The Bank Secrecy Act (BSA) was created in 1970 to assist in criminal, tax, and regulatory investigations.

The Financial Crimes Enforcement Network (FinCEN) is responsible for compliance.

The BSA Program and policies are mandated by statute.

BSA compliance is required for all financial institutions, including banks.
The Bank Secrecy Act applies to:

- Banks;
- Money Services Businesses (includes check cashers and money transmitters);
- Securities and commodities firms (brokers/dealers, mutual funds, commodities traders);
- Casinos and card clubs;
- Insurance companies;
- Precious metals dealers; and
- Loan or finance companies and pawnbrokers.
Bank Secrecy Act Program

Regulatory requirements for a BSA Program include the following components:

- System of Internal Controls;
- Independent Review;
- BSA Officer;
- Training; and
- Customer Identification Program.
Components of a BSA Program

- **System of Internal Controls**
  - Includes policies, procedures, and processes to manage, monitor, and control risks;
  - Ensures compliance with BSA regulations;
  - Establishes controls commensurate with BSA risk profile; and
  - Includes recordkeeping and reporting requirements.
Components of a BSA Program

- **Independent Review**
  - Must be completed by a qualified party;
  - Must be independent (in-house or external);
  - Should be conducted every 12 to 18 months, depending on risk profile; and
  - Can be a risk-based process.
Components of a BSA Program

- Bank Secrecy Act Officer
  - Must be designated by the Board of Directors;
  - Must be qualified;
  - Must have sufficient authority, knowledge, and resources; and
  - Is responsible for ensuring overall BSA compliance.
Components of a BSA Program

- **Training**
  A training program must be documented and should:
  - Be tailored to specific job duties;
  - Address regulatory requirements;
  - Reference bank policies, procedures, and processes;
  - Be performed on an ongoing basis; and
  - Reiterate employee responsibilities.
Components of a BSA Program

- **Customer Identification Program**
  - Must form a reasonable belief of customer identity;
  - Must include account opening procedures and verification methods;
  - Must ensure collection of minimum data elements; and
  - May use risk-based procedures for additional documentation and verification of customer identity.
Requirements of the BSA include:

- Recordkeeping;
- BSA Reporting; and
- Suspicious Activity Monitoring.
Reporting requirements to the Financial Crimes Enforcement Network (FinCEN) include:

- Currency Transaction Reports (CTRs);
- Designations of Exempt Persons (for CTR filings only); and
- Suspicious Activity Reports (SARs).

Records must be maintained for 5 years:

- Transaction data – 5 years from transaction; and
- Customer identification data – 5 years from account closure.
Currency Transaction Reports (CTRs)

CTR Filing Requirements:

- CTRs must be filed for currency (cash or coin) transactions over $10,000 conducted by, or on behalf of, one person.
- CTRs must be filed for multiple currency transactions that aggregate over $10,000 in a single day.
- Banks must obtain personal identification information about the individual conducting the transaction such as a Social Security number as well as a driver’s license or other government issued document.
CTR Filing Exemptions

Requirements for Filing Exemptions:

• The BSA establishes various exemptions from reporting currency transactions conducted by banks, governmental departments or agencies, and listed public companies and their subsidiaries.

• Banks may exempt an otherwise eligible non-listed business customer or payroll customer after the customer has conducted five or more reportable transactions.
Suspicious Activity Reports (SARs)

- SARs must be filed for the following transactions:
  - Those involving insider abuse in any amount; aggregating $5,000 or more when a suspect can be identified; and aggregating $25,000 or more regardless of a potential suspect.
  - Those aggregating $5,000 or more, if the bank knows, suspects, or has reason to suspect the transaction may involve potential money laundering or other illegal activity; may be designed to evade the BSA; or has no business or apparent lawful purpose or is not the type of activity a customer would normally conduct.
Reporting requirements to the Financial Crimes Enforcement Network (FinCEN) include:

- Currency Transaction Reports (CTRs);
- Designation of Exempt Persons (for CTR filings only); and
- Suspicious Activity Reports (SARs).

Records must be maintained for 5 years:

- Transaction data – 5 years from transaction; and
- Customer identification data – 5 years from account closure.
Suspicious Activity Monitoring

- Monitoring, identifying, and reporting unusual or suspicious activity are regulatory requirements and form the cornerstone of BSA reporting.
- SARs are filed for unusual or suspicious activity, including, but not limited to, terrorist financing, tax evasion, fraud, and structuring.
- Banks are not investigating, or “confirming” underlying crime.
- Board of Directors should regularly review overall SAR activity.
- Your SAR may link activity to SARs filed by others.
Policies should outline how the bank will address recurring SAR filings, escalation procedures, and account closure.

