Current Regulatory Hot Spots

WBA Webinar
August 13, 2018

Presented by:
Jeremy Taylor, Co-CEO, AuditOne LLC

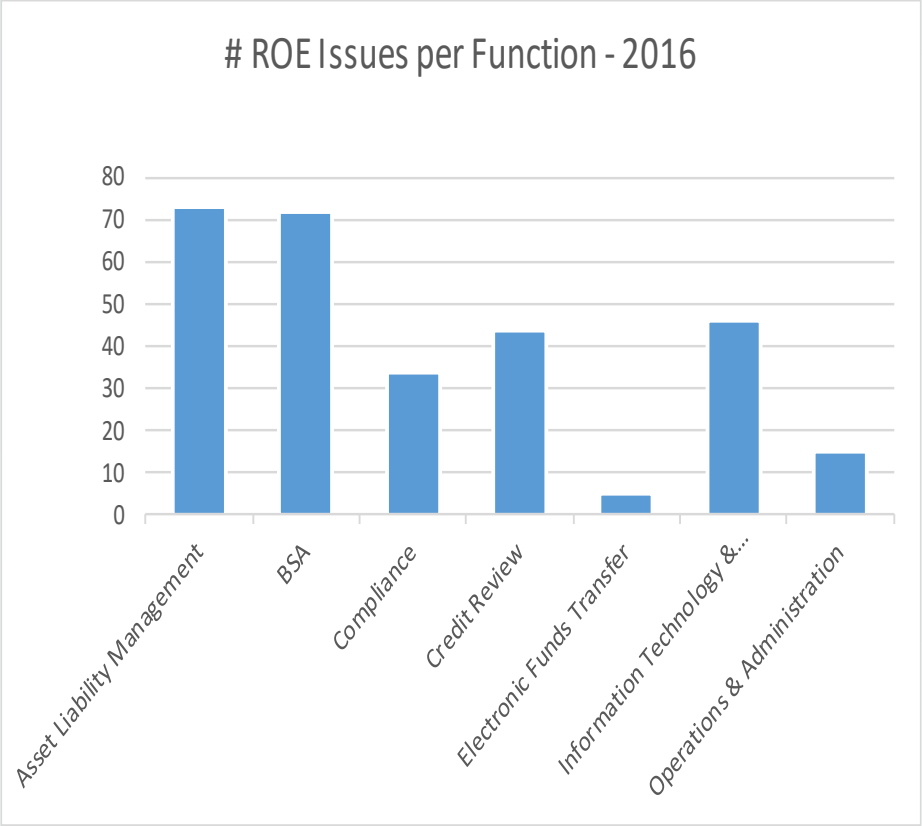
AuditOne LLC

Western Bankers Association (WBA) makes no representations or warranties about the accuracy or suitability of any information in the webinars and related materials (such as presentation documents and recordings); all such content is provided to webinar registrants on an "as is" basis. WBA HEREBY DISCLAIMS ALL WARRANTIES and Conditions Express Implied Statutory or Otherwise REGARDING THE CONTENTS OF THESE MATERIALS, INCLUDING WITHOUT LIMITATION ALL WARRANTIES OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. WBA is not liable for any claims, losses, or damages of any kind arising out of or in any way related to this information provided by presenters of these webinars. WBA hereby disclaims all liability for any claims, losses, or damages of any kind in connection with use or application of these materials. The information contained in these webinars and related materials is not intended to constitute legal advice or the rendering of legal, consulting, or other professional services of any kind. Users of these materials should not in any manner rely upon or construe the information or resource materials in these materials as legal, or other professional advice and should not act or fail to act based upon the information in these materials without seeking the services of a competent legal or other professional.

