Bank Secrecy Act Training For Volunteers

Presented By: Utah's Credit Unions

Agenda

- Purpose and Background
- Latest Developments
- Penalties for Non-Compliance
- Board of Director Responsibilities
- Your Bank Secrecy Act (BSA) Program
- Suspicious Activity Reporting
- Office of Foreign Assets Control

PURPOSE AND BACKGROUND
Purpose

• To identify the source, volume and movement of currency and monetary instruments among US financial institutions
• To aid in the investigation of money laundering, tax evasion, international terrorism and other criminal activity

Background

<table>
<thead>
<tr>
<th>YEAR</th>
<th>LAW</th>
<th>PURPOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1970</td>
<td>Bank Secrecy Act</td>
<td>Recordkeeping • Currency Transaction Reports</td>
</tr>
<tr>
<td>1986</td>
<td>Money Laundering Control Act</td>
<td>Money Laundering made a crime • Prohibited structuring transactions to evade BSA • Procedures to comply with BSA</td>
</tr>
<tr>
<td>1988</td>
<td>Anti-Drug Abuse Act</td>
<td>Records of purchase of monetary instruments</td>
</tr>
<tr>
<td>1992</td>
<td>Annunzio-Wylie Anti-Money Laundering Act</td>
<td>Suspicious Activity Reports • Recordkeeping for wire transfers</td>
</tr>
<tr>
<td>2001</td>
<td>USA Patriot Act</td>
<td>Criminalized the financing of terrorism • Enhanced Due Diligence Procedures • Information Sharing • Enhanced BSA Program Requirements • Customer Identification Programs</td>
</tr>
</tbody>
</table>

LATEST DEVELOPMENTS
Final FinCEN Customer Due Diligence (CDD) rules

- Meant to enhance customer due diligence requirements
- Adds a fifth major requirement to Anti-Money Laundering (AML) programs
- Contains explicit CDD requirements
- New requirement to identify beneficial owners of legal entity customers
- Compliance with new rules mandatory on May 11, 2018.
- Credit unions can opt to comply early.

Advisory on Cyber-Events and Cyber-Enabled Crime

Through this advisory FinCEN advises financial institutions on:

- Reporting cyber-enabled crime and cyber-events through Suspicious Activity Reports (SARs)
- Including relevant and available cyber-related information (e.g., Internet Protocol (IP) addresses, account numbers, next-of-kin, email, and telephone numbers)
- Collaborating between BSA/FinCEN and cybersecurity units to identify suspicious activity
- Sharing information, including cyber-related information, among financial institutions to guard against and report money laundering, terrorism financing, and cyber-enabled crime (must be a registered 314b sharer)

PENALTIES FOR NON-COMPLIANCE
Penalties

For the Credit Union
- Cease and desist order
- Loss of charter
- Civil and Criminal money penalties

Penalties

For Individuals
- Removal and bar from banking
- Civil and criminal money penalties
- Prison time

Case Study

- Charles Sanders
- Former chief compliance officer for Gibraltar Private Bank and Trust Company
- Failed to timely file suspicious activity reports on a set of accounts for a customer who was later convicted of crimes related to an illegal Ponzi scheme.
- The bank's BSA officer investigated the suspicious accounts and reported them—but Mr. Sanders did not file the SARs in a timely manner.
- $2,500 civil money penalty (CMP) on March 15, 2016
- Ordered to share a copy of the Consent Order with the Board of Directors of any financial institution with which he becomes affiliated in the future.
- Respondent violated a law or regulation and engaged in reckless or careless conduct, which he knew, or should have known, constituted an 18 U.S.C. § 1956 standard for money laundering, or that the violations or practices were part of a pattern of misconduct that caused more than a minimal loss to the bank.
- Respondent's conduct resulted in a material loss to the bank and was not caused by, or resulting from, any negligence or carelessness.
- Respondent's conduct also involved a reckless disregard for the safety and soundness of the bank, and involved a reckless disregard for the law or applicable regulations.
Case Study

- Bethex Federal Credit Union, Bronx, NY
- $12 Million in assets
- Low-income designated, community development CU.
- Systemic BSA deficiencies since 2011 (cited in 13 examinations), including issues with:
  - Training
  - Customer Identification Program
  - Recordkeeping
  - Designating an appropriately competent BSA officer
- $500,000 civil money penalty levied on December 15, 2016
- Takeaways:
  - Began providing banking services to a large number of wholesale, commercial money service businesses (MSBs) outside New York.
  - Did not take steps to update AML program
  - Relied on a third party to conduct due diligence and suspicious activity monitoring without appropriate verification or inspections
  - BSA program deficiencies contributed in part to its conservatorship and eventual liquidation

Board of Director Responsibilities

“While the board of directors may not require the same degree of training as banking operations personnel, they need to understand the importance of BSA/AML regulatory requirements, the ramifications of non compliance, and the risk posed to the credit union.”

- FFIEC BSA/AML Manual

BOARD OF DIRECTORS RESPONSIBILITIES
Board Responsibilities

• Approve the BSA Program annually
• Appoint a BSA Officer
• Review the BSA Risk Assessment as applicable
• Review periodic BSA program updates
• Ensure BSA officer has adequate staffing and resources
• Review reports of filed Suspicious Activity Reports
• Champion policy and procedure

YOUR BSA COMPLIANCE PROGRAM

Risk Assessment First

• Risk assessment not required
• Examiners will complete one if the credit union does not
• Tell your own story
• BSA program should be based on the risk assessment
Risk Assessment Considerations

The risk assessment should answer the following questions:
• What types of products and services does the credit union offer?
• Who is using them?
• Where is the potential exposure to money laundering?
• What steps have been taken to mitigate risk?