When activity is unusual and the need is immediate, contact local law enforcement before filing the SAR.
An effective BSA program also includes:

- BSA/AML Risk Assessment;
- Customer Due Diligence; and
- Enhanced Due Diligence.
Risk Assessments

- Risk assessments are the foundation of a BSA/AML Program.
- **Purpose:** Identify the BSA/AML risk profile and use the results to apply appropriate controls to mitigate risk.
- **Steps:**
  - Identify specific risk categories, such as: customers, products, services, and geographies.
  - Quantify the specific risk categories.
Customer Due Diligence and Enhanced Due Diligence

- Due diligence concept is a basic tenet of BSA;

- Provides information to assess baseline risks and form expectations of future transactions; and

- Establishes baseline information essential to effectively identify and report unusual or suspicious activity.
Office of Foreign Assets Control (OFAC)

An Office of the Treasury that administers and enforces economic and trade sanctions based on U.S. foreign policy objectives and national security goals against targeted:

- Foreign countries and regimes;
- Individuals;
- Entities; and
- Practices.

Applies to all U.S. persons (individuals and entities).
The sanctions programs administered by OFAC require transactions, accounts and/or other property to be blocked or rejected, depending on the specific program requirements.

OFAC can assess Civil Money Penalties (CMPs) for processing or engaging in an apparent violation of a U.S. sanctions program.
Office of Foreign Assets Control (OFAC)

- OFAC operates under a clause of strict liability.
- If a sanctioned transaction is processed, there is a violation of law.
- When determining whether a CMP is appropriate, or in calculating the CMP amount, OFAC reviews the existence, nature, and adequacy of the bank’s OFAC compliance program, including the views of the institution’s regulator.
A financial institution OFAC program should:

- Identify high-risk business areas and potential sanctions exposure;
- Provide for appropriate internal controls for screening, reporting, recordkeeping, due diligence, and updating;
- Establish independent testing/audits for compliance;
- Designate a bank employee for OFAC compliance; and
- Create and implement training programs.
Banks should compare and/or review their products and services (accounts, wire transfers, etc.) with OFAC lists and/or broader prohibitions outlined in country-based sanctions.

Frequency for reviewing OFAC lists should be commensurate with:

- Timing and frequency of OFAC list updates; and
- Risk of bank product, service, geography, and customer base.
Emerging Issues and Trends

- Be aware of the BSA risks of new products and services such as:
  - Third-Party Payment Processors;
  - Remote Deposit Capture; and
  - Stored Value Card Relationships.
TPPP Characteristics:

- May serve international and higher-risk businesses;
- Are typically not subject to BSA/AML requirements; and
- May expose the bank to illicit transactions and money laundering or fraud risks.
Remote Deposit Capture

Remote Deposit Capture Characteristics:

- Establishes a method to deposit checks by scanning and transmitting its digital images; and
- Can expose the bank to increased risks of money laundering, fraud, and compromised data transmissions.
Stored Value Card Relationships

- Stored Value Card Characteristics:
  - Have varied risk profiles depending on the characteristics of the card;
  - May pose a money laundering risk to the institution, particularly cards lacking dollar limits or reloading restrictions; and
  - Pose various levels of risk based on the bank’s role in the relationship (such as issuer, intermediary, marketer, or distributor).
Enforcement Actions

- **Enforcement Actions can be issued for BSA/AML and OFAC program deficiencies.**
  - Formal enforcement actions for BSA are mandated when:
    - entire program is deficient, or
    - repeat problems indicate management has failed to take corrective action in a timely and cohesive manner.
  - Depending on the nature and duration of deficiencies, the bank may be subject to Civil Money Penalties.
Resources

- [www.fdic.gov](http://www.fdic.gov)
  - FFIEC BSA/AML Examination Manual
  - FDIC Rules and Regulations, Section 326.8 - BSA
  - FDIC Rules and Regulations, Part 353 - SARs
  - July 19, 2007 Interagency Statement on Enforcement of BSA/AML Requirements

- [www.fincen.gov](http://www.fincen.gov)
- [www.treasury.gov/ofac](http://www.treasury.gov/ofac)
- Directors’ Resource Center: [www.fdic.gov/resourcecenter](http://www.fdic.gov/resourcecenter)
- Mailbox: [supervision@fdic.gov](mailto:supervision@fdic.gov)
Key Presentation Concepts include:

- Applicability of BSA/AML requirements to your bank;
- Components of a strong and effective BSA/AML program;
- BSA recordkeeping and reporting requirements;
- Processes for monitoring, identifying, investigating and reporting unusual or suspicious activity;
Key Presentation Concepts (continued):

- Importance of understanding the risk profile of your bank in order to develop appropriate policies and procedures;
- Application of appropriate customer due diligence to customer activity; and
- Understanding the risks and controls necessary for OFAC compliance.