Introduction

- Our business provides us regular insights into what regulators are emphasizing, their expectations for financial institutions (FIs), etc.
- Insights obtained from:
  - (Safety & Soundness, Compliance) exam reports
  - Client discussions
  - Auditor feedback
  - Conversations with regulators
- Data shows as 2016 exam reports; 2017 results still only partially reflected in our audit reports
- More information on AuditOne is provided in the Appendix to this presentation

From a Sample of 79 2016 Safety & Soundness Reports of Examination



AuditOne LLC

Start with Governance Issues

- More of a FRB/OCC concern, but percolating down
- Strategic planning
  - Board involvement
  - Time horizon – at least 3 years
  - Integrate with budget
- Succession planning
  - Short-term emergency procedures
  - Longer-term succession
- Risk appetite
  - Sets concentration and other risk limits
  - Incorporates stress-test results
  - Accounts for constraints (capital, liquidity, etc.)

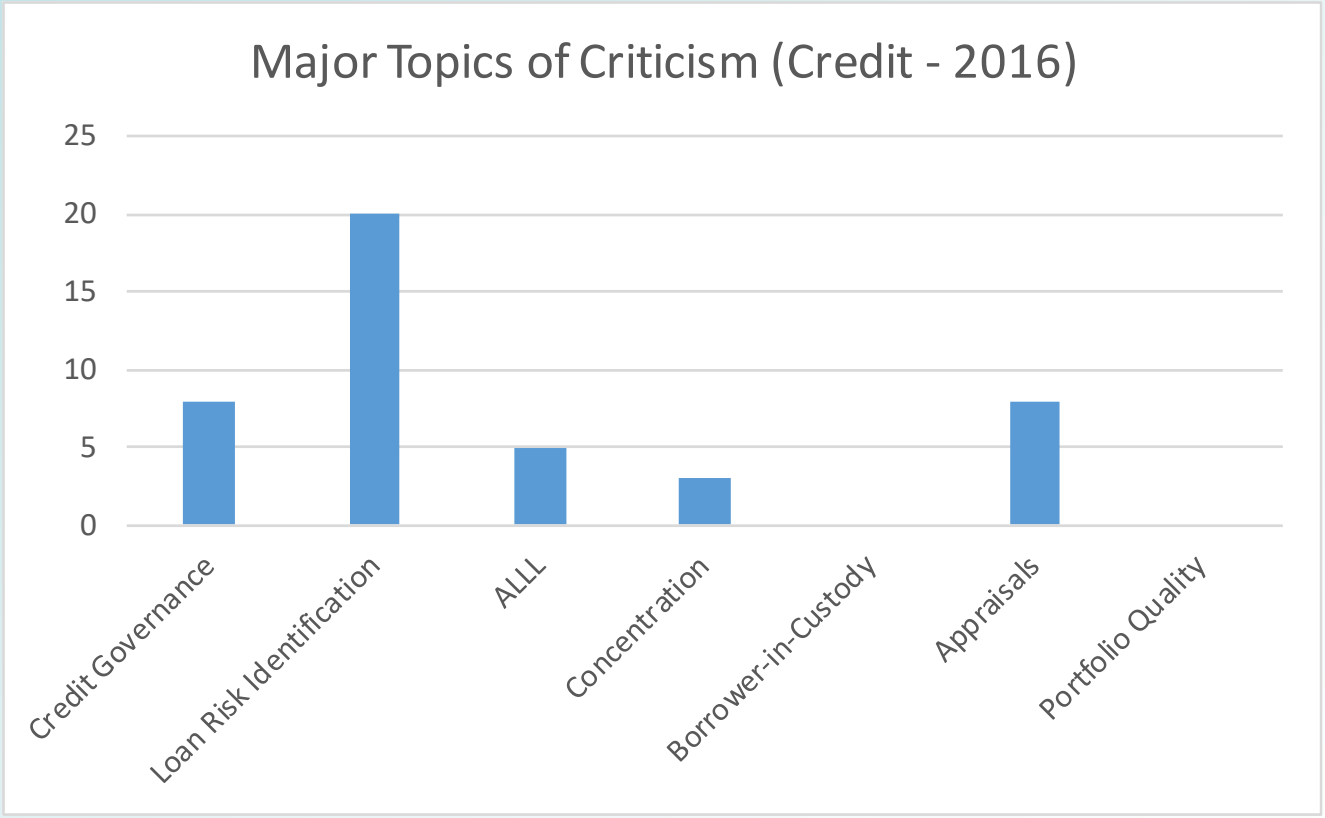
ERM, ERA

- Enterprise Risk Management (ERM)
  - No roadmap, but some regulators looking for moves
  - ERA (see below) is a core component; so is risk culture and communication, plus tools and processes for monitoring and reporting on risk profile
  - Big challenge: standardized risk measurement
- Enterprise Risk Assessment (ERA)
  - Required for annual audit plan foundation
  - Based on inherent risk across each functional area, but should also reflect control environment (residual risk)
  - Determination of audit needs independently of mgmt.

Board Oversight

- Ensure meeting minutes capture relevant discussion
- Annual review and approval of policy docs
- Exception reporting, limit violations – including strategy to address violations
- Corrective action tracking
- Audit and Supervisory Committees gets particular attention
- Importance of direct communication between AC/SC and auditors, incl. presentation of results
- Executive session with auditors (in minutes)

Credit and Lending: Sampled S&S ROE Criticisms



AuditOne LLC

Credit and Lending Issues

- Loan risk identification (i.e., sampled loan file review): getting more attention again, esp. for (indirect) auto, multifamily, leveraged loans – has overtaken ALLL in ROE comments
- Concentration risk management becoming ever more important (and not just for CRE)
- Stress-testing: percolating down-market
- TDRs: getting the accounting right (e.g., what's a modification), and the required reporting (e.g., Call Report vs. ALLL reporting)
- Timely receipt of borrower financial info

