FDIC San Francisco Region's Regulatory Update

Introductions

From the San Francisco Regional Office:

- Assistant Regional Director Paul Worthing
- IT Examination Specialist Lloyd Miller
- IT Examination Specialist Eugene (Gene) Moyes
- Compliance Analyst Linda Nutter
- Special Activities Case Manager Christy Cornell-Pape

Joining us from Washington, D.C. is

- Senior Technology Specialist Robert Drozdowski

Today's Topics

- FDIC returning to full-scope 2007 IT Relationship Manager Program (IT-RMP) Examination Procedures
- Common IT Examination Findings
- Relationships with Third Party Payment Processors

IT Relationship Manager Program (IT-RMP) Examination Procedures

Concepts

- Risk focused program applies to all FDIC-supervised financial institutions
- “Top Down” – Management Centric focus
- Flexible use of work programs
- All bank IT Examinations will continue to be embedded within the S&S Examinations

IT-RMP Focus Points

IT-RMP focuses on management of the Information Security Program with emphasis on:

- Risk Assessments
- Controls/Mitigation (Operations Security and Risk Management)
- Independent review/testing (Audit)
- Business Continuity Management
- Service Provider Oversight
- Board/Management Oversight/Reporting
- Compliance with FACTA
- All of the above impact GLBA compliance

Procedures

- **Ratings**
  - Composite rating only
    - Quality of the Information Security Program is management centric
  - Placing the IT rating with the Risk Management ratings will serve to highlight the relationship between business-related risks and technology-related risks

Common IT Examination Findings

Safe Guarding Customer Information (GLBA) Program Weak or Out-of-Date

- Poor independent review process to ensure compliance (Either not annual; not independent, or not comprehensive)
- Poor risk assessment process and/or out-of-date
- Weak Vendor Management Program to ensure bank customers info is adequately protected.
- Weak documentation of Board and senior management oversight
- Weak Incident Response Program (FIL-27-2005 “Guidance on Response Programs”)
- Weak training program

GLBA - Risk Assessment - GLBA

- Should cover anywhere sensitive information is transported; processed; stored; and ultimately destroyed whether via people; paper; or technology.
- Cover information for its entire lifecycle

Common Weaknesses

- Not enterprise-wide – Misses departments, technology specific, forgets service providers
- Does not detail how risks are mitigated
- Does not detail how controls/mitigation strategies are tested

Annual GLBA Program Status Report to the Board

- The Board should receive reports, at least **annually**, on the overall status of the program that includes and documents a discussion of all the below items:
  - Overall status of the program
  - Material Risk Issues
  - Risk Assessment
  - Risk management and control decisions
  - Vendor oversight
  - Results of testing
  - Security Breaches (If none, document there were none in the minutes)
  - Recommendations for program changes

Third Party Oversight

- Three Reasons for a bank to conduct third party oversight
  - They have access to sensitive customer information (GLBA)
    - Do they have independent security reviews that cover their program to protect sensitive customer information. (SAS-70 or equivalent)
  - Critical to the operation – (Cannot replace them tomorrow)
    - Are they financially viable
    - Do they have adequate business continuity plans that are tested annually.
  - Ensure relationship does not expose the bank to excessive reputational, transactional, credit, legal, liquidity, and compliance risk.

IT Audit

- IT Audit program is weak
  - GLBA requires annually
  - High risk areas not receiving the frequency or depth needed.

Business Continuity Planning

- Plans are out of date/obsolete
- Plans do not cover the entire enterprise
- Plans do not prioritize
- Plans are not tested
- Personnel are not trained

User Access Management

- User Access – Are there periodic reviews of user access on all systems? (It is the bank's responsibility to set user access on serviced systems)

Automated Clearing House (ACH)/Remotely Created Checks (RCC) and Merchant Capture

- ACH, RCC, Merchant Capture
  - Management not conducting initial and ongoing due-diligence including financial and an analysis to ensure the relationship is not introducing excessive credit, legal, liquidity, and reputational risk.
  - Is there a system in place to monitor activity and returns?

