Lessons Learned from Recent Enforcement Actions

Presented by:
Bryant (B.J.) Moravek
Maleka Ali

KAUFMAN | ROSSIN

ARC-SERV

Exam Focus

Regulators, especially examiners and supervisors, are focused on banking organizations' risk and risk management related to all third-party relationships, especially those involving fintechs and BaaS.

However, Common themes of deficiencies with BSA basics are still evident

The OCC's Perspective

Key areas of heightened focus for supervisory strategies in FY 2024:

- Asset and liability management
- Credit
- Allowance for credit losses
- Cybersecurity
- Operations
- Digital ledger technology activities
- Change management
- Payments
- Bank Secrecy Act/Anti-money Laundering/Countering the Financing of Terrorism and Office of Foreign Assets Control
- Consumer compliance
- Community Reinvestment Act
- Fair lending
- Climate-related financial risks

Key Takeaways for 2024

Third-Party Risk Management

Third-party risk management (TPRM) is no longer a standalone topic. TPRM can be applied to and is now embedded throughout several relevant OCC topics including cyber, operations, change management and consumer compliance. Given the interconnectivity of fintech and banking ecosystems, the OCC added language that directs examiners to assess a bank's existing risk management processes and controls of third-party relationships, particularly those with fintech companies.

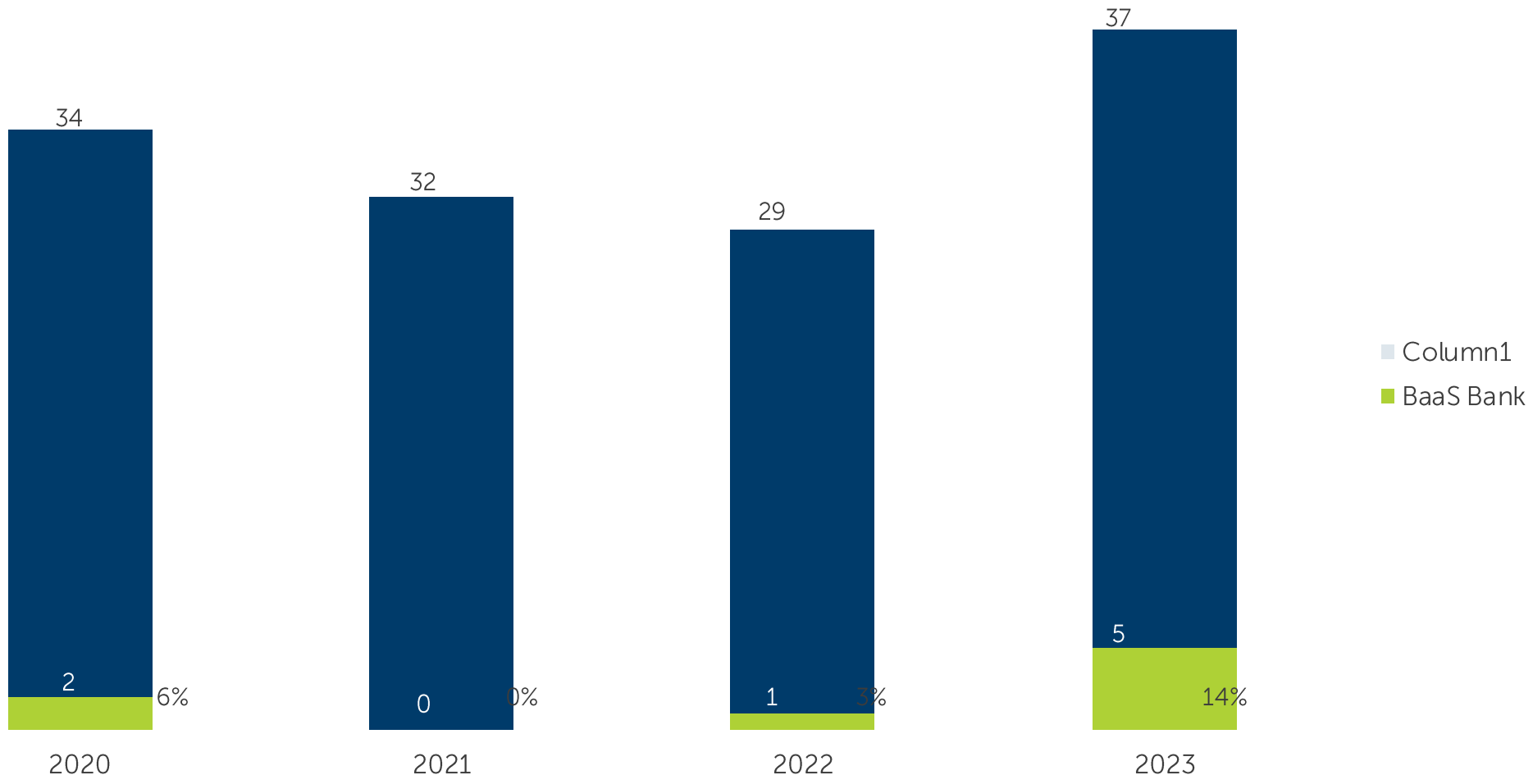
New Products and Services

Similar to TPRM, new products and services are no longer a standalone topic. Now embedded throughout relevant OCC topics, specific guidance within various sections is provided on considering novel products in the assessment of operations, change management, payments, distributed ledger technology, consumer compliance and credit. As an example, the OCC empowers examiners to evaluate existing payment systems, including the related products that are offered or planned – especially new or original products, services or delivery channels (e.g., person-to-person payments).

Board and Management Risk and Control Oversight

The OCC added language in the closing statement of the FY 2024 operating plan directing examiners to focus on significant risks and "the board and management's ability to control those risks." Examiners will continue to scrutinize the board and management's qualifications to provide effective challenges of risk and control activities. The OCC emphasized the importance of management having sufficient expertise to manage distributed ledger technology (DLT).