Four Five Main BSA Program Requirements

1. Independent testing of BSA compliance.
2. A specifically designated person or persons responsible for managing BSA compliance (BSA compliance officer)
3. Training for appropriate personnel
4. A system of internal controls to ensure ongoing compliance
5. Appropriate risk-based procedures for conducting ongoing CDD to understand the nature and purpose of customer relationships and to conduct ongoing monitoring to identify and report suspicious transactions, and, on a risk basis, to maintain and update customer information (Added as of May 11, 2018)

Independent Testing

- Qualified
- Independent
- Transaction Testing
- Comprehensive work papers
BSA Officer

- Authority
- Adequate Staffing
- Other Resources
- Training

Training

- New employees upon hire
- All employees periodically (annually)
- Tailored to specific business lines
- Cover employee accountability for compliance
- Credit union should maintain training records and materials
- Coverage of credit union policies, procedures, processes, and new rules and regulations
- Coverage of different forms of money laundering and terrorist financing
- Penalties for noncompliance with internal policies and regulatory requirements

Internal Controls

Minimum Requirements

- Customer/Member Identification Procedures
- Customer/Member Due Diligence
- Suspicious Activity Reporting
- Currency Transaction Reporting
- CTR Exemptions
- Information Sharing under the USA Patriot Act
- Monetary Instrument Recordkeeping
- Funds Transfer Recordkeeping
- Office of Foreign Assets Control (Can be a separate policy)
- Program Continuity
Expanded Internal Controls

- Third Party Payment Processing
- Foreign accounts/branches/services
- Correspondent Accounts
- Brokered Deposits
- Non-Deposit Investment Products
- Insurance
- Private Banking

Customer Identification Procedures

- Based on risk
- Each institution sets their own identification parameters
- Approved by the board as part of BSA Program

Customer Identification Program

The Customer Identification Program (CIP) contains procedures to:
- Verify the identity of any person seeking to open an account
- Maintain records of the information used to verify a person’s identity
- Determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations
SUSPICIOUS ACTIVITY REPORTING

Suspicious Activity Reports
Credit unions are required to file a Suspicious Activity Report (SAR) if the institution knows or suspects that a transaction:
- Involves illegal activity
- Is designed to evade BSA regulations
- Has no business or apparent lawful purpose

SAR Reporting Limits
- Insider abuse in any amount
- Aggregate transactions of $5,000 or more when a suspect can be identified
- Aggregate transactions of $25,000 or more regardless of a potential suspect
SAR Examples

- Insufficient or suspicious member information
- Activity inconsistent with the member’s business
- Unusual cash transactions
- Unexpected or frequent funds transfers
- Avoiding reporting or record keeping requirements (structuring)
- Loan or check fraud

SAR Secrecy

- Strict confidentiality required
- All SAR filings reported to the board
- Board only needs minimal information (for example, amount, any losses, reason for filing)
OFAC
- Office of Foreign Assets Control
- Requirements are separate and distinct from the BSA
- Share a common national security goal

OFAC Requirements
- Freeze accounts or
- Prohibit or reject transactions with specified countries, entities and individuals
- Report blocked accounts and/or prohibited transactions to OFAC

OFAC Program
- Risk assessment
- Internal controls:
  - How data will be scanned
  - Investigations of possible hits
  - Process used to block and reject transactions
  - Managing blocked accounts
  - Reporting
- Independent Testing
- Responsible Individual
- Training
Questions

Heather Line
Compliance Specialist
801-599-2168
heather@utahscreditunions.org
Purpose of the Bank Secrecy Act (BSA)

- To identify the source, volume and movement of currency and monetary instruments among US financial institutions
- To aid in the investigation of money laundering, tax evasion, international terrorism and other criminal activity

Background of the BSA

<table>
<thead>
<tr>
<th>YEAR</th>
<th>LAW</th>
<th>PURPOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1970</td>
<td>Bank Secrecy Act</td>
<td>• Recordkeeping</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Currency Transaction Reports</td>
</tr>
<tr>
<td>1986</td>
<td>Money Laundering Control Act</td>
<td>• Money Laundering made a crime</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Prohibited structuring transactions to evade BSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Procedures to comply with BSA</td>
</tr>
<tr>
<td>1988</td>
<td>Anti-Drug Abuse Act</td>
<td>• Records of purchase of monetary instruments</td>
</tr>
<tr>
<td>1992</td>
<td>Annunzio-Wylie Anti-Money Laundering Act</td>
<td>• Suspicious Activity Reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Recordkeeping for wire transfers</td>
</tr>
<tr>
<td>2001</td>
<td>USA Patriot Act</td>
<td>• Criminalized the financing of terrorism</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enhanced Due Diligence Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Information Sharing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Enhanced BSA Program Requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Customer Identification Programs</td>
</tr>
</tbody>
</table>

Latest Developments

FinCEN Customer Due Diligence (CDD) Rules

- Meant to enhance customer due diligence requirements
- Adds a fifth major requirement to Anti-Money Laundering (AML) programs
- Contains explicit CDD requirements
- New requirement to identify beneficial owners of legal entity customers
- Compliance with new rules mandatory on May 11, 2018.
- Credit unions can opt to comply early.

Advisory on Cyber-Events and Cyber-Enabled Crime

Through this advisory FinCEN advises financial institutions on:
2017 Bank Secrecy Act Training for Volunteers

- Reporting cyber-enabled crime and cyber-events through Suspicious Activity Reports (SARs)
- Including relevant and available cyber-related information (e.g., Internet Protocol (IP) addresses with timestamps, virtual-wallet information, device identifiers) in SARs;
- Collaborating between BSA/Anti-Money Laundering (AML) units and in-house cybersecurity units to identify suspicious activity
- Sharing information, including cyber-related information, among financial institutions to guard against and report money laundering, terrorism financing, and cyber-enabled crime (Must be a registered 314b sharer).

Penalties for Non-Compliance

For the Credit Union
- Cease and desist orders
- Loss of charter
- Civil and Criminal money penalties

For Individuals
- Removal and bar from banking
- Civil and criminal money penalties ($250,000 to $500,000)
- Prison time

Case Studies
- Charles Sanders, Former chief compliance/risk officer for Gibraltar Private Bank and Trust
- Bethex Federal Credit Union, Bronx, NY

Board of Directors Responsibilities
- Approve the BSA Program annually
- Appoint a BSA Officer
- Review the BSA Risk Assessment as applicable
- Review periodic BSA program updates
- Ensure BSA officer has adequate staffing and resources
- Review reports of filed Suspicious Activity Reports
- Champion policy and procedure

BSA Compliance Program

Risk Assessment
- Risk assessment not required
- Examiners will complete one if the credit union does not
• Tell your own story
• BSA program should be based on the risk assessment
• The risk assessment should answer the following questions:
  • What types of products and services does the credit union offer?
  • Who is using them?
  • Where is the potential exposure to money laundering?
  • What steps have been taken to mitigate risk?