Third Party Payment Processor Relationships

Definitions

- **Third Party Payment Processing**
  - Account relationships w/entities that process payments for other businesses.
  - Alternative payment types may include electronic checks created through Remote Deposit Capture or Remotely Created Checks (RCCs) that never existed in paper form.
  - Bank provides channel for clearing and settlement a variety of payment types: ACH, checks, payment cards, etc.
  - Differs from traditional business banking relationships where payment transactions (e.g., ACH, checks, etc.) are made on behalf of the business customer.

Business

- **Businesses Creating Challenges for Third Party Payment Processors:**

  - Coin Dealers
  - Credit Repair Services
  - Dating Services
  - Government Grants
  - *"Get Rich Quick"* type products
  - Home-Based Businesses
  - Membership/Purchasing Clubs
  - Travel Clubs

Recent Cases

- Regulators observing an increase in the number of problem cases involving payment processors
- Most cases involve a failure to conduct appropriate due diligence and monitor transaction activity
- Some cases involve the inappropriate use of "Remotely Created Checks" or "Demand Drafts" that are processed through the check channel with an item that never existed in original paper form
- Payment processors appear to be targeting smaller less sophisticated banks that may be seeking alternative non-interest income streams
- Challenges exist when there is not a direct customer relationship with the originating business

Regulatory Enforcement Actions

- **Federal banking regulators have take a variety of enforcement actions related to illicit payment processor activity including:**
  - Required restitution to customers
  - Civil monetary penalties
  - Cease & Desist Orders
  - Restrictions on Business Activities and
  - Other corrective actions

Avoiding Detection...

- Problem businesses go to great lengths to avoid detection by both banks and the payments processors

- Potential for complacent or collaborating payment processors creates challenges – trust but verify...

- Strategies to avoid detection include:
  - Use of multiple banking relationships
  - Misleading ownership declarations
  - Consolidated return processing
  - Multiple company names/accounts for same entity

Red Flags

- High level of consumer complaints
- High level of returns/charge-backs
- Unverifiable merchant information (e.g., website, business registration, etc.)
- Unexpected volume/value activity or change
- Prior civil, criminal and regulatory actions against processor or its principals
- Law enforcement inquiries

TPPP Risks

- Operational
- Credit
- Compliance
- Transaction
- Legal

TPPP Risks (continued)

- Reputation
  - Customer Complaints
  - Returned Items
  - Harmful/Abusive Consumer Practices
- BSA/AML Compliance

Bank's MINIMUM Responsibilities

- Establish Comprehensive Policies and Procedures
- Review all Contracts with Processors and Sub-Processors
- Establish sound and enforceable contractual requirements for all parties
- Evaluate Due Diligence Performed by Processors on the Merchants They Work With
- Perform In-Depth and/or Enhanced Due Diligence
- Perform Adequate Risk Assessment of Processing Entities
- Perform Ongoing Monitoring
- Establish and Maintain Adequate Reserve Accounts
- Provide Ongoing Training

Third-Party Payment Processors

- Can include:
  - Nested TPPPs / Aggregators
- TPPPs currently have no BSA/AML obligations as established by FinCEN
- TPPPs can be used to facilitate illegal or high-risk activities

Third-Party Payment Processors

- The bank retains ultimate responsibility for all transactions flowing through the bank and must file SARs on unusual or suspicious activities
- As such, the bank must have sufficient understanding of each merchant to identify unusual activity.

Third-Party Payment Processors

- It is not sufficient that the bank rely entirely on TPPP systems for merchant approval and monitoring.
- Cursory merchant reviews without ensuring appropriate ongoing monitoring of the TPPP and transaction activity is inappropriate.
- Any reliance placed on the TPPP for initial or ongoing tasks need to be verified at least periodically by an external or bank audit of TPPP policies, procedures, and processes

FDIC

References and Tools

- FIL-127-2008 "Guidance on Payment Party Relationships"
- FIL-44-2008 "Third–party Risk Guidance for Managing Third Party Risk
- Payment Systems IT Handbook
- BSA/AML Regulations
- FIL-17-2010 "Revised Bank Secrecy Act/Anti-Money Laundering Examination Manual"
- FIL-35-2010: Reg GG "Uniform Internet Gambling Enforcement Act"
- BBB.org
- Complaintsboard.com
- Ripoffreport.com

- Questions?
- FDICSanFrancisco@FDIC.gov