Bank Secrecy Act Hot Topics
October 24, 2017

David A. Larocque, CAMS
Regulatory Compliance Manager
About Wolf & Company, P.C.

- Established in 1911
- Offer Audit, Tax, and Risk Management services to over 320 financial institutions
- Offices located in:
  - Boston, Massachusetts
  - Springfield, Massachusetts
  - Albany, New York
  - Livingston, NJ
- Over 200 professionals

As a leading regional firm founded in 1911, we provide our clients with specialized industry expertise and responsive service.
Have Marketing Update, if needed

Shea, Brian M., 6/2/2017
Financial Institution Expertise

- Over 80 Risk Management Professionals:
  - Regulatory Compliance Services Group
  - IT Assurance Services Group
  - Internal Audit Services Group
  - WolfPAC® Solutions Group

- Provide services to over 320 financial institutions:
  - Approximately 90 FIs with assets > $1B
  - Approximately 25 publicly traded FIs
  - Constant regulatory review of our deliverables

- Provide Risk Management Services in 27 states and 2 U.S. territories
SBM3  Have Marketing Update
Shea, Brian M., 6/2/2017
Today’s Agenda

• Recent Regulatory News
• High Risk Customer Reviews
• BSA Beneficial Ownership Final Rule
• Third Party Payment Processors
• Marijuana-Related Businesses
• Human Trafficking
• BSA Reasonableness
• OFAC Verification Thresholds
• Recent BSA Actions/Penalties
Recent Regulatory News

• February 24, 2017
  – BSA/AML Self-Assessment Tool Released
    • https://www.csbs.org/regulatory/resources/Pages/JobAids.aspx

• OCC criticism regarding Enhanced Due Diligence Monitoring

• FFIEC BSA Exam Manual Updates
High Risk Customer Reviews
High Risk Customer Reviews

Examiners are concerned about inadequate detail regarding high risk customer relationships

The cause appears to be that management is relying on their working knowledge of customer relationships in lieu of detailed analysis and documentation of enhanced due diligence reviews

The recommended corrective action is to develop EDD for higher risk customers that provides analysis and documentation of items detailed in the FFIEC BSA/AML Examination Manual
High Risk Customer Reviews

- Higher risk entities require closer monitoring
- No defined frequency or exact rules, but in a perfect world
  - High Risk: Quarterly
  - Moderate/Medium Risk: Semi-Annually
  - Low Risk: Annually
- Reviews must be documented in great detail
- Accompanying processes must be documented in policies and procedures
BSA Beneficial Ownership Final Rule

FinCEN
KEEP CALM AND CARRY ON WITH CDD
Effective Date – July 11, 2016
Mandatory Compliance Date – May 11, 2018
Mandatory requirement for financial institutions to know the identity of individuals who own or control a legal entity customer

- Each individual who directly or indirectly owns 25% or more of the equity interests of a legal entity customer
- A single individual who has significant responsibility to control, manage or direct a legal entity customer

Model certification form to be used at account opening – not mandatory
Prior to the rule, there was no mandatory requirement for financial institutions to know the identity of individuals who own or control a legal entity customer.

The rule is also intended to:

- Provide information that will assist law enforcement in financial investigations
- Help prevent evasion of sanctions programs
- Improve the ability of financial institutions to assess risk
- Facilitate tax compliance, and
- Advance U.S. compliance with international standards and commitments
• Beneficial ownership identification and verification
  – Added by the new CDD rule
  – Will assist the institution to understand the nature and purpose of customer relationships to develop a customer risk profile
• Requires ongoing monitoring for reporting suspicious transactions and, on a risk basis, maintaining and updating customer information
What is a Legal Entity Customer?

- A Corporation
- A Limited Liability Company (LLC)
- Other Entity created by filing a public document with the Secretary of State
- A General Partnership
- Any similar entity formed under the laws of a foreign jurisdiction
What is NOT a Legal Entity Customer?

- A financial institution regulated by a federal functional regulator or a bank regulated by a state bank regulator
- A department or agency of the United States, a State or the political subdivision of a State
- An entity established under the laws of the United States, a State or the political subdivision of a State that exercises governmental authority
- An entity other than a bank whose stock is listed on a national exchange or a subsidiary of that entity if the listed entity owns at least 51% of the equity of the subsidiary
Other entities not covered by the CDD requirement:

- An issuer of certain securities registered with the SEC
- An investment company
- An investment adviser
- An exchange or clearing agency
- Any other entity registered with the SEC

- Certain entities registered with the CFTC
- A public accounting firm registered under Sarbanes-Oxley
- A bank holding company
- A pooled investment vehicle
- A state-regulated insurance company
- A foreign financial institution
Third Party Payment Processors
Third Party Payment Processors

What are Third Party Payment Processors?