Severe Enforcement Actions 2020 - 2023



Source: S&P Global, January 2024 © CCG Catalyst

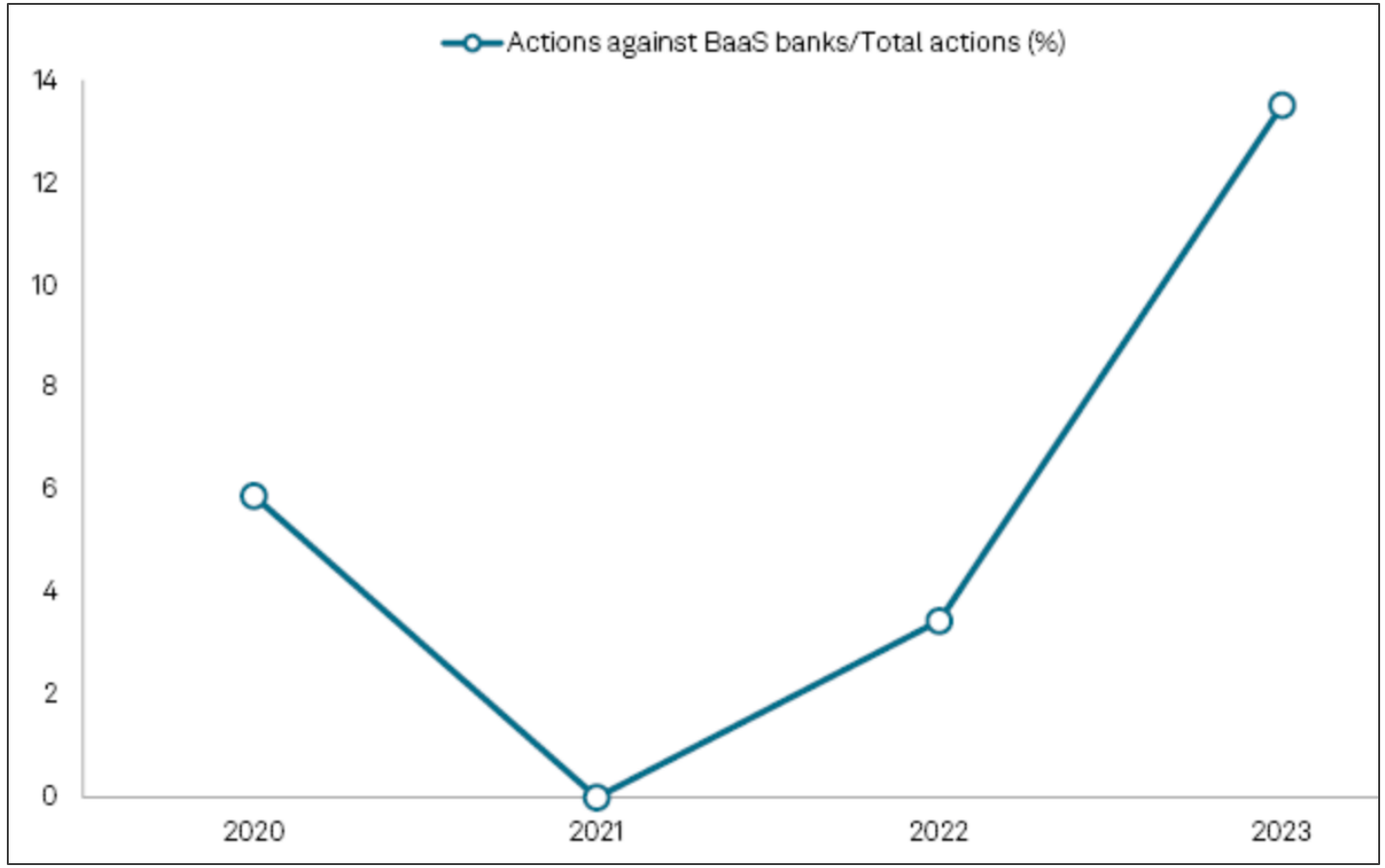
Severe Actions Include:

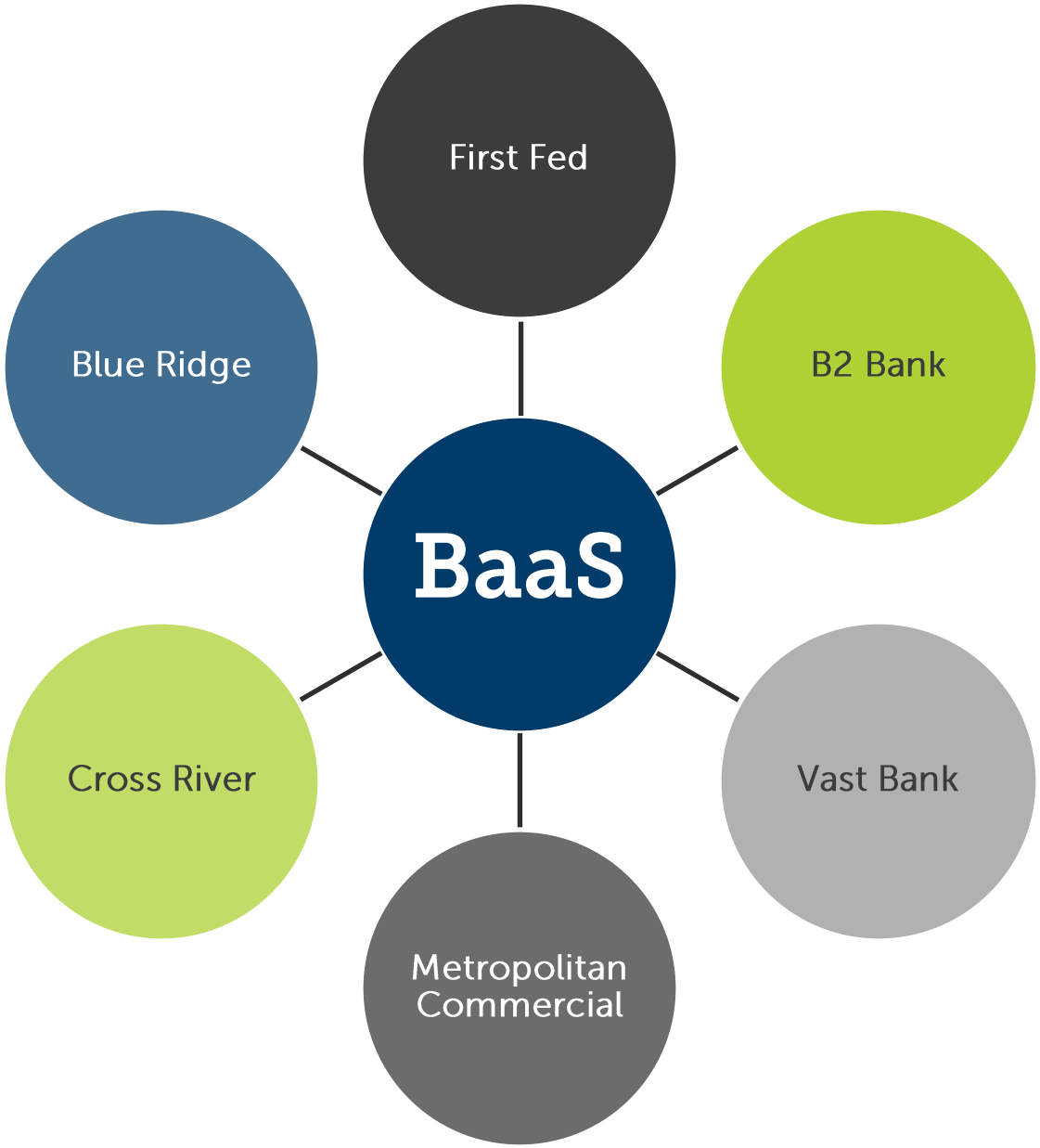
Prompt Corrective Action Directives

Cease and Desist Orders

Consent Orders

Formal Agreements made public by Federal regulatory agencies





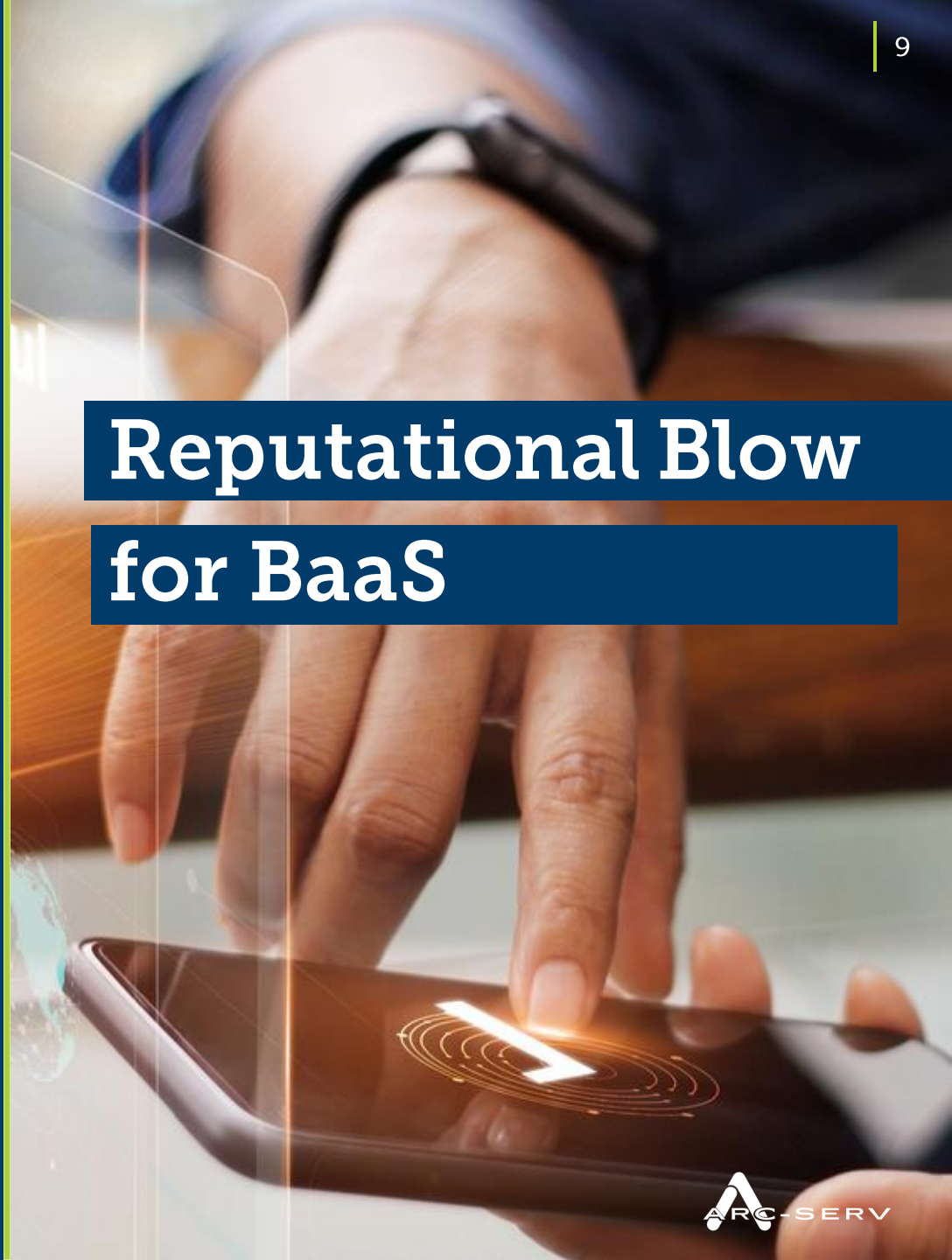
BaaS Troubles

Maybe Lapses in The Boring Aspects of Banking or...

- Poor risk management, insufficient capital controls, an absent compliance committee, or fair lending practices,
- Big difference for BaaS banks
  - problem often from one or more fintech partnerships
  - Third-party risk issue
- Complicated by fintechs' breakneck growth and lack of experience in financial services clashes with banks' risk and compliance obligations.

Reputational Blow for BaaS

- Problems related to third-party risk management and oversight
- Not the model itself (there are BaaS banks operating today without issue)
- De-risking all BaaS opportunities may not necessarily be the answer
- Goal
  - Know what you're getting into
  - What makes sense for your FI
- Heavy investment and commitment to a mix of:
  - Governance
  - Risk management
  - Taking special care with new partnerships and products



New Products, Programs, Services, Business Lines, Program Managers

- Written Program
- Close Oversight of Fintech Business Units
- Better KYC
- Third-Party Risk Management
- Stricter Controls
- Infrastructure to effectively manage third-party risk

Sponsor Bank Hardships

- About 2% of U.S. Banks, however account for 13.5% of severe enforcement actions last year.
- Number is rising and impacts can be severe.
- Several BaaS banks received consent orders/cease and desist orders and forced to pay $$$$$.
- Remediation costs can amount to 12x the original fine.
- Enforcement actions may result in loss of new programs, vendors, reputational damage, compromised business plans.
- A bank under a consent order cannot make major changes to grow the business.