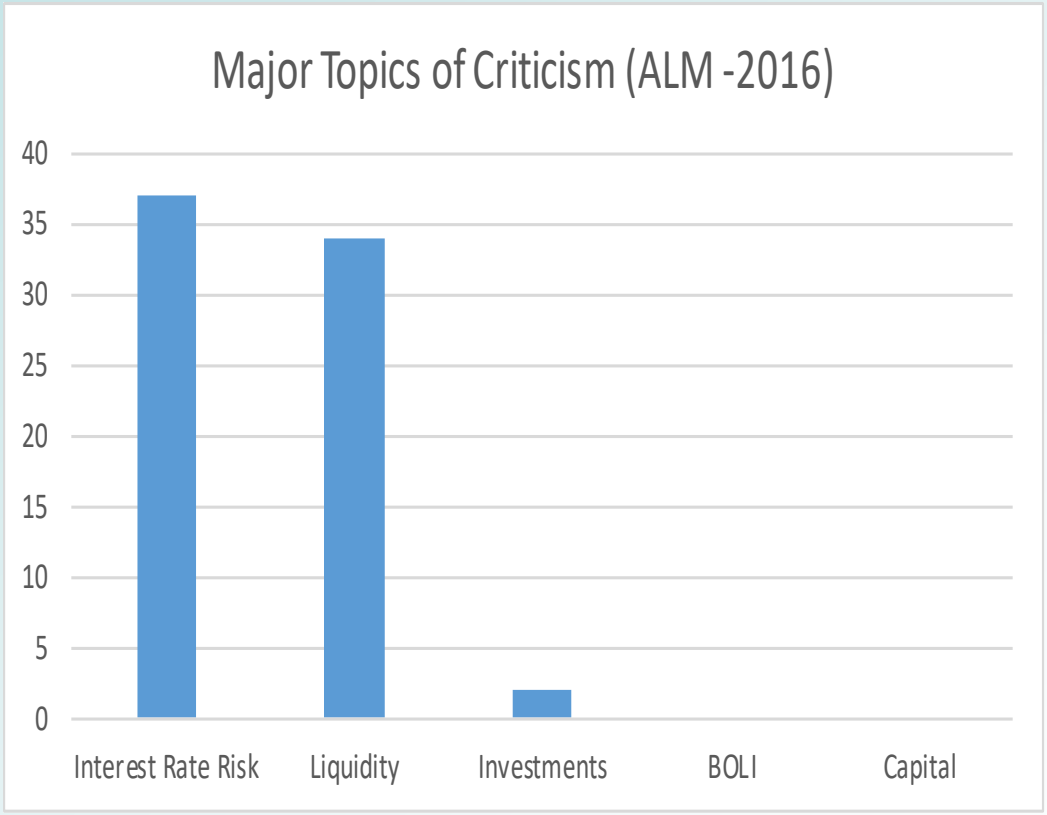
Credit Issues – Cont'd

- HELOC end-of-draw risk
- Cash flow calculations
  - Global
  - Living expenses
  - Exclude non-recurring items
- Annual term loan review process
- Risk rating system clarity
- Avoid incentives for risky lender behavior
- Participations (re-underwrite to purchaser's standards) plus due diligence on pool purchases
- Board reporting: exceptions, stress test results

ALLL

- Use internal loss history, and with longer look-back (at least 3 – 4 years)
- Two-dimensional loss factors, differentiated according to 1) loan type, 2) risk grade
- Use Q&E adjustments (per 2006 Guidance) to bridge between look-back period and today; directional consistency, ballpark reasonableness
- Impairment documentation/support
- Off-balance sheet reserving per ASC 450-20
- Prepare for CECL: more granular data collection for more variables, as far back as possible

Asset/Liability Management: Sampled S&S ROE Criticisms



AuditOne LLC

Interest Rate Risk

- ALCO: meeting frequency, reporting of policy (incl. limit) exceptions, detailed minutes
- Emphasis on model assumptions: customize and validate, with regular ALCO presentation
- Non-maturity deposits: repricing, average life
- “Surge deposits” = recent deposit growth at risk of departing as rates rise, with implications for funding cost, NII
- Non-interest income effects, NII back-testing
- EVE-at-Risk: not so user-friendly, but regulators expect education, discussion

Liquidity Risk

- Getting heavy emphasis (even though liquidity is mostly strong) – due to surge deposit risk
- Contingent funding plan, liquidity stress-testing: tie the two together, in particular to address significant loss in deposits