BSA Program Requirements

Independent Testing
• Qualified
• Independent
• Transaction Testing
• Comprehensive work papers

BSA Officer
• Authority
• Adequate Staffing
• Other Resources
• Training

Training
• New employees upon hire
• All employees periodically (annually)
• Tailored to specific business lines
• Cover employee accountability for compliance
• Credit union should maintain training records and materials
• Coverage of credit union policies, procedures, processes, and new rules and regulations
• Coverage of different forms of money laundering and terrorist financing
• Penalties for noncompliance with internal policies and regulatory requirements

Minimum Internal Controls
• Customer/Member Identification Procedures
• Customer/Member Due Diligence
• Suspicious Activity Reporting
• Currency Transaction Reporting
• CTR Exemptions
• Information Sharing under the USA Patriot Act
• Monetary Instrument Recordkeeping
• Funds Transfer Recordkeeping
• Office of Foreign Assets Control (Can be a separate policy)
• Program continuity despite changes in management or employee composition or structure
2017 Bank Secrecy Act Training for Volunteers

**Expanded Controls (as required)**
- Third Party Payment Processing
- Foreign accounts/branches/services
- Correspondent Accounts
- Brokered Deposits
- Non-Deposit Investment Products
- Insurance
- Private Banking

**CDD Procedures**
- Appropriate risk-based procedures for conducting ongoing CDD to understand the nature and purpose of customer relationships and to conduct ongoing monitoring to identify and report suspicious transactions, and, on a risk basis, to maintain and update customer information
- (Added as of May 11, 2018)

**Customer Identification Program (CIP)**

**Overview**
- Based on risk
- Each institution sets their own identification parameters
- Part of BSA Program

**Required Procedures**
- Verify the identity of any person seeking to open an account
- Maintain records of the information used to verify a person’s identity
- Determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations

**Suspicious Activity Reporting**
Credit unions are required to file a Suspicious Activity Report (SAR) if the institution knows or suspects that a transaction:
- Involves illegal activity
- Is designed to evade BSA regulations
- Has no business or apparent lawful purpose

**SAR Reporting Limits**
- Insider abuse in any amount
- Aggregate transactions of $5,000 or more when a suspect can be identified
- Aggregate transactions of $25,000 or more regardless of a potential suspect
Examples of Suspicious Activity
- Insufficient or suspicious member information
- Activity inconsistent with the member’s business
- Unusual cash transactions
- Unusual or frequent funds transfers
- Avoiding reporting or record keeping requirements (structuring)
- Loan fraud
- Check fraud

SAR Secrecy
- Strict confidentiality required
- All SAR filings reported to the board
- Board only needs minimal information (for example, amount, any losses, reason for filing)

OFAC

Overview
- Office of Foreign Assets Control
- Requirements are separate and distinct from the BSA
- Share a common national security goal

Requirements
- Freeze accounts or
- Prohibit or reject transactions with specified countries, entities and individuals
- Report blocked accounts and/or prohibited transactions to OFAC

Program Requirements
- Risk assessment
- Internal controls:
  - How data will be scanned
  - Investigations of possible hits
  - Process used to block and reject transactions
  - Managing blocked accounts
  - Reporting
- Independent Testing
- Responsible Individual
- Training
The Financial Crimes Enforcement Network (“FinCEN”) is issuing these FAQs to assist covered financial institutions in understanding the scope of the Customer Due Diligence Requirements for Financial Institutions,” published on May 11, 2016 (the “CDD Rule”), available at https://www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf. These FAQs provide interpretive guidance with respect to the CDD rule. FinCEN intends to issue additional FAQs or guidance as appropriate.

Frequently Asked Questions (FAQs)

**Question 1: Purpose of CDD Rule**

Q: Why is FinCEN issuing the CDD Rule?

A: FinCEN is issuing the CDD Rule to amend existing BSA regulations in order to clarify and strengthen customer due diligence requirements for certain financial institutions. The CDD Rule outlines explicit customer due diligence requirements and imposes a new requirement for these financial institutions to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions. Within this construct, as stated in the preamble to the Rule, FinCEN intends that the legal entity customer identify its ultimate beneficial owner or owners and not “nominees” or “straw men.”

**Question 2: Rule application**

Q: Does the CDD Rule apply to all financial institutions?

A: No. The CDD Rule applies to covered financial institutions.
Question 3: Covered financial institutions

Q: Which financial institutions are covered under the CDD Rule?

A: For purposes of the CDD Rule, covered financial institutions are federally regulated banks and federally insured credit unions, mutual funds, brokers or dealers in securities, futures commission merchants, and introducing brokers in commodities.¹

Question 4: CDD requirements for covered financial institutions with respect to beneficial ownership

Q: What are the requirements for covered financial institutions to collect beneficial ownership information?

A: The CDD Rule requires covered financial institutions to establish and maintain written procedures that are reasonably designed to identify and verify the beneficial owners of legal entity customers. These procedures must enable the institution to identify the beneficial owners of each customer at the time a new account is opened, unless the customer is otherwise excluded or the account is exempted. Also, the procedures must establish risk-based practices for verifying the identity of each beneficial owner identified to the covered financial institution, to the extent reasonable and practicable. The procedures must contain the elements required for verifying the identity of customers that are individuals under applicable customer identification program ("CIP") requirements.²

In short, covered financial institutions are now required to obtain, verify, and record the identities of the beneficial owners of legal entity customers.

Question 5: Amendments to the anti-money laundering ("AML") program requirements

Q: Are there any changes to the AML program requirements for covered financial institutions in the Rule?

A: Yes. The CDD Rule amends the AML program requirements for each covered financial institution to explicitly require covered institutions to implement and maintain appropriate risk-based procedures for conducting ongoing customer due diligence, to include:

- understanding the nature and purpose of the customer relationships; and
- conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.

A covered financial institution’s AML program must include, at a minimum: (1) a system of internal controls; (2) independent testing; (3) designation of a compliance officer or individual(s) responsible for day-to-day compliance; (4) training for appropriate personnel; and (5) appropriate risk-based procedures for conducting ongoing CDD to understand the nature and

¹“Covered financial institution” is defined at 31 CFR 1010.605(e)(1).
purpose of customer relationships and to conduct ongoing monitoring to identify and report suspicious transactions, and, on a risk basis, to maintain and update customer information.

**Question 6: Procedures for identification and verification of identity of beneficial owners**

Q: Must a covered financial institution’s procedures for identifying and verifying the identity of beneficial owners of legal entity customers be identical to its customer identification program?

A: No. However, the CDD Rule requires that the procedures, at a minimum, contain the same elements as required for verifying the identity of customers that are individuals under the applicable CIP rule. However, financial institutions may use photocopies or other reproductions of identification documents in the case of documentary verification.

**Question 7: Anti-money laundering procedures**

Q: Are covered financial institutions required to include the procedures for identifying and verifying the identity of the beneficial owners of legal entity customers in the institution’s AML compliance program?

A: Yes. The CDD procedures must be included in the covered financial institution’s AML compliance program.

**Question 8: Collection of beneficial ownership information**

Q: Are covered financial institutions required to collect any information about beneficial ownership from the legal entity customer?

A: Yes. Covered financial institutions must collect information on individuals who are beneficial owners of a legal entity customer in addition to the information they are required to collect on the customer under the CIP requirement.