First Fed Bank – Washington – FDIC

Included in Consent order:

- Board must participate in oversight of bank's compliance management system
- Submit list of products to the FDIC regional director for review
- Can't enter a binding commitment or agreement with a new 3rd party without regional director's written non-objection
- Ordered to implement several policies to enhance third-party oversight
- Review/approve all third-party marketing materials
- Establish processes managing regulatory agency inquiries, customer complaints and legal actions
- Review third-party service providers' policies and practices to determine compliance with all consumer protection laws

B2 Bank – Minnesota – OCC

Unsafe or unsound practices relating to internal controls

Requirements:

- Board appointed a Compliance Committee
- Strategic Plan
- 3rd Party risk management processes
- Model risk management program
- New products and services risk assessment process
- BSA/AML Risk Assessment Program
- Concentration Risk Management

Metropolitan Commercial Bank – NY - FRB

- CIP rule requires MCB to implement a CIP *"verify the identity of each customer sufficient to enable MCB to form a reasonable belief that it knows the customer's true identity"*
- Widespread fraud related to Movo program
- Must implement new product review program
- Enhance Customer Identification Program (CIP)
- Implement 3rd Party Risk Program

Cross River Bank – New Jersey - FDIC

- Unsafe or unsound banking practices
- New CRB Credit Products and New 3rd Parties
- Information System Review
- Fair Lending Compliance Risk Management
- 3rd Party Compliance Internal Controls
- Directors' Compliance Oversight Committee
- Non-Objection Adherence/Progress Reports/ Shareholder Disclosure

Choice Financial Group – North Dakota - FDIC

- Board must improve oversight of AML/CFT Program and assume full responsibility and meet monthly to discuss compliance with the consent order:

- Bank's 3rd-Party Relationships
- Revise the AML/CFT Program
  - ML/TF Risk Assessment
- Revise the System of Internal Controls
  - Customer Identification Requirements
  - Customer Due Diligence Policies
  - Suspicious Activity Monitoring/Reporting
- **Lookback Review for all customers on-boarded thru 3rd-Party Relationship**
  - Ensure compliance with CIP, CDD, and SAR requirements of BSA
- AML/CFT Model Validation
- AML/CFT Staffing and Resources – Staffing Assessment – Resource Plan
- Independent Testing (Audit) Program
- Training

ARC-SERV

Blue Ridge Bank – Virginia - OCC

Unsafe or unsound practices, including:

- 3rd Party Risk Management
- BSA/AML Risk Management – Risk Assessment
- BSA Audit Program
- BSA Compliance Personnel
- Customer Due Diligence-Enhanced Due Diligence- High-Risk Customers
- Suspicious Activity Reporting – Must include Fintech 3rd Party activity
- Lookback to include high-risk customer activity involving 3rd party relationship partners
- Information Technology Control and Risk Governance