• Subset of a Third Party Service Providers (TPSP)
  – Provide services on behalf of other entities
  – Non-Bank entities
• Processors specifically provide payment processing services to merchants/other parties
  – Transactions tend to be in format of Automated Clearing House (ACH) and International Automated Clearing House (IAT) transactions, Remotely Created Checks (RCC), and debit/credit card transactions
Third Party Payment Processors

- 2Checkout
- Airpay
- Authorize.net
- Beanstream
- BitPay
- Braintree
- Cardstream
- CashEnvoy
- Conekta
- CyberSource
- DataCash
- DirecPay
- Doku
- Dwolla
- E-xact
- Elavon MyVirtualMerchant
- ePay
- PayPal
What are the BSA/AML/OFAC Risks?

- Entity may not be subject to BSA/AML/OFAC and Regulation GG
- Risk Comprised of TPPP’s Customer Base
- Potential for High Transaction Volume spanning geographies
- Multiple Layers of Related Parties
- Multiple Senders/Obscured Identities
- Anonymity
- Reliance
Third Party Payment Processors

What Are Regulatory Expectations?

• Recent exams have revealed a renewed interest in Third Party Payment Processor Due Diligence
• Institutions have a method to identify Third Party Payment Processors at or soon after account opening
• Institutions have a method to identify Third Party Payment Processing Activity within the existing database
• Institutions that decide to Bank Third Party Payment Processors perform sufficient due diligence
What are Regulatory Expectations?

- Institutions have policies, procedures, and processes in place to assess risk:
  - Compliance
  - Fraud
  - Safety & Soundness
  - BSA/AML/OFAC

- Institutions have methods to detect and report Suspicious Activity
Effective Detection – Common Practices

• Asking at Account Opening
• Regular Transaction Monitoring of ACH/IAT activity
  – Higher than Expected ACH/IAT activity
  – Washing of ACH Transactions

• What should a Bank consider in the potential onboarding of such customers?
  – What is the Bank’s Risk Tolerance?
  – Does the Bank have the resources to uphold monitoring expectations?
Onboarding Due Diligence - Common Practices

- Background Check
- Promotional Materials
- Processors policies and procedures
- Relationship to additional third parties
- Have Processor Identify Major Customers
- View Public Information on owners and businesses
- Perform a Site Visit
Third Party Payment Processors

Transactional Due Diligence and Monitoring - Common Practices

• Monitoring of Regular ACH/IAT transactions
• Monitor transactional suspicious activity alerts/suspicious activity reports
• Monitoring of Regularly Credit Card, Debit Card Transactions, and RCC Transactions
• Do the transactions make sense?

Any deviations should warrant additional due diligence, investigation, and documentation.
Third Party Payment Processors

Periodic Due Diligence - Common Practices

• Objectives of Periodic Due Diligence
• What Should Be Assessed?
  – Merchant Base
  – Merchant Activities
  – Average volumes
  – “Swiping” versus “keying” for credit card transactions
  – Chargeback History
  – Consumer Complaints and Negative News Reports
  – Suspicious Activity Alerts or Notations from Bank’s overall suspicious activity monitoring
Marijuana-Related Businesses

- 29 states have legalized medical marijuana in some form, 8 of which have also legalized marijuana for recreational use
- No further guidance provided since FinCEN February 2014 guidance
- Current bills in various stages of development
  - Several marijuana banking bills since 2015
  - Secure and Fair Enforcement (SAFE) Banking Act of 2017
  - Marijuana Policy Gap Act
  - Marijuana Revenue and Regulation Act
Marijuana-Related Businesses

Recommended due diligence:

• Verifying with state authorities that the business is duly licensed and registered

• Reviewing the license application and related documentation

• Requesting available information about the business and related parties from state licensing and enforcement authorities
Marijuana-Related Businesses

Recommended Due Diligence

• Developing an understanding of the normal and expected activity for the business, including types of product to be sold and customers to be served

• Ongoing monitoring of public sources for possible adverse information about the business and related parties

• Refreshing information about the business on a periodic basis
Human Trafficking

Human Trafficking
A Global Problem
What is Human Trafficking?

• The act of recruiting, harboring, transporting, providing or obtaining a person for forced labor or commercial sex acts through the use of force, fraud or coercion.

• Involves the use of force or coercion and the exploitation of victims.

• Includes, but is not limited to, involuntary servitude, forced labor, debt bondage and sexual exploitation.
Human Trafficking

What is Human Trafficking?