- NII impact via cost of funds, net interest margin
- Core deposits vs. wholesale funding
- Brokered deposits: some easing in treatment of CDARS, but more scrutiny of Internet deposits
- Test borrowing lines annually
- Inaccurate ratio calculations

Investments

- Most small FI investment portfolios remain low credit risk, even as they absorb excess liquidity
- Credit analysis (pre-purchase, plus post-purchase updating) for all but Treasurys and Agencies: not just agency ratings (per Dodd-Frank)
- Regulators watching for duration extension ("reaching for yield")
- Policy limit for investment portfolio impact on EVE under specified (e.g., +300 bps) rate shocks

Capital

- Basel III phase-in (began Jan./15), with more complex calculations, reporting requirements
- Most small FIs still comfortably above required minimums, even allowing for 2.5% Capital Conservation Buffer (to avoid dividend and bonus restrictions)
- More attention to capital policy, including contingency planning
- Lots of capital = less concern with other CAMELS weaknesses
- EGRRCP Act gives banks < $3B more options, incl. minimum Community Bank Leverage Ratio

Compliance

- Compliance Mgmt. System (CMS) = Board/mgmt. oversight + Compliance Program (CP) + audit
- CP = policy & procedures + training + monitoring
- Risk Assessments: for Compliance overall and for key regs individually
- Management oversight of third party providers in terms of consumer compliance
- Reviewing for regulatory violations is important, but those are problems that have already happened; reviewing CMS helps prevent future problems