City National Bank – California – OCC

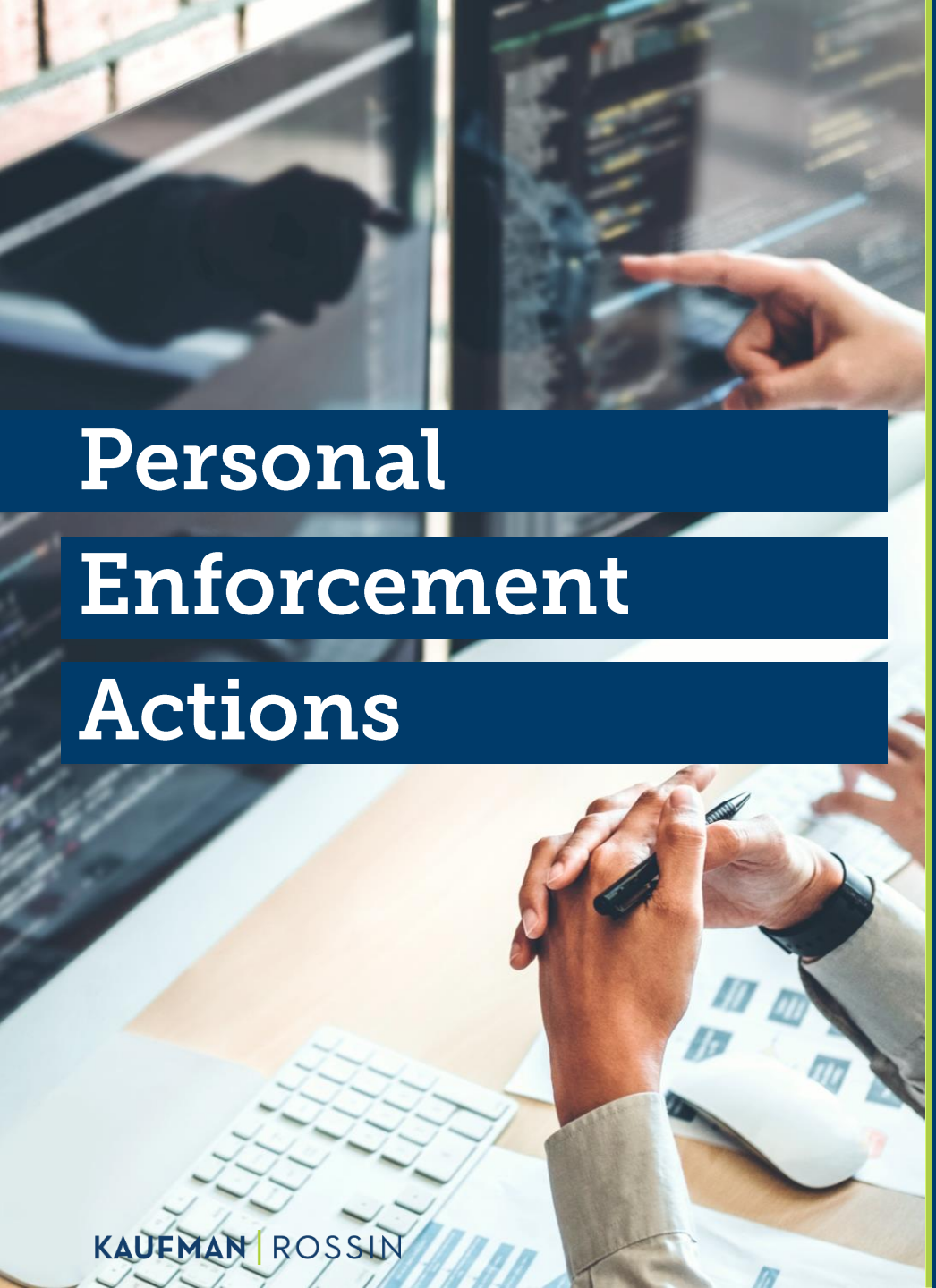
BSA/AML Articles include:

- Change control and validation of AML system models
- Procedures to ensure accurate and timely SARs and CTRs
- Staffing Assessment
- Customer Due Diligence and Risk Identification
- BSA/AML and OFAC Risk Assessments
- Internal Audit

Royal Business Bank – California – FDIC/DFPI

Comply with AML/CFT Rules and Regulations – within 120 days

- Enhance and implement written acceptable compliance program
- Review and improve the system of internal controls
- Qualified officer
- Provide and document tailored training (updated and ongoing)
- SARs Policy and Procedures
- Acceptable Customer Due Diligence Program
  - Risk scoring system calibration/validation
  - High-risk customer reviews
  - Reviewing alerts for high-risk customers



Personal Enforcement Actions

Regulators use enforcement actions and fines against individuals to deter, encourage correction of, or prevent violations, unsafe or unsound practices, or breaches of fiduciary duty.

Enforcement actions against individuals reinforce accountability for their conduct.

An Order of Prohibition would prohibit a party from ever working for a Federally insured depository institution.

The Path Forward

Upfront Threat assessments for new products, services, and 3rd party relationships

Include 3rd Party relationships in all aspects of the AML/OFAC program

Enhanced Independent Audits

More oversight

Questions?