The U.S. Department of Justice and banking regulators have stepped up the pace of criminal, civil and administrative actions against banks, payment processors, money transmitters, and other financial institutions, for violations of the Bank Secrecy Act, including through a DOJ initiative known as "Operation Chokepoint." Criminal charges for failing to maintain an effective Anti-Money Laundering Program, or for failing to file Suspicious Activity Reports, are no longer uncommon when the government believes, sometimes with the benefit of hindsight, that a financial institution missed "red flags" in connection with a customer's account.

In This Presentation:

Discussion Points:
- What is Operation Choke Point?
- Why and for whom is this important?
- What does the government expect?
- What do the critics say?
- What enforcement actions have been brought?
- What steps should banks and processors take?
- Excerpt from What is Operation Choke Point?

- Launched in March 2013 Justice Department's effort to "crack down" on banks and payment processing firms that have relationships with certain "high risk" merchants. Goal: to identify banks that are: – Processing transactions they know are fraudulent; or – Willfully ignoring evidence of fraud. Over the past year, DOJ has issued more than 50 subpoenas to banks and third-party payment processors, 15 pending criminal and civil investigations, 1 major settlement (Four Oaks Bank, although there have been similar settlements prior to the advent of Operation Choke Point.)

Co-Authored by Jonny Frank of the StoneTurn Group. Presentation co-published by The StoneTurn Group.

Please see full presentation below for more information.

Davis Wright Tremaine LLP

StoneTurn Group

OPERATION CHOKE POINT AND THE BRAVE NEW WORLD OF CRIMINAL LIABILITY

Presented by:

Jeffrey B. Coopersmith, Davis Wright Tremaine

Jonny Frank, StoneTurn Group

Discussion Points

- What is Operation Choke Point?
- Why and for whom is this important?
- What does the government expect?
- What do the critics say?
- What enforcement actions have been brought?
- What steps should banks and processors take?

What is Operation Choke Point?

- Launched in March 2013
- Justice Department's effort to "crack down" on banks and payment processing firms that have relationships with certain "high risk" merchants
- **Goal**: to identify banks that are:
  - Processing transactions they know are fraudulent; or
  - Willfully ignoring evidence of fraud

What is Operation Choke Point? (cont'd)

- Over the past year, DOJ has issued more than 50 subpoenas to banks and third-party payment processors
- 15 pending criminal and civil investigations
- 1 major settlement (Four Oaks Bank, although there have been similar settlements prior to the advent of Operation Choke Point

Operation Choke Point's Targets

- Banks
- Third-Party Payment Processors ("TPPPs")
- Merchants
  - "High-risk" merchants like coin dealers, firearm sellers, ammunition sellers, "get rich" schemes

Key Focus: Payday Lending Industry

Potential New Targets?

- Major companies introducing online or mobile wireless payment systems should be aware of potential risks
  - Google Wallet
  - Apple Pay
  - Amazon Payments
  - Android Mobile Payment Systems
- Bank Secrecy Act applies to "money service businesses" in addition to banks
  - This includes "money transmitters": anyone who engages as a business in the transfer of funds
  - Must file SARs, maintain AML program

How Are Banks Reacting?

- Self-disclosing relationships with TPPPs
- Terminating long-term banking relationships with payday lender merchants
  - Ex. Capital One Financial, Fifth Third Bancorp
- Tailoring compliance programs

Not Just the DOJ: Interagency Involvement

- FDIC
- OCC
- Federal Reserve
- FinCEN
- State Regulators, *e.g.*, NY DFS

Interagency Involvement (cont'd)

- Federal Deposit Insurance Corporation (FDIC)
  - In 2011, issued "Managing Risks in Third-Party Payment Processor Relationships"
  - Areas of concern:
    - "High risk" merchants
      - Abusive telemarketers, deceptive online merchants, illegal organizations
      - High interest
    - "High risk" payments
      - Consumer unfamiliar with merchant; uncertainty of quality of goods sold; goods sold over the phone or Internet
      - High rate of returns or "charge backs"
    - "High Risk" payment processor relationships
      - High volume of customer complaints; misleading sales tactics