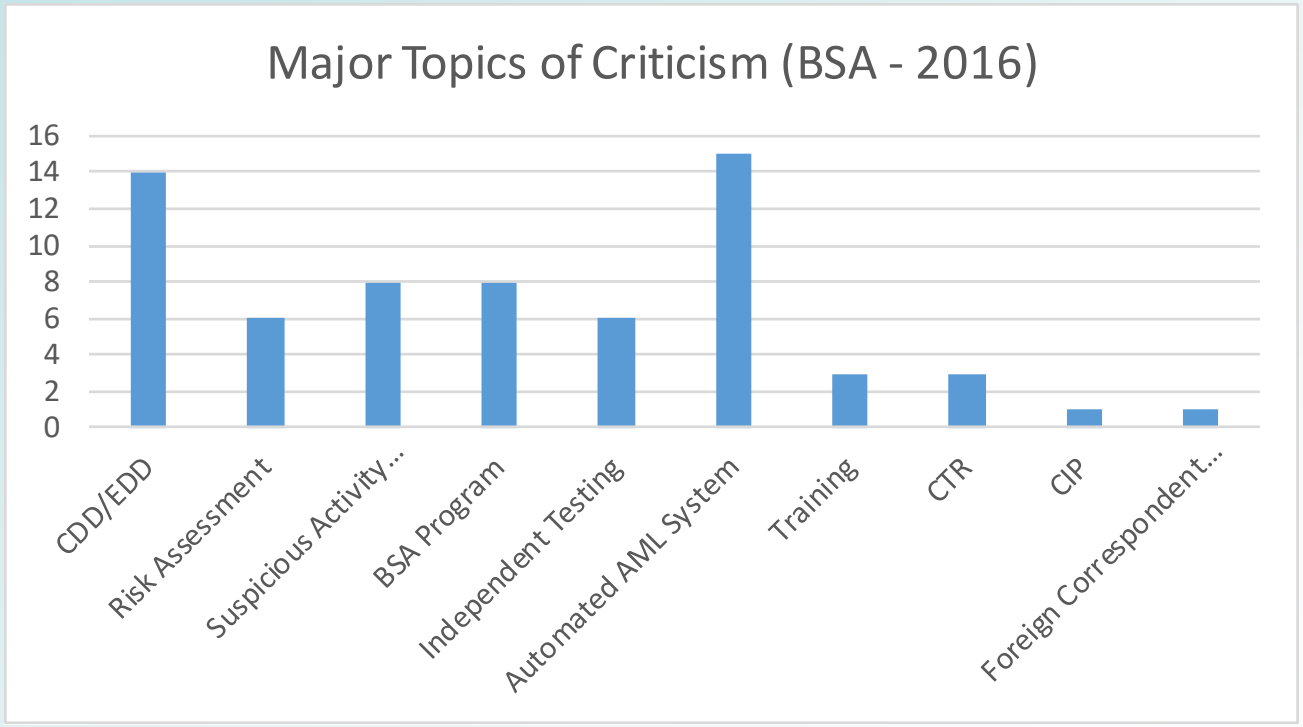
CFPB/Dodd Frank Focus on Lending Regs

- … Especially mortgage and consumer lending
- HMDA: low tolerance for LAR errors … and now increased GMI reporting requirements
- Fair Lending: looking for disparate impact, not just for mortgages (using GMI) but also for consumer and other loans (using “surrogates”)
- Fair Lending Risk Assessment, training
- Flood insurance: continued pickiness
- 2016 FFIEC’s UICCRS (Uniform Interagency Consumer Compliance Rating System)

Lending Regs – Cont'd

- Reg Z/RESPA: getting TRID disclosures right
- Appraisals: criticism of appraiser calculations; internal review process (incl. reviewer qualifications); independence (re: ordering appraisals); updates for OREO properties
- Reg O: verifying non-preferential treatment
- UDAAP: early days, only preliminary indications of CFPB aggressiveness (overdrafts, credit cards, payday loans) but more to come?