**Question 9: Definition of beneficial owner**

Q: Who is a beneficial owner?

A: The Rule defines beneficial owner as each of the following:

- each individual, if any, who, directly or indirectly, owns 25% or more of the equity interests of a legal entity customer (i.e., the ownership prong); and
- a single individual with significant responsibility to control, manage, or direct a legal entity customer, including an executive officer or senior manager (e.g., a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer); or any other individual who regularly performs similar functions (i.e., the control prong). This list of positions is illustrative, not exclusive, as there is significant diversity in how legal entities are structured.
Under this definition, a legal entity will have a total of between one and five beneficial owners (i.e., one person under the control prong and zero to four persons under the ownership prong).

**Question 10: Collection of information for beneficial owners**

Q: Are covered financial institutions required to obtain information directly from the beneficial owners of legal entity customers?

A: No. The Rule requires financial institutions to obtain information about the beneficial owners of a legal entity from the individual seeking to open a new account at the covered financial institution on behalf of the legal entity customer. This individual could, but would not necessarily, be a beneficial owner.

**Question 11: Beneficial ownership information that must be collected for legal entity customers**

Q: What types of information are covered institutions required to collect on the beneficial owners of legal entity customers?

A: As with CIP for individual customers, covered financial institutions must collect from the legal entity customer the name, date of birth, address, and social security number or other government identification number (passport number or other similar information in the case of foreign persons) for individuals who own 25% or more of the equity interest of the legal entity (if any), and an individual with significant responsibility to control/manage the legal entity at the time a new account is opened.

**Question 12: Nominee owners**

Q: May a legal entity provide the identification of a nominee owner in response to a financial institution’s request for the identification of a beneficial owner?

A: No. As stated in the preamble to the Rule, FinCEN intends that the legal entity customer identify its ultimate beneficial owner or owners and not “nominees” or “straw men.” FinCEN reiterates that it is the responsibility of the legal entity customer to identify its ultimate beneficial owners and that the financial institution may rely upon the information provided, unless the institution has reason to question its accuracy.

**Question 13: The control prong of the beneficial ownership requirement**

Q: What types of individuals satisfy the definition of a person with “significant responsibility to control, manage, or direct a legal entity customer?”

A: Under the Rule, a legal entity must provide information on a control person with “significant responsibility to control, manage, or direct the company.” The rule also provides examples of the types of positions that could qualify, including “[a]n executive officer or senior manager (e.g., a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer).” FinCEN’s expectation is that the control person identified must be a high-level official in the legal entity, who is responsible for how the organization is run, and who will have access to a range of
information concerning the day-to-day operations of the company. The list of positions is illustrative, not exclusive.

**Question 14: Definition of account**

Q: How is “account” defined in the CDD Rule?

A: In order to maintain consistency with CIP, FinCEN added to the CDD Rule the same definition of the term “account” that is in the CIP rules for banks, brokers or dealers in securities, mutual funds, and futures commission merchants and introducing brokers in commodities.

**Question 15: Definition of new account**

Q: What is a new account?

A: The Rule defines a new account as each account opened at a covered financial institution by a legal entity customer on or after the May 11, 2018 applicability date.

**Question 16: Application to Existing Accounts**

Q: Does a covered financial institution have to obtain beneficial information on existing accounts?

A: No. The rule does not cover existing accounts that were opened before the applicability date.

**Question 17: Exemptions and limitations on exemptions**

Q: Are there any other type of accounts that are not covered by the CDD Rule?

A: Yes. Subject to certain limitations, covered financial institutions are also not required to identify and verify the identity of the beneficial owner(s) of a legal entity customer when the customer opens any of the following four categories of accounts:

- accounts established at the point-of-sale to provide credit products, solely for the purchase of retail goods and/or services at these retailers, up to a limit of $50,000;
- accounts established to finance the purchase of postage and for which payments are remitted directly by the financial institution to the provider of the postage products;
- accounts established to finance insurance premiums and for which payments are remitted directly by the financial institution to the insurance provider or broker; and
- accounts established to finance the purchase or lease of equipment and for which payments are remitted directly by the financial institution to the vendor or lessor of this equipment.

These exemptions will not apply under either of the following two circumstances:
- if the accounts are transaction accounts through which a legal entity customer can make payments to, or receive payments from, third parties.
- if there is the possibility of a cash refund for accounts opened to finance purchase of postage, insurance premium, or equipment leasing. If there’s the possibility of a cash refund, the financial institution must identify and verify the identity of the beneficial owner(s) either at the initial remittance, or at the time such refund occurs.

**Question 18: Collection of beneficial ownership information**

Q: Must covered financial institutions collect beneficial ownership information on all of the beneficial owners of a legal entity customer?

A: Covered financial institutions must collect and verify the beneficial ownership information of each person who meets the definition under the ownership prong, and of one person under the control prong. Under the ownership prong, covered financial institutions are required to collect the beneficial ownership information only for each individual who owns directly or indirectly 25% or more of the equity interest of a legal entity and under the control prong, for one individual with significant responsibility to control, manage, or direct the entity. However, the rule recognizes that there may be instances when no one individual owns 25% or more of the equity interest of the legal entity; in such instances, the financial institution is still required to collect the required information for one individual who controls, manages, or directs the legal entity customer.

**Question 19: Certification Form**

Q: Are covered financial institutions required to use the Certification Form that is in Appendix A of the final CDD Rule?

A: No. The Certification Form is provided as an optional form that financial institutions may use to obtain the required beneficial ownership information. Financial institutions may choose to comply by using the sample Certification Form, using the institution’s own forms, or any other means that complies with the substantive requirements of this obligation.

**Question 20: Definition of legal entity customer**

Q: Who is a legal entity customer?

A: The Rule defines a legal entity customer as a corporation, limited liability company, other entity created by the filing of a public document with a Secretary of State or similar office, a general partnership, and any similar entity formed under the laws of a foreign jurisdiction that opens an account. The definition also includes limited partnerships, business trusts that are created by a filing with a state office, and any other entity created in this manner.

A legal entity customer does not include sole proprietorships, unincorporated associations, or natural persons opening accounts on their own behalf.
**Question 21: Exclusions from the definition of legal entity customer**

**Q:** Are there any entities that are excluded from the definition of the legal entity customer and for which a covered financial institutions is not required to obtain beneficial ownership information?

