JENNER & BLOCK

Fintech Focus: How Regulatory Events of 2023 Should Guide Financial Institutions' New Year's Resolutions for 2024

Publications

January 10, 2024
By: Laurel Loomis Rimon, Gina Shabana

As consumer-facing financial institutions of all types—from well-established banks to newly-launched fintechs—set their 2024 regulatory compliance goals, they may wonder if their New Year's resolutions align with those that have been set by financial regulators for the upcoming year. In this article, we review the principles financial regulators outlined in 2023 guidance, regulation, and through individual enforcement actions, and highlight statements they have made in supervision and examination of priorities letters, all of which provide a roadmap to regulatory focus in 2024.

For instance, across all areas subject to regulatory focus, enforcement actions in 2023 reflected two overarching themes: (1) regulators expect financial institutions to be proactive in identifying and remediating risks and issues (e.g., through comprehensive risk assessments and planning); and (2) regulators are taking more coordinated/parallel actions where their jurisdiction overlaps and/or their interests align. An action by one regulator can be the impetus for other regulators to join in the action. It is also worth noting the expansion and restructuring of agency enforcement and supervisory teams in the past year. So, as you plan for annual risk assessments or other evaluations of programs subject to regulatory requirements, it is wise to keep the 2024 resolutions of financial regulatory agencies in focus.

A. Third-Party Relationships

Regulators' interest in third-party relationships is perhaps the loudest message coming out of the past year. As we described in a prior article, the Federal Deposit Insurance Corporation ("FDIC"), Federal Reserve System ("FRS"), and Office of the Comptroller of the Currency ("OCC") issued comprehensive Interagency Guidance on Third-Party Relationships on June 6, 2023, codifying their expectations for banks managing risks during the full life cycle of the third-party relationship. Similarly, 2024 examination priorities published by the OCC focus heavily on third-party relationships, with an expectation that third-party risk management programs should broadly cover all business areas including anti-money laundering, cybersecurity, and consumer protection (including data security). Key themes that we noted from regulators during 2023 include:

- **Comprehensive, enterprise-wide program**: Regulators expect a comprehensive 360-degree view of third-party relationships on an enterprise-wide level, meaning a third-party risk management program must (1) adequately address all areas of the business (e.g., cybersecurity, AML, etc.); (2) address due diligence prior to contracting and onboarding and continuously during the contractual relationship; (3) include adequate governance of the third-party's controls; and (4) timely and adequately escalate and remediate issues.

- **Heightened risks and novel issues**: Regulators expect the due diligence process to account for heightened and novel risks and have specifically called out relationships with fintechs in this category.

- **Governance**: Third-party risk assessment programs should adequately involve and inform the appropriate senior management and board of directors and include sufficient independent reviews and oversight of third-party relationships.

- **Remediation (or termination if necessary)**: Regulators expect financial institutions to hold third-parties liable and responsible for complying with the financial institution's expectations and contractual terms, and to terminate relationships where risk and issues cannot be alleviated.

- **Tailored**: Third-party relationship programs are not one-size-fits-all. Compliance programs must be customized to the particular product, service, and relationship, and must focus on corresponding risks.

- **Documentation and Record Retention**: Relying on a third party does not alleviate a financial institution's own responsibilities and risks. Due diligence and oversight relating to third-party relationships should be well documented and readily available to demonstrate compliance to regulators.

Noteworthy enforcement actions in 2023 relating to third-party relationships include Comenity Servicing LLC FDIC action, and Metropolitan Commercial Bank Federal Reserve Board and NYDFS actions.

B. AML/OFAC

AML/OFAC compliance has frequently been a key focus of regulators, and it continues to be the subject of regulatory enforcement actions and a regulatory priority for 2024. The Financial Crimes Enforcement Network's ("FinCEN") new Beneficial Ownership Information Reporting Rule also adds new requirements in the upcoming year. Key themes and information include:

- **Staffing and resources**: Regulators continue to focus on financial institutions' staffing and allocation of resources to ensure: (1) adequate and timely review of transaction monitoring

alerts (i.e., backlogs of alerts present a regulatory red flag), and (2) AML staff are properly qualified for their assigned functions.