BSA/AML:
Sampled S&S ROE Criticisms



AuditOne LLC

BSA/AML – Pillar Issues

- Adequacy of AML Program resources, incl. BSA Officer qualifications, trained support staff
- Fifth Pillar, Customer Due Diligence (CDD): documentation of expected vs. actual transaction activity, consistent/accurate customer risk ratings
- Preparation for beneficial ownership (May/18)
- Independent testing (audit):
  - depth of testing
  - customization for the FI's risk profile
  - workpaper review
- Board reporting

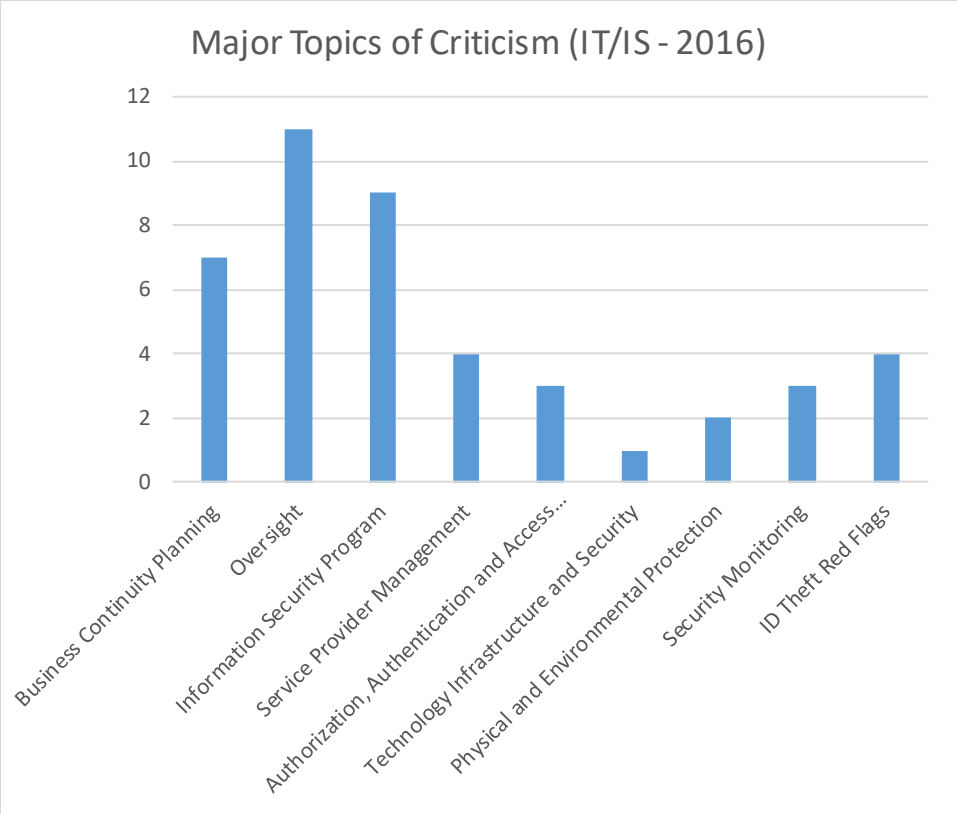
BSA/AML – High Risk Areas

- Documentation of EDD reviews
- Particular attention to MSBs, NRAs, TPPPs, MRBs, et al. – all requiring extra due diligence and monitoring
- Include all potentially high-risk areas in the BSA Risk Assessment
- Support the risk ratings, quantitatively where possible
- Overall rating for inherent and residual risk

BSA/AML – Suspicious Activity Monitoring

- Managing alerts, responding in timely and appropriate fashion
- Documenting decision not to file a SAR
- International activity monitoring
- Validation of automated monitoring system data integrity
- Internal review of the effectiveness of filter criteria