**A:** Yes. The CDD Rule excludes from the definition of legal entity customer certain entities that are subject to Federal or State regulation and for which information about their beneficial ownership and management is available from the Federal or State agencies, such as:

- Financial institutions regulated by a Federal functional regulator or a bank regulated by a State bank regulator;
- Certain exempt persons for purposes of the currency transactions reporting obligations:
  - A department or agency of the United States, of any State, or of any political subdivision of a State;
  - Any entity established under the laws of the United States, or any State, or of any political subdivision of any State, or under an interstate compact;
  - Any entity (other than a bank) whose common stock or analogous equity interests are listed on the New York, American, or NASDAQ stock exchange;
  - Any entity organized under the laws of the United States or of any State at least 51% of whose common stock or analogous equity interests are held by a listed entity;
- Issuers of securities registered under section 12 of the Securities Exchange Act of 1934 (SEA) or that is required to file reports under 15(d) of that Act;
- An investment company, as defined in section 3 of the Investment Company Act of 1940, registered with the U.S. Securities and Exchange Commission (SEC);
- An SEC-registered investment adviser, as defined in section 202(a)(11) of the Investment Advisers Act of 1940;
- An exchange or clearing agency, as defined in section 3 of the SEA, registered under section 6 or 17A of that Act;
- Any other entity registered with the SEC under the SEA;
- A registered entity, commodity pool operator, commodity trading advisor, retail foreign exchange dealer, swap dealer, or major swap participant, defined in section 1a of the Commodity Exchange Act, registered with the Commodity Futures Trading Commission;
- A public accounting firm registered under section 102 of the Sarbanes-Oxley Act.
Additional regulated entities:

- A bank holding company, as defined in section 2 of the Bank Holding Company Act of 1956 (12 USC 1841) or savings and loan holding company, as defined in section 10(n) of the Home Owners’ Loan Act (12 USC 1467a(n));
- A pooled investment vehicle operated or advised by a financial institution excluded from the definition of legal entity customer under the final CDD rule;
- An insurance company regulated by a State;
- A financial market utility designated by the Financial Stability Oversight Council under Title VIII of the Dodd-Frank Wall Street Reform and Customer Protection Act of 2010;

Excluded Foreign Entities:

- A foreign financial institution established in a jurisdiction where the regulator of such institution maintains beneficial ownership information regarding such institution;
- A non-U.S. governmental department, agency or political subdivision that engages only in governmental rather than commercial activities; and
- Any legal entity only to the extent that it opens a private banking account subject to 31 CFR 1010.620.

Question 22: Trusts

Q: Are trusts included in the definition of legal entity customer?

A: No. The definition of legal entity customers only includes statutory trusts created by a filing with the Secretary of State or similar office. Otherwise, it does not include trusts. This is because a trust is a contractual arrangement between the person who provides the funds or other assets and specifies the terms (i.e., the grantor/settlor) and the person with control over the assets (i.e., the trustee), for the benefit of those named in the trust deed (i.e., the beneficiaries). Formation of a trust does not generally require any action by the state.

The CDD Rule does not supersede existing obligations and practices regarding trusts generally. The preamble to each of the CIP rules notes that, while financial institutions are not required to look through a trust to its beneficiaries, they “may need to take additional steps to verify the identity of a customer that is not an individual, such as obtaining information about persons with control over the account.”

We understand that where trusts are direct customers of financial institutions, financial institutions generally also identify and verify the identity of trustees, because trustees will necessarily be signatories on trust accounts. Furthermore, under supervisory guidance for banks, “in certain circumstances involving revocable trusts, the bank may need to gather information about the settlor, grantor, trustee, or other persons with the

---

3 See, e.g., “Customer Identification Programs for Broker-Dealers,” 68 FR at 25116 n.32. (May 9, 2003).
authority to direct the trustee, and who thus have authority or control over the account, in order to establish the true identity of the customer.”

**Question 23: Office of Foreign Assets Control (OFAC) Regulations**

Q: Are covered financial institutions required to comply with the OFAC regulations with respect to beneficial ownership information?

A: Covered financial institutions should use beneficial ownership information as they use other information they gather regarding customers (e.g., through compliance with the CIP requirements), including for compliance with OFAC-administered sanctions.

**Question 24: Section 314(a) Requirements**

Q: Do covered financial institutions now have additional obligations under Section 314(a) for beneficial ownership information?

A: FinCEN does not expect the information obtained under the CDD Rule to add additional 314(a) requirements for financial institutions. The regulation implementing section 314(a) does not require the reporting of beneficial ownership information associated with an account or transaction matching a named subject in a 314(a) request. Covered financial institutions are required to search their records for accounts or transactions matching a named subject and report whether a match exists using the identifying information provided in the request.

**Question 25: Effective Date of the final CDD Rule**

Q: What is the effective date of the CDD Rule?

A: July 11, 2016, which is 60 days from the publication of the CDD Rule in the Federal Register.

**Question 26: Applicability Date of the final CDD Rule**

Q: When must covered financial institutions implement the final rule?

A: Covered financial institutions will have until May 11, 2018, two years from the date the final CDD Rule was published in the Federal Register, to implement and comply with the CDD Rule.

---

Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime

Cybercriminals target the financial system to defraud financial institutions and their customers and to further other illegal activities. Financial institutions can play an important role in protecting the U.S. financial system from these threats.

The proliferation of cyber-events and cyber-enabled crime represents a significant threat to consumers and the U.S. financial system. The Financial Crimes Enforcement Network (FinCEN) issues this advisory to assist financial institutions in understanding their Bank Secrecy Act (BSA) obligations regarding cyber-events and cyber-enabled crime. This advisory also highlights how BSA reporting helps U.S. authorities combat cyber-events and cyber-enabled crime.

Through this advisory FinCEN advises financial institutions on:

I. Reporting cyber-enabled crime and cyber-events through Suspicious Activity Reports (SARs);

II. Including relevant and available cyber-related information (e.g., Internet Protocol (IP) addresses with timestamps, virtual-wallet information, device identifiers) in SARs;

III. Collaborating between BSA/Anti-Money Laundering (AML) units and in-house cybersecurity units to identify suspicious activity; and

IV. Sharing information, including cyber-related information, among financial institutions to guard against and report money laundering, terrorism financing, and cyber-enabled crime.

For the purpose of this advisory:

**Cyber-Event:** An attempt to compromise or gain unauthorized electronic access to electronic systems, services, resources, or information.

**Cyber-Enabled Crime:** Illegal activities (e.g., fraud, money laundering, identity theft) carried out or facilitated by electronic systems and devices, such as networks and computers.
For the purpose of this advisory (continued):

**Cyber-Related Information:** Information that describes technical details of electronic activity and behavior, such as IP addresses, timestamps, and Indicators of Compromise (IOCs). Cyber-related information also includes, but is not limited to, data regarding the digital footprint of individuals and their behavior.

