise risk management. Complementary advisory services are provided through Insight Risk Consulting, a registered trade name of AuditOne OH LLC, with responsibilities structured to preserve independence and objectivity.

For questions about this Advisory, contact Celeste Burton, CIA, Practice Director, Compliance and Director Credit Union Engagement Services, at Celeste.Burton@AuditOneLLC.com or (408) 597-4261.

To discuss AuditOne's services or request a proposal, contact Joe Saig, Chief Client Strategy and Growth Officer, at Joe.Saig@AuditOneLLC.com or (216) 505-6220, or Denise Shade, CEO, at Denise.Shade@AuditOneLLC.com or (213) 634-4001. Learn more at www.AuditOneLLC.com.