- **Oversight of third parties**: Although regulated financial institutions can outsource some of their AML and sanctions screening functions, their legal obligation and liability cannot be transferred. Proper oversight and documentation of third-party relationships thus remains critical.

- **Governance**: Regulators remain focused on whether senior management and directors are sufficiently vested in compliance and remediation efforts.

- **Transaction monitoring**: Regulators (especially NYDFS) continue to focus on the adequacy of the validation and testing of AML transaction monitoring rules because they drive the detection of suspicious activity and subsequent reporting as needed. Further, regulators expect that a financial institution's systems will be integrated such that information is shared across platforms (e.g., transaction monitoring should integrate CDD, EDD and onboarding information, and should flag shared customer attributes – e.g., shared customer address or identification number).

- **Self-reporting**: Regulators are more forgiving when financial institutions self-identify, self-report, and adequately remediate issues, signaling that they have matters under control without a regulator's intervention.

- **NYDFS 504 Certification**: NYDFS continues to focus on Part 504.3 transaction monitoring certification requirements, which must be authorized by a company's Board of Directors or Senior Officer and attest to an institutions' compliance with NYDFS AML expectations, which are more expansive and prescriptive than those of other regulators.

Relevant enforcement actions in this area include Shinhan Bank America FinCEN and FDIC actions, Metropolitan Commercial Bank Federal Reserve Board and NYDFS actions, and the Coinbase, Inc. NYDFS Consent Order.

FinCEN Beneficial Ownership Information Reporting Rule: Subject to various exemptions and qualifications, the rule requires "covered entities" to report their beneficial ownership information to FinCEN starting on ***January 1, 2024***, and thereafter within certain time periods, depending on the date of formation of the company.

C. CONSUMER PROTECTION

Consumer protection continued to gain traction in 2023 as a significant regulatory focus, led by the Consumer Financial Protection Bureau ("CFPB"), but also by prudential and other federal and state financial regulators. As the Federal Reserve noted in its November 2023 Supervision and Regulation report, its "consumer-focused supervisory work is designed to promote a fair and transparent

marketplace for financial services and to ensure supervised institutions comply with applicable federal consumer protection laws and regulations." Banking-as-a-service activities and bank-fintech partnerships are particularly in focus for bank examiners, as reflected in the OCC's 2024 supervisory operating plan, along with unfair, deceptive, or abusive acts or practices (UDAAP). Consistent with the interagency guidance on third-party management referenced above, the OCC also highlighted a focus on third-party relationships, including ensuring clear and consistent communication and disclosures to consumers related to specific products or services and compliance challenges relating to fraud and error resolution, given the rise in the use of person-to-person payments.

Additionally, the CFPB issued its long-awaited proposed "open banking" rule, which would require "data providers," including fintechs that hold consumer financial data, to share that financial data with authorized third parties at the consumer's request. Although the rule is not yet final, financial institutions should prepare for that to come, which the CFPB has indicated should happen by ***fall of 2024***. The CFPB also published two "issue spotlights," one addressing digital payment apps, and the other on AI-powered customer service chatbots, both of which reflect the agency's intent to draw attention to consumer protection issues related to new technologies and platforms.

Finally, the CFPB proposed new regulation to extend its supervisory reach to "larger nonbank companies (with over 5 million annual transactions) that offer services like digital wallets and payment apps." The rule would impose on those entities the same rules, including those relating to fund transfers, privacy, and consumer protection, which apply to large banks and other financial institutions under the CFPB's jurisdiction.

Relevant enforcement actions: CitiBank, N.A. CFPB action, Chime, Inc. d/b/a Sendwave CFPB action, and Bank of America CFPB action.