**Background**

The size, reach, speed, and accessibility of the U.S. financial system make financial institutions attractive targets to traditional criminals, cybercriminals, terrorists, and state actors. These actors target financial institutions’ websites, systems, and employees to steal customer and commercial credentials and proprietary information; defraud financial institutions and their customers; or disrupt business functions. Financial institutions can play an important role in safeguarding customers and the financial system from these threats through timely and thorough reporting of cyber-events and cyber-related information in SARs.

**Value of BSA Reporting in Combating Cybercriminals and Cyber-Enabled Crime**

FinCEN and law enforcement regularly use information financial institutions report under the BSA to initiate investigations, identify criminals, and disrupt and dismantle criminal networks. The cyber-related information that financial institutions include in this reporting is a valuable source of investigatory leads. Law enforcement has been able to use cyber-related information reported—such as IP addresses with timestamps, cyber-event data, and virtual-wallet information—to track criminals, identify victims, and trace illicit funds.

For example, BSA reporting by more than 20 financial institutions—on transactions related to cyber-enabled crimes—played an important role in the investigation of an internet-based company, its co-founders, and other collaborators. This company acted as an unregistered online money-transmitting business and offered digital currency services specifically designed to provide anonymity to facilitate international crime and money laundering. Criminals used this company to conduct over $6 billion in illicit transactions involving proceeds from cyber-attacks, credit card fraud, child pornography, Ponzi schemes, identity theft, and trafficking in narcotics and other contraband.

---

1. Unless otherwise defined by FinCEN, FinCEN uses the [Glossary of Key Information Security Terms](#) and other publications issued by the [National Institute of Standards and Technology (NIST)](#) for definitions of cyber-related terms. NIST is a non-regulatory federal agency within the U.S. Department of Commerce. Financial Institutions are encouraged to refer to the NIST Glossary for definitions.
Regulatory Expectations

This advisory does not change existing BSA requirements or other regulatory obligations for financial institutions. Financial institutions should continue to follow federal and state requirements and guidance on cyber-related reporting and compliance obligations.

Financial institutions should also note that filing a SAR does not relieve financial institutions from any other applicable requirements to timely notify appropriate regulatory agencies of events concerning critical systems and information or of disruptions in their ability to operate. In addition, the recently enacted Cybersecurity Act of 2015, also known as the Cybersecurity Information Sharing Act (CISA), does not change any SAR-reporting requirements under the BSA, SAR confidentiality rules, or the safe harbor protections under section 314 of the USA PATRIOT Act.

Guidance to U.S. Financial Institutions

The following guidance explains how BSA regulations and requirements apply to cyber-events, cyber-enabled crime, and cyber-related information.

I. SAR Reporting of Cyber-Events

Cyber-events targeting financial institutions often constitute criminal activity and can serve as means to commit a wide range of further criminal activity. For instance, criminals may seek to obtain unauthorized electronic access to electronic systems, services, resources, or information to conduct unauthorized transactions. Cyber-events can target or affect funds...
directly—such as in cases of fraud, identity/credential theft, and misappropriation of funds. Similarly, cyber-events can generate illicit proceeds—such as in cases of ransomware attacks and the sale of stolen proprietary information and credit card numbers.

**Mandatory SAR reporting of cyber-events**

A financial institution is required to report a suspicious transaction conducted or attempted by, at, or through the institution that involves or aggregates to $5,000 or more in funds or other assets. If a financial institution knows, suspects, or has reason to suspect that a cyber-event was intended, in whole or in part, to conduct, facilitate, or affect a transaction or a series of transactions, it should be considered part of an attempt to conduct a suspicious transaction or series of transactions. Cyber-events targeting financial institutions that could affect a transaction or series of transactions would be reportable as suspicious transactions because they are unauthorized, relevant to a possible violation of law or regulation, and regularly involve efforts to acquire funds through illegal activities.

In determining whether a cyber-event should be reported, a financial institution should consider all available information surrounding the cyber-event, including its nature and the information and systems targeted. Similarly, to determine monetary amounts involved in the transactions or attempted transactions, a financial institution should consider in aggregate the funds and assets involved in or put at risk by the cyber-event.

Financial institutions should also be familiar with any other cyber-related SAR-filing obligations required by their functional regulator. For instance, the Office of the Comptroller of the Currency (OCC) requires national banks to file SARs to report unauthorized electronic intrusions. The Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA) issued guidance concerning the filing of SARs to report certain computer-related crimes.

9. *See*, 31 C.F.R. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.20. The monetary threshold for filing money services businesses SARs is, with one exception, set at or above $2,000. 31 C.F.R. § 1022.320(a)(2).

10. Guidance on the reporting of Unauthorized Electronic Intrusions (UEIs) remains unchanged; see supra note 2. Financial institutions should report cyber-events as UEIs when such cyber-events meet the definition of a UEI. A UEI is defined as gaining access to a computer system of a financial institution to: a) remove, steal, procure or otherwise affect funds of the financial institution or the institution’s customers; b) remove, steal, procure or otherwise affect critical information of the financial institution including customer account information; or c) damage, disable, disrupt, impair or otherwise affect critical systems of the financial institution.


The following examples illustrate situations in which SAR reporting of cyber-events is mandatory. These examples do not, however, describe all instances when cyber-events require the filing of a SAR.

Example 1: Through a malware intrusion (a type of cyber-event), cybercriminals gain access to a bank’s systems and information. Following its detection, the bank determines the cyber-event put $500,000 of customer funds at risk, based on the systems and/or information targeted by the cyber-event. Accordingly, the bank reasonably suspects the intrusion was in part intended to enable the perpetrators to conduct unauthorized transactions using customers’ funds.

The bank must file a SAR because it has reason to suspect the cybercriminals, through the malware-intrusion, intended to conduct or could have conducted unauthorized transactions aggregating or involving at least $5,000 in funds or assets. As explained in the next section, the bank should include all available information in the SAR relevant to the suspicious activity, including cyber-related information such as a description and signatures of the cyber-event, attack vectors, command-and-control nodes, etc.

Example 2: Through a cyber-event, cybercriminals gain access to a financial institution’s systems/networks. The cyber-event exposes sensitive customer information such as account numbers, credit card numbers, balances, limits, scores, histories, online-banking credentials, passwords/PINs, challenge questions and answers, or other similar information useful or necessary to conduct, affect, or facilitate transactions.

By evaluating the cyber-event and the type of information sought by its perpetrators, the financial institution reasonably suspects the cyber-event may have targeted information for the purpose of conducting, facilitating, or affecting transactions aggregating to at least $5,000. For instance, the financial institution could reasonably suspect the cybercriminals intended to steal and sell the exposed sensitive customer information to other criminals for financial exploitation to include unauthorized transactions at the institution. As further described below, the targeted financial institution should file a SAR to report all relevant information, including cyber-related information and information pertaining to any related unauthorized transactions.