IT / IS / Cybersecurity: Sampled S&S ROE Criticisms



AuditOne LLC

IT / IS Governance

- Documenting in Board meeting minutes: discussion points; annual approval of policies, risk assessments; review of critical service providers
- Monitor corrective action status of prior (exam, audit, pen test) findings, with annual reevaluation and reaffirmation of accepted risks
- Board-appointed IT Steering Committee, with at least quarterly meetings
- IT Manager separate from ISO: for > $1B
- Annual ISO Report to the Board (e.g., security incidents, handling of sensitive data), per FDIC

IT Risk Assessment

- Address all information assets (incl. hardware, software, data, connections, cloud services)
- Tie in with end-of-life management
- Identify source of threats (internal, external, service provider)
- Bring in controls and their effectiveness (to link inherent and residual risk)
- Provide overall (H/M/L) rating

Cybersecurity

- FDIC expects cybersecurity to be integrated into the IS Program and the IT/IS audit plan
- Preparation of Cybersecurity Assessment Tool
- Multi-layer controls to prevent hackers from destroying your data, your replicated environment, and your back-up
- For critical vendors, you need to understand their cybersecurity resilience, safeguards, etc.
- Info sharing (e.g., FS-ISAC, US-CERT), educating employees

BCP/DRP

- Plan components:
  - Plan may contain out of date information
  - Ensure recovery procedures are in place for critical business functions, incl. back-up power and staff
  - Alternate site not too close to head office
- Importance of regular and comprehensive tests:
  - Run cyber-threats, including key vendor contract obligations (per FDIC testing guidance)
  - Include transactional testing for alternate site test
  - Tabletop testing on pandemic outbreak
  - Define DR test success criteria – e.g., compare actual recovery times with RTOs

Vendor Management

- Risk assessment for each vendor
- Robust due diligence (with contract checklist), plus timely, ongoing, risk-based monitoring
- It's not just IT service providers, and it's not just high risk vendors
- Ask for regulatory reports on critical vendors (e.g., core providers, BSA-related services)
- Other reviews: CS awareness, audit results, BCP test results, SLA compliance
- Not just a check-the-box review
- Vendor contracts: IS breaches, confidentiality

ID Theft / Red Flags

- Training, especially for new hires
- Annual update of ID Theft risk assessment and policy
- Annual ID Theft/Red Flags report to the Board
- Review of core processor's compliance with ID Theft/Red Flags requirements

Access Issues

- Annual review of user access rights on all critical systems
- Isolate security cameras, ATMs, VOIP devices to a separate network
- Independent administrator activity review for critical systems
- Shared system administrator credentials
- Delete access for terminated users

Other IT Issues

- Periodic review of firewall rules
- Social engineering should test all employees
- Pen test frequency driven by IT Risk Assessment, but moving towards quarterly scans
- Corrective action tracking of pen tests results, with Board sign-off for risk acceptance
- Develop formal document imaging policy
- Expand patch management policy to outline timeframes based on criticality of the patch

Other IT Issues – Cont'd

- Hardening policy:
  - Change default credentials and default configurations
  - Unauthorized software installs
  - Remove unnecessary programs
- Background checks on contractors as well as employees
- Mobile devices not configured with standard security controls
- External hard drives used for back-up rotation not encrypted

EFT – General Issues

- Risk assessments for all EFT services and E-Banking applications: cash management (RDC, ACH, wires), online banking, mobile banking, merchant card services, etc.
- New risk assessment required for new service offering or converting to a new service provider
- Ensure policies reflect current practices (e.g., uncollected funds, suspicious activity reporting to BSA department)

EFT – General Issues (Cont'd)

- Ensure customer due diligence is completed and well documented
- Common examiner findings include:
  - Missing date of execution in cash management agreements
  - No record for new RDC customer training
  - Lack of wire transfer agreement for not-in-person wire transfers

Wires: Fraud Risk Concerns

- Wire Transfer Policy should be comprehensive, should reflect actual practice (e.g., current system used), should be supported by written procedures for processing wires
- Separation of duties:
  - Incoming wires: between receipt of wire vs. posting to customer account
  - Outgoing wires: between enterer vs. verifier, between oversight vs. reconciliation functions, between balancing vs. servicing of FRB and correspondent accounts