D. CYBERSECURITY

Cybersecurity requirements also received substantial attention in 2023, with NYDFS significantly updating its Cybersecurity Regulation; regulated entities are required to have complied with reporting requirements by December 1, 2023 and to comply with most of the new requirements by April 29, 2024. Additionally, the Federal Trade Commission ("FTC") amended its Safeguards rule to impose reporting requirements for "certain data breaches and other security events," on non-banking financial institutions, including fintechs, financial planners, mortgage brokers, and others. The rule also requires these entities to establish and implement a "comprehensive security program" to protect customers' information.

Further, cybersecurity remains a focus area for regulators from an examination perspective, including the OCC. Specifically, regulators are looking into the adequacy of a financial institutions' incident response and reporting, data recovery, operational resilience, cybersecurity assessment, system and data backup techniques, inventory of assets, determining assets' life cycles and end-of-

life risks, vulnerability detection and remediation, multifactor authentication, and due diligence relating to third parties including validating third-party controls and data protections.

Relevant enforcement actions: bitFlyer USA, Inc. NYDFS Consent Order; OneMain Financial Group, LLC NYDFS Consent Order

E. FINTECHS IN FOCUS

As discussed above, regulators in 2023 explicitly highlighted their focus on fintechs, and banks' relationships with fintechs, as both high-risk and involving new and novel technologies and issues to be considered during examinations of financial institutions. Leading concerns in this area include products and services involving digital assets. In that vein, NYDFS continues leading the way, with California now having jumped into the arena and following in its footsteps. Both states took significant action in the last year to establish processes and requirements applicable to virtual currency businesses:

- **NYDFS Virtual Currency Guidance**: New York codified its expectations relating to listing of virtual currencies. The new guidance went into effect immediately upon its proposal on ***September 18, 2023***, and was revised/published in final form on ***November 15, 2023***. The regulation, among other things, requires all NYDFS Bitlicensees to establish a delisting policy, to meet with NYDFS by ***December 8, 2023***, to discuss their draft coin-delisting policy, and to submit their policy to NYDFS for review and approval by ***January 31, 2024***.

- **California Virtual Currency Regulations**: California signed into law The California Digital Financial Assets Law ("DFAL") and the Digital Financial Asset Transaction Kiosks on October 13, 2023. While exact contours of the regulation are yet to be defined, it is not too soon for digital asset businesses to start preparing for compliance under the new regulatory regimes. Effective ***July 1, 2025***, those engaging in digital asset business with or on behalf of a California resident must be licensed with the California Department of Financial Protection and Innovation ("DFPI"). The law includes reciprocity for those who are already licensed with NYDFS as of January 1, 2023, allowing Bitlicensees to receive a conditional license from DFPI, provided they satisfy certain fee requirements and comply with DFAL's requirements. Further, effective ***January 1, 2025***, operators of virtual currency ATMs will be required to comply with the new law's limitations on acceptance or dispensing amounts and transaction disclosure requirements, among other things.

- **CFPB Explicitly Addresses Digital Assets**: The CFPB's proposed rule regarding supervision of non-banks providing general-use digital consumer payment applications reflects the first instance in which the Bureau has explicitly defined digital assets as within its jurisdiction.

In sum, financial regulators are not hiding the ball. They laid out a roadmap in 2023, through blog posts, speeches, formal guidance, new regulations, and formal strategy and priority documents of what to expect in the new year on the regulatory compliance front. Each of these priorities should

now be reflected in the planning and updates being developed by each financial institution and/or the partner it relies on.

Related Attorneys

Laurel Loomis Rimon
Partner
lrimon@jenner.com
+1 202 639 6868

Gina Shabana
Associate
gshabana@jenner.com
+1 202 639 6076

Related Capabilities

Fintech and Crypto Assets

the laws of the State of Delaware, USA and is authorised and regulated by the Solicitors Regulation Authority with SRA number 615729. Information regarding the data we collect and the rights you have over your data can be found in our Privacy Notice. For further inquiries, please contact dataprotection@jenner.com.

Stay Informed →