Examples 1 and 2 describe instances where a financial institution should file a SAR in response to a cyber-event. Although no actual transactions may have occurred in these examples, the circumstances of the cyber-events and the systems and information targeted could reasonably lead the financial institutions to suspect the events were intended to be part of an attempt to conduct, facilitate, or affect an unauthorized transaction or series of unauthorized transactions aggregating or involving at least $5,000 in funds or assets.
Example 3: A Money Services Business (MSB) knows or suspects a Distributed Denial of Service (DDoS) attack prevented or distracted its cybersecurity or other appropriate personnel from immediately detecting or stopping an unauthorized $2,000 wire transfer.

In this case, the financial institution should file a single SAR to report both the unauthorized wire transfer and the related DDoS attack. The financial institution should report the transaction because it was unauthorized and meets the filing threshold; and it should report the DDoS attack because the DDoS attack was perpetrated to conceal the unauthorized wire transfer.

Voluntary reporting of cyber-events

FinCEN encourages, but does not require, financial institutions to report egregious, significant, or damaging cyber-events and cyber-enabled crime when such events and crime do not otherwise require the filing of a SAR.

To illustrate, consider a DDoS attack that disrupts a financial institution’s website and disables the institution’s online banking services for a significant period of time. After mitigating and investigating the DDoS attack, the affected financial institution determines the attack was not intended to and could not have affected any transactions. Although a financial institution is not required to report such DDoS attack, FinCEN encourages the financial institution to consider filing a SAR because the attack caused online banking disruptions that were particularly damaging to the institution. SAR reporting of cyber-events, even those that may not meet mandatory SAR-filing requirements, is highly valuable in law enforcement investigations.

II. Including Cyber-Related Information in SAR Reporting

Financial institutions are required to file complete and accurate reports that incorporate all relevant information available, including cyber-related information. Because everyday financial transactions increasingly rely on electronic systems and resources, illicit financial activity often has a digital footprint, which may correspond to illicit actors and their associates, their activity, and related suspicious transactions.

Thus, financial institutions should include available cyber-related information when reporting any suspicious activity, including those related to cyber events as well as those related to other activity, such as fraudulent wire transfers. Cyber-related information includes, but is not limited to, IP addresses with timestamps, virtual-wallet information, device identifiers, and cyber-event information. FinCEN also encourages the filing of all such cyber-related information when a financial institution files a voluntary SAR. For additional information on reporting cyber-related information in SARs, please refer to these Frequently Asked Questions (FAQs) available on FinCEN’s website.
Reporting cyber-related information involving cyber-events

When filing a mandatory or voluntary SAR involving a cyber-event, financial institutions should provide complete and accurate information, including relevant facts in appropriate SAR fields, and information about the cyber-event in the narrative section of the SAR—in addition to any other related suspicious activity. As needed, financial institutions may also attach a comma separated value (CSV) file to SARs to report data, such as cyber-event data and transaction details, in tabular form. For example, to the extent available, SARs involving cyber-events should include:

- Description and magnitude of the event
- Known or suspected time, location, and characteristics or signatures of the event
- Indicators of compromise
- Relevant IP addresses and their timestamps
- Device identifiers
- Methodologies used
- Other information the institution believes is relevant

Financial institutions subject to large numbers of cyber-events may report them through a single cumulative SAR filing when such events are similar in nature. For instance, a financial institution may file one SAR to report several malware intrusions if these events share common characteristics and indicators such as the methodology used, the vulnerability exploited, and IP addresses involved.

FinCEN also encourages financial institutions to incorporate cyber-related information into their BSA/AML monitoring efforts and report relevant cyber-related information in SARs. In the event a financial institution’s filing software is not yet capable of including certain relevant information such as cyber-related information, as clarified by FinCEN in May 2013, the institution should manually complete discrete SAR filings until it updates its software to allow the inclusion such information. Financial institutions can submit discrete SARs through FinCEN’s BSA E-Filing System.

This advisory is not intended to, and does not, create any new obligation or expectation requiring financial institutions to collect cyber-related information as a matter of course.

---

13. A CSV file is a part of, but not a substitute for, the SAR narrative. In addition, like other information prepared in connection with a SAR filing but not attached to a SAR, an unattached CSV file is considered supporting documentation and should be accorded confidentiality to the extent it indicates the existence of a SAR.

14. See FAQs regarding the Reporting Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information through SARs (October 2016).

15. See Frequently Asked Questions Regarding the FinCEN SAR (May 2013).
III. Collaboration between BSA/AML and Cybersecurity Units

As the examples above illustrate, collaboration and ongoing communication among BSA/AML, cybersecurity, and other units will help financial institutions conduct a more comprehensive threat assessment and develop appropriate risk management strategies to identify, report, and mitigate cyber-events and cyber-enabled crime. Accordingly, financial institutions are encouraged to internally share relevant information from across the organization including, as appropriate, with BSA/AML staff, cybersecurity personnel, fraud prevention teams, and other potentially affected units.

Information provided by cybersecurity units could reveal additional patterns of suspicious behavior and identify suspects not previously known to BSA/AML units. For instance, BSA/AML units can use cyber-related information, such as patterns and timing of cyber-events and transaction instructions coded into malware among other things, to (1) help identify suspicious activity and criminal actors and (2) develop a more comprehensive understanding of their BSA/AML risk exposure. Likewise, cybersecurity personnel can use information provided by BSA/AML units to help the institution guard against cyber-events and cyber-enabled crime. In addition, this type of internal cooperation provides for more comprehensive and complete SAR reporting and is consistent with the principles involved in establishing a strong culture of compliance.16

IV. Sharing Cyber-Related Information between Financial Institutions

Financial institutions can work together to identify threats, vulnerabilities, and criminals. By sharing information with one another, financial institutions may gain a more comprehensive and accurate picture of possible threats, allowing for more precise decision making in risk mitigation strategies. FinCEN continues to encourage financial institutions to use all lawful means to guard against money laundering and terrorist activities presented through cyber-events and cyber-enabled crime.

