

The Regulatory Environment for Remittances



Federal Reserve Bank of San Francisco

Objectives

- Discuss primary anti-money laundering laws: BSA and USA PATRIOT Act
- Review bank requirements
- Discuss other compliance issues
 - FinCEN, OFAC, CRA

Conclusions

- Remittances present a strong market opportunity for banks, and serve the banking needs of a growing immigrant population.
- Offering remittances will change the bank's compliance risk profile, and compliance systems, policies, procedures, and training should reflect the change.
- Work with your regulator to ensure a smooth transition to any new products or compliance procedures.

Regulatory Environment

- USA PATRIOT Act: October 26, 2001
- “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism”
- Title III: International Money Laundering Abatement and Anti-Terrorism Act of 2001
- Generally, amends the Bank Secrecy Act
- The BSA is administered by the U.S. Treasury Department

Key PATRIOT Act Provisions

- 311: Special measures
- 312: Enhanced Due Diligence
- 313: Prohibition of Shell Bank Accounts
- 314: Information Sharing
- 319: Availability Of Records
- 326: Customer Identification

Section 326: Customer ID

- Requires that financial institutions have a Customer Identification Program (CIP). The CIP:
 - Outlines procedures to verify identity of customers opening accounts
 - Must be in writing; approved by board of directors
 - Must be incorporated into existing AML/BSA compliance program

Section 326: Customer ID

CIP must include risk-based procedures to account for risks represented by:

- Types of accounts offered
- Methods of opening accounts
- Type of identification available
- Bank's size and location
- Customer base

CIP General Requirements

- Obtain minimum required information and verify identity of person opening an account; bank must form reasonable belief that it knows the true identity of the customer.
- Maintain record of information used to verify customer's identity.
- Determine whether customer appears on any list of known/suspected terrorists or terrorist organizations provided to the financial institution by any government agency.

CIP Information Required

- Minimum customer information required prior to opening account:
 - name
 - street address
 - identification number
 - for individuals, date of birth

CIP: Identification Number

- U.S. Person

- SSN or taxpayer identification number

- Non-U.S. Person

One or more of following:

- Taxpayer identification number
- Passport number and country of issuance
- Alien ID card number
- Number and country of issuance of other government document showing nationality or residence and bearing photograph

Matricula Consular

- Issued by Mexican consulate since 1871
- Official record for Mexican individuals living abroad
- Over 4 million issued
- Accepted by states, cities, police departments and banks nationwide
- Enhanced security features
- Matricula is allowed under Section 326 of USA PATRIOT Act

CIP: Verification of Identification Information

- CIP should include risk-based procedures for verifying identification information within a reasonable amount of time.
- Verification procedures should be sufficient to allow bank to form reasonable belief of customer's true identity.
- Procedures should focus on verifying information contained in identification used; not on verifying the veracity of each individual type of identification.

OFAC Known/Suspected Terrorist List

- OFAC enforces sanctions programs against countries, groups, and individuals.
- CIP must include procedures for determining if customer is on any list of known/suspected terrorists or terrorist organizations (i.e. OFAC list).
- Must check both purchaser AND beneficiary of remittance against OFAC list.

OFAC Program

- OFAC program should be commensurate with F.I.'s OFAC risk profile.
- Risk profile should reflect products and services offered, customers, and geographic location.
- OFAC program should:
 - identify high-risk areas for OFAC purposes
 - provide appropriate internal controls for screening and reporting
 - address compliance
 - include training for all bank personnel

OFAC program cont'd

- All new accounts must be checked against OFAC during account opening process (as part of CIP).
- Existing accounts should be reviewed regularly.
- Specific types of transactions should be checked against OFAC list prior to execution (e.g. fund transfers or noncustomer transactions).
- Bank policy should address OFAC screening process and how bank will determine if initial OFAC "hit" is valid match or false hit.
- Screening process and filtering criteria should reflect F.I.'s overall OFAC risk level.

OFAC Notifications

- If individual covered, F.I. must “block” or “freeze” an already established account and notify OFAC.
- If it’s a new account, F.I. must “reject” the transaction and notify OFAC.
- Checking at the time of a “Hit”
 - Call: 1-800-540-OFAC (6322)
 - Do appropriate due diligence first to eliminate false positives
- If a true “Hit,” F.I. must report transaction to OFAC in writing within 10 business days and include backup documentation.

Community Reinvestment Act

- The regulators have interpreted the CRA to permit favorable consideration of remittance products developed to serve LMI communities and increase access to financial products and services for LMI persons.

For More Information

- BSA resources and exam procedures:
www.ffiec.gov/bsa_aml_infobase/default.htm
- OFAC:
www.ustreas.gov/offices/enforcement/ofac/
- FinCEN:
www.fincen.gov
- CRA consideration:
www.ffiec.gov/cra/pdf/060304remittances.pdf