Wire Transfers – Cont'd

- Outgoing wires:
  - Only allow e-banking or fax as a submission channel; avoid e-mail and telephone (high fraud risk)
  - Perform callback on a different communication channel (e.g., telephone callback for e-banking wires)
  - Enable call-back feature when processing manual wire transfer telephone request from correspondent
- Ensure client wire transfer agreement is in place
- Have dual (back-up) wire system/channel – e.g., Fedline plus PCBB or Wells Fargo
- Remove unnecessary wire users
- At least annual testing on DR wire system

Remote Deposit Capture

- Daily limits
- Educate customers re handling/disposition of remotely deposited checks
- Periodic monitoring of high risk customers (once or twice a year is acceptable), duly documented
- BSA department review before accepting new RDC customer

EFT – Other Concerns

- Online Banking, Mobile Banking:
  - Implement MFA controls
  - Ensure completed cash management agreements
  - Address “jail-broken” phones (= privilege escalation to get around software restrictions imposed by Apple and Android)
- Automated Clearing House (ACH):
  - Doesn’t get much examiner attention – rely on annual WesPay self-audit
  - Watch controls over IATs (international ACH transactions)

Operations, Administration

- Generally low risk profile (e.g., infrequent S&S exam report attention)
- Certifications program does get attention: it provides ongoing assurance to management and Board re effectiveness of internal controls
- Audit to ensure key G/L accounts and functions get certified (accurately, regularly)
- Segregate certifications from accounting and operational duties
- Segregation of duties always a challenge for small FIs (sharing, cross-training)
- Dormant controls, incl. timely escheatment

Other Ops/Admin Concerns

- Controls over garnishment processing
- Multi-branch FIs: Does Central Ops set branch procedures (see below) and perform oversight function (e.g., exception monitoring, loss monitoring, large item review)?
- New account opening: CIP/KYC
- Also: branch staff knowledge of BSA/AML
- Branch security
- Two-week vacation for sensitive positions
- Call Report errors
- Timely charge-off of suspense items, O/Ds

And Finally …
Written Procedures

- Having comprehensive and up-to-date written procedures is an important discipline:
  - Responsibility
  - Accountability
  - Continuity
  - Consistency
  - Education/training
- Should be reviewed and approved by senior manager – but (unlike policies) Board approval not necessary

Appendix:

Overview of AuditOne LLC

AuditOne: Who We Are

- A high-quality, cost-effective provider of outsourced internal audit and credit review services, plus related advisory work
- Around 300 clients nationally, most of them community banks or credit unions and based mainly in the Western states
- We are the largest firm in the Western US focused on internal audit services for FIs
- Close to 40 professional employees, with a broad and deep range of banking expertise; our staff averages 25+ years of relevant experience

A Full-Service Menu

- Credit/ALLL
- Compliance/BSA
- IT/IS
- Operations/Administration
- Asset/Liability Management

- We also offer advisory services (via our affiliate, Insight Risk Consulting), as well as set-up and testing for both Sarbanes-Oxley Section 404 and FDICIA 36

Our Management Team

- Bud Genovese, Chairman
- Jeremy Taylor, Co-CEO (Northern clients)
- Kevin Watson, Co-CEO (Southern clients)
- Ling Genovese, CFO
- Angela Canda, Office Manager
- Practice Directors:
  - Celeste Burton, Compliance
  - Kevin Tsuei, Technology
  - Brock Williamson, Credit
  - Gary Andreini, Operations
  - David Kellerman, ALM
  - Genelle Wrzesinski, EFT

How to Reach Us

- Northern office: 408-980-8099
- Southern office: 562-802-3581
- jeremy.taylor@auditonellc.com, 949-981-0420
- kevin.watson@auditonellc.com, 562-455-6979
- bud.genovese@auditonellc.com, 408-691-6844