Interagency Involvement (cont'd)

- Federal Deposit Insurance Corporation (FDIC)
  - Recommended Due Diligence:
    - Monitor Internet for complaints against TPPPs, merchants, banks
    - "Know the customer"
      - Review processor's promotional materials, website, etc.
      - Visit processor's business operations center
    - Maintain ongoing BSA/AML compliance program
      - Develop procedures for monitoring payment processor information
    - File Suspicious Activity Reports ("SARs") when necessary

Interagency Involvement (cont'd)

- Office of the Comptroller of the Currency (OCC)
  - In 2013, issued "Third-Party Relationships: Risk Management Guidance"
  - Effective risk-management includes:
    - Plan outlining bank's strategy for dealing with risks
    - Due diligence when selecting third-parties
    - Written contracts outlining rights and responsibilities of parties
    - Contingency plans for effective termination of relationships
    - Clear roles and responsibilities for overseeing relationship and risk-management process
    - Documentation
    - Independent reviews

Interagency Involvement (cont'd)

- Federal Reserve
  - In late 2013, issued updated "Guidance on Managing Outsourcing Risk"
  - Identifies six "core elements" of an effective risk-management program:
    1. Risk assessments
    2. Due diligence and selection of service providers
    3. Contract provisions and considerations
    4. Incentive compensation review
    5. Oversight and monitoring of service providers
    6. Business continuity and contingency plans

Interagency Involvement (cont'd)

1. Risk assessments
   - Weigh benefits and risks of outsourcing
   - Update frequently
2. Due diligence and selection of service providers
   - Look at business background, reputation, strategy
   - Look at financial performance and conditions
   - Look at operations and internal controls
3. Contract provisions and considerations
   - Clearly define rights and responsibilities

Interagency Involvement (cont'd)

4. Incentive compensation review
   - Inappropriately structured incentives result in reputational damage, increased litigation
   - "Inappropriate": ex. Variable fees encouraging service providers to work with customers with higher profit regardless of suitability
5. Oversight and monitoring of service providers
   - Adjust risk mitigation plans based on the level of risk presented
6. Business continuity and contingency plans
   - Plan for "disaster recovery" plan

- Additional risks:
  - Failure to file SARs
  - Foreign-based service providers

Interagency Involvement (cont'd)

- Financial Crimes Enforcement Network (FinCEN)
  - In 2012, issued "Risk Associated with Third-Party Payment Processors"
  - Identified "red flags" for illicit use of payment processors
    - High number of consumer complaints, high numbers of returns and chargebacks
    - Accounts at multiple financial institutions (especially moving from one financial institution to another in a short time frame)
    - ACH credit transactions originating from foreign sources
    - Telemarketers, online businesses

Interagency Involvement (cont'd)

- Financial Crimes Enforcement Network (FinCEN)
  - Recommended due diligence
    - Update AML programs
    - Check for pending investigations or legal actions against payment processors
    - File SARs if illegal activity suspected

Critics of Operation Choke Point

- **Congress:**
  - May 2014: House Committee on Oversight and Government Reform released highly critical report
    - Operation Choke Point requires banks to serve as **"moral arbiters and policemen of the commercial world"**
  - July 2014: Congressional hearings on Operation Choke Point
  - August 2014: Rep. Blaine Luetkemeyer (MO) introduced bill seeking to put limits on Operation's subpoena power under FIRREA
  - October 2014: Rep. Luetkemeyer leads effort to request internal investigators at DOJ and FDIC to examine Operation Choke Point

Critics of Operation Choke Point (cont'd)

- **Banks and Payment Processors:**
  - Banks argue DOJ placing undue burden, forcing them to adopt role of fraud investigators
  - Investigation forcing banks to terminate long-standing relationships with legal businesses
- **Payday Lenders**
  - Consumer Financial Services Association of America, payday lending industry group, sued Fed, FDIC, OCC to stop participation in Operation Choke Point