To encourage information sharing, Section 314(b) of the USA PATRIOT Act extends a safe harbor from liability to financial institutions—after notifying FinCEN and satisfying certain other requirements—that voluntarily share information with one another for the purpose of identifying and, where appropriate, reporting potential money laundering or terrorist activities.17 Under Section 314(b), financial institutions may share information, including cyber-related information, regarding individuals, entities, organizations, and countries for

---


17. For further information regarding Section 314(b), including requirements for sharing information, please refer to the Section 314(b) Fact Sheet available on FinCEN’s website.
the purposes of identifying and reporting money laundering and terrorist activities. Thus, financial institutions may receive 314(b) safe harbor protections when sharing cyber-related information for the above mentioned purposes.¹⁸

Cyber-related information, such as information about specific malware signatures, IP addresses and device identifiers, and seemingly anonymous virtual currency addresses, for example, can help identify the individuals, entities, organizations, or countries involved or responsible for the cyber-event or cyber-enabled crime linked to money laundering or terrorist activities.

**For Immediate Assistance, Contact Regulatory and Law Enforcement Agencies**

Financial institutions needing immediate assistance in the event of a cyber-event or a cyber-enabled crime should contact appropriate regulatory and law enforcement agencies. Regulatory and law enforcement agencies can help affected financial institutions normalize systems and operations and, in some cases, reduce monetary losses. The U.S. Department of Homeland Security (DHS) published a fact sheet on obtaining threat and asset response assistance following a cyber incident.¹⁹ In addition, the U.S. Department of Justice published a guide outlining appropriate government agencies to contact in the event of computer hacking, fraud, and other internet-related crime.²⁰

**For Further Information**

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Resource Center at FRC@fincen.gov, (800) 767-2825 (Option 9), or (703) 905-3591 (Option 9). Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day). The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

FinCEN’s mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

---


¹⁹. The DHS fact sheet was issued pursuant to Presidential Policy Directive 41, which sets forth principles governing the Federal Government’s response to any cyber incident, whether involving government or private sector entities. The DHS fact sheet also lists key points of federal contact and is available at [https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Response%20United%20Message.pdf](https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Response%20United%20Message.pdf).

CONSENT ORDER

WHEREAS, the Office of the Comptroller of the Currency ("OCC") intends to initiate cease and desist and civil money penalty proceedings against Charles Sanders ("Respondent") pursuant to 12 U.S.C. § 1818(b) and (i) on the basis of Respondent’s activities while serving as Chief Compliance Officer and Chief Risk Officer ("CCO and CRO") of Gibraltar Private Bank and Trust Company, Coral Gables, Florida ("Bank");

WHEREAS, in the interest of cooperation and to avoid the costs associated with future administrative and judicial proceedings with respect to the above matter, Respondent, without admitting or denying any wrongdoing, desires to consent to the issuance of this Consent Order ("Order") issued pursuant to 12 U.S.C. § 1818(b) and (i);

NOW, THEREFORE, it is stipulated by and between the OCC, through the duly authorized representative of the Comptroller of the Currency ("Comptroller"), and Respondent that:

ARTICLE I

JURISDICTION

(1) The Bank is an “insured depository institution” as that term is defined in 12 U.S.C. § 1813(c)(2).
(2) Respondent was an officer of the Bank and was an “institution-affiliated party” of the Bank as that term is defined in 12 U.S.C. § 1813(u), having served in such capacity within six (6) years from the date of this Order. See 12 U.S.C. § 1818(i)(3).

(3) The Bank is a Federal savings association within the meaning of 12 U.S.C. § 1813(q)(1)(C), and is examined by the OCC. See 12 U.S.C. §§ 1461 et seq., 5412(b)(2)(B).

(4) The OCC is the “appropriate Federal banking agency” as that term is defined in 12 U.S.C. § 1813(q) and is therefore authorized to initiate and maintain this cease and desist and civil money penalty action against Respondent pursuant to 12 U.S.C. § 1818(b) and (i).

ARTICLE II

COMPTROLLER’S FINDINGS

The Comptroller finds, and Respondent neither admits nor denies, the following:

(1) During the period from May 2008 to November 2009, while the Respondent was CCO and CRO, the Bank failed to timely file suspicious activity reports on a set of accounts for a customer who was later convicted of crimes relating to an illegal Ponzi scheme (“Relevant Accounts”). Based on the information known to the Bank about the customer and the Relevant Accounts, transactions occurring within the Relevant Accounts had no business or apparent lawful purpose. The Bank’s Bank Secrecy Act (“BSA”) Officer investigated this activity, reported this information to Respondent, prepared suspicious activity reports, and communicated the preparation of those reports to Respondent. Respondent agreed with the contents of those reports, but he failed to ensure the Bank filed timely suspicious activity reports, causing the Bank to be in violation of laws and regulations, including 12 C.F.R. § 163.180.
(2) By reason of the foregoing conduct, Respondent violated a law or regulation and engaged in reckless unsafe or unsound practices; which violations or practices were part of a pattern of misconduct that caused more than a minimal loss to the Bank. Respondent’s misconduct resulted in loss to the Bank; demonstrated willful or continuing disregard for the safety and soundness of the Bank, and involved a reckless disregard for the law or applicable regulations.

ARTICLE III

ORDER TO CEASE AND DESIST

Respondent consents to, and it is ORDERED that:

(1) Whenever Respondent is employed by, or is offered employment at, a depository institution (as defined in 12 U.S.C. § 1813(c)(1)) or otherwise becomes an institution-affiliated party within the meaning of 12 U.S.C. § 1813(u), Respondent shall:

(a) Comply fully with all laws, regulations, and policies applicable to any insured depository institution with which he is or may become affiliated including but not limited to 31 U.S.C. § 5318, 12 C.F.R. §§ 21.11, 21.21, and 163.180;

(b) Provide the Board of Directors of the depository institution of which Respondent is currently an institution-affiliated party with a copy of this Order. Respondent shall provide written certification of compliance with this paragraph to the Director, Enforcement and Compliance Division, Office of the Comptroller of the Currency, 400 7th Street SW, Washington, DC 20219, within ten (10) days of execution of this Order; and
(c) With respect to any future employment, prior to accepting employment at a depository institution or becoming an institution-affiliated party, provide the President or Chief Executive Officer of the depository institution with a copy of this Order. Respondent shall provide written notice of such acceptance to the Director, Enforcement and Compliance Division, Officer of the Comptroller of the Currency, 400 7th Street SW, Washington, DC 20219, along with a written certification of his compliance with this paragraph within ten (10) days after acceptance of such position.

(2) If, at any time, Respondent is uncertain whether a situation implicates paragraph (1) of this Article, or if Respondent is uncertain about his duties arising from these or any other requirements of this Order, he shall obtain, at his own expense, and abide by, the written advice of counsel regarding his duties and responsibilities with respect to the matter. To comply with his paragraph, Respondent shall engage counsel who is in no way affiliated with the institution; and who has never been subject to any formal sanctions by any Federal banking agency, either by agency order or consent, as disclosed