• Anyone can be a victim regardless of origin, sex, age or legal status.

• There is no need for a person to cross a border to be trafficked; individuals can be trafficked within the borders of a country.
Potential Red Flags

- A business customer does not exhibit normal payroll expenditures (e.g., wages, payroll taxes, social security contributions)

- Substantial deductions to wages. To the extent a financial institution is able to observe, a customer with a business may deduct large amounts from the wages of its employees alleging extensive charges (e.g., housing and food costs), where the employees only receive a small fraction of their wages; this may occur before or after the payment of wages.

- Cashing of payroll checks where the majority of the funds are kept by the employer or are deposited back into the employer’s account. This activity may be detected by those financial institutions that have access to paystubs and other payroll records.
Human Trafficking

Potential Red Flags

• Transactional activity (credits and/or debits) inconsistent with a customer’s alleged employment, business or expected activity, or where transactions lack a business or apparent lawful purpose.

• Cash deposits or wire transfers are kept below $3,000 or $10,000 in apparent efforts to avoid record keeping requirements or the filing of Currency Transaction Reports (CTRs), respectively.

• Frequent outbound wire transfers, with no business or apparent lawful purpose, directed to countries at higher risk for human trafficking or to countries that are inconsistent with the customer’s expected activity.
Potential Red Flags

• A customer’s account appears to function as a funnel account, where cash deposits occur in cities/states where the customer does not reside or conduct business. Frequently, in the case of funnel accounts, the funds are quickly withdrawn (same day) after the deposits are made.

• Frequent transactions, inconsistent with expected activity and/or line of business, carried out by a business customer in apparent efforts to provide sustenance to individuals (e.g., payment for housing, lodging, regular vehicle rentals, purchases of large amounts of food).

• Payments to employment or student recruitment agencies that are not licensed/registered or that have labor violations.
Human Trafficking

Potential Red Flags

- A customer establishes an account or visits a branch to conduct transactions while always escorted by a third party (e.g., under the pretext of requiring an interpreter). Correspondingly, the third party escorting the customer may always have possession of the customer’s ID.

- Inflows are largely received in cash where substantial cash receipts are inconsistent with the customer’s line of business. Extensive use of cash to purchase assets and to conduct transactions.
Human Trafficking

What can Institutions do?

• Train front-line employees to identify potential red flags
• Update policies and procedures
• Share information under Section 314(b)
• File SARs for any potential human trafficking activity
  – Within the narrative, include “ADVISORY HUMAN TRAFFICKING” to assist law enforcement
BSA Reasonableness
Why is BSA Reasonableness so important?

• Migration to use of automated software by Banks and Credit Unions

• FFIEC BSA Examination Manual includes the following:
  – Periodic testing and focus of testing
    • Ongoing testing
  – Documented reasoning and determination of effectiveness
  – Adherence to policies and procedures
BSA Reasonableness

• Insufficient Monitoring
  – Suspicious activity monitoring does not adequately cover certain transaction, customer and/or account types
  – Keyword searches do not cover all recommended activities

• Missing/Insufficient Risk Ratings
  – Account types
  – Transaction types
  – Business/Industry types
  – Zip codes
BSA Reasonableness

• Insufficient Documentation
  – Methodology used to develop parameters
  – Methodology and reasoning for changes to parameters
  – Policies and procedures
BSA Reasonableness

- Insufficient Processes
  - Change management
  - Periodic review to ensure parameters remain effective and reasonable
  - Use or creation of new parameters
- Insufficient Training
  - Lack of understanding of system capabilities
OFAC Verification Thresholds

Office of Foreign Assets Control
OFAC Verification Thresholds

• OFAC has a zero tolerance for performing verification on non-customer entities

• Non-performance of OFAC on certain transactions or use of thresholds
  – Institution discretion

• These decisions must be documented
  – Analysis to support these decisions
  – Documentation in OFAC Risk Assessment/Board Approved Policy

• Board Notification
Recent examples against financial institutions include:

**December 2016** – Bethex Federal Credit Union, Bronx, NY - $500,000 penalty from FinCEN

**January 2017** – Western Union Financial Services, Inc. - $184 million penalty from FinCEN

**February 2017** – Merchants Bank, Carson, CA - $7 million penalty from FinCEN and $1 million penalty from the OCC
Helpful Links

FinCEN Website
http://www.fincen.gov/

OFAC Website
http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx

Official BSA Examination Manual
Thank You

David A. Larocque, CAMS
Regulatory Compliance Manager
617-933-3354
dlaroncque@wolfandco.com
http://www.wolfandco.com