DOJ Resistant to Criticisms

- **Attorney General Eric Holder:**
  - "We recognize that most of the businesses that use the banking system are not fraudsters."
  - "In the months ahead, we expect to resolve other investigations involving financial institutions that chose to process transactions even though they knew the transactions were fraudulent, or willfully ignored clear evidence of fraud." (June 23, 2014)

Operation Choke Point in Action

- Four Oaks Bank (North Carolina)
  - DOJ sued Four Oaks in early 2014
  - DOJ found:
    - Bank had earned $850,000 in fees on $2.4 billion in debit transactions by TPPPs
    - These transactions were with "high risk" merchants:
      - Payday lenders, internet gambling operations, online Ponzi scheme
    - Reversal rates of 30-70% (normal = 1.5%)
  - Penalties
    - $1.2 Civil Money Penalty from DOJ
    - $200,000 forfeiture to US Postal Inspection Service
    - Consent Order limiting bank's dealings with TPPPs and certain merchants

What Tools Does the DOJ Have?

- FIRREA Section 951
- 31 U.S.C. § § 5318, 5322
- Mail Fraud (18 U.S.C § 1341)
- Wire Fraud (18 U.S.C § 1343)
- Injunctions (18 U.S.C § 1345)

FIRREA Section 951

- Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA)
  - Enacted in response to savings and loan crisis of late 1980s
- Originally intended to help **defend** banks from fraud by third parties
- Now being used to seek civil penalties **against** banks for failing to identify fraud
- "Affecting Financial Institution" issue

FIRREA Section 951

- Under FIRREA, DOJ can:
  - Issue administrative subpoenas for civil investigations
  - Prove criminal offense (like wire fraud) by preponderance standard
  - Impose civil money penalties
    - $1.1 million per violation
    - If continuing violation, increases to $1.1 million per day or $5.5 million per violation
    - Or, alternatively, fine equal to gain or loss

31 U.S.C. 5318 and 31 U.S.C. 5322

- Bank Secrecy Act and Anti-Money Laundering ("BSA/AML")
- Together, these statutes can impose criminal penalties on banks for **willful** failure to establish effective AML programs or to file SARs
- 31 U.S.C. § 5318:
  - Banks must:
    - Develop internal policies, procedures, and controls
    - Designate compliance officer
    - Establish ongoing employee training program
    - Establish independent audit function to test programs
    - File SARs

Suspicious Activity Reports (SARs)

- "Suspicious"
  - Transaction has no apparent business purpose
  - Transaction is not the type customer is expected to engage in
  - Transaction derived from illegal funds/designed to hide origin of funds
  - Bottom line: largely a judgment call
- Must file within 30 days of detection of activity

Mail and Wire Fraud

- Requires "knowing" participation in scheme to defraud and "intent to defraud"
- DOJ would likely try to prove using "deliberate ignorance" theory (*i.e.*, turning a blind eye)
- Legal issue applicability of "aiding and abetting" concept to deliberate ignorance
- Beyond a reasonable doubt proof in a criminal case, but only preponderance in a FIRREA case

Criminal Remedies

- Penalties for companies:
  - Deferred Prosecution Agreements
  - Fines
  - Probation
  - Restitution
- Penalties for individuals
  - Jail
  - Fines
  - Probation
  - Restitution

INJUNCTIONS UNDER 18 USC 1345

- Injunctions against Fraud
- 2007: DOJ used Section 1345 to go after a third-party payment processor directly
  - Injunction terminating TPPP's operations, imposing receivership over assets, $4 million in restitution to victims, lifetime prohibition against certain types of transactions
- 2014: DOJ seeks injunction in Four Oaks Bank case

Regulatory Remedies—Charter Revocation

- Money-laundering related convictions could trigger hearing on revocation of bank's charter
- Significant risk to banks: loss of customer confidence, revocation of license
- OCC
  - 12 U.S.C. § 93
    - If conviction under Title 18, OCC ***must*** issue notice of intention to terminate all rights and privileged and schedule pretermination hearing
    - If conviction under Title 31, OCC ***may*** issue such notice and schedule such hearing
- Federal Reserve
  - 12 U.S.C. § 327
  - If violation of the Fed's regulations, may compel hearing, require bank to surrender stock, membership rights

Class Actions

- Oct. 2013: Private plaintiffs (payday lending consumers) brought putative class actions against several banks
  - **Four Oaks Bank;** BMO Harris Bank, N.A.; First Primier Bank, Bay Cities Bank, Missouri Bank & Trust, National Bank of California
- Claims:
  - Banks unlawfully engaging in "collection of unlawful debts" under federal RICO statute; knowingly supporting payday lenders
- Plaintiffs seek refund of every ACH debit where defendant banks were the originating depository financial institution (ODFI)

J.P. Morgan Chase and Bernie Madoff

- Massive Ponzi Scheme
  - $10-20 billion stolen
- Bank held Madoff's accounts from 1986-2008
- DOJ's claims against bank included:
  - Failure to establish and maintain AML program
  - Failure to file SARs
- Bank's penalties:
  - Deferred Prosecution Agreement with DOJ, including $1.7 billion forfeiture for restitution
  - $461 million fine by FinCEN
  - $350 civil money penalty by OCC

Banks Penalized for BSA/AML Failures

- CommunityONE Bank, N.A.(North Carolina)
  - Failed to file SARs, failed to maintain adequate BSA/AML programs
    - Merchant engaging in Ponzi scheme with deposits of between $35 million and $40 million
  - Penalties:
    - Deferred Prosecution Agreement with DOJ
    - $400,000 restitution

Banks Penalized for BSA/AML Failures

- Wachovia Bank, N.A. (North Carolina)
  - Failed under BSA to monitor suspicious deposits
    - Ex. Failed to monitor $41 billion in deposits (consisting of 6 million consecutively numbered checks) for foreign accounts
    - Ex. Failure to file 4,300 SARs
  - Penalties:
    - $110 million fine by DOJ and FinCEN
    - Deferred Prosecution Agreement with DOJ
    - $50 million Civil Money Penalty and Cease and Desist Order by OCC

Banks Penalized for BSA/AML Failures

- First Bank of Delaware (Delaware)
  - Repeated failure to implement BSA/AML controls for TPPPs, despite numerous warnings, consent orders, fines.
  - Penalties:
    - $15 million fine by DOJ, FinCEN, FDIC
    - $500,000 restitution
  - Lasting impact on bank:
    - Sold its assets, lost its charter and FDIC insurance, ultimately closed.

Banks Penalized for BSA/AML Failures

- Saddle River Valley Bank (New Jersey)
  - BSA/AML Violations
    - Executed $1.5 billion for Mexican and Dominican casas de cambio (suspected laundering of drug money)
    - Failed to properly file SARs
  - Penalties:
    - $4.1 million Civil Money Penalty by DOJ, FinCEN, and OCC (concurrently)
  - Lasting impact on bank:
    - Ceased operations and relocated after fines exhausted all of the bank's assets

Banks Penalized for BSA/AML Failures

- BankAtlantic (Florida)
  - Failed to maintain proper BSA and AML compliance policies
    - Ex. Failed to monitor high-risk, high-volume international wire transfers
  - Penalties:
    - Deferred Prosecution Agreement with DOJ
    - $10 million Civil Money Penalty by FinCEN
    - $10 million Civil Money Penalty by Office of Thrift Supervision (OTS)

Mitigating Risk: Pre-Incident

- Conduct risk assessment
- Leverage compliance analytics
  - Link risks to “red flags”
  - Develop data based smoke detectors
- Test entity and transaction level controls
- Document, document, document

Mitigating Risk: Post-Incident Remediation

- Timeliness – “will remediate” vs. “have already corrected”
- Root cause analysis
- Forensic analytics and audit procedures to identify other misconduct
- Enhance entity and transaction level controls and compliance analytics
- Periodic, third-party audits or reviews

Contact

Jeffrey B. Coopersmith
Partner
Davis Wright Tremaine LLP
jeffcoopersmith@dwt.com
206.757.8020 direct
206.708.9396 mobile

Jonny Frank
Partner
StoneTurn Group
jfrank@stoneturn.com
212.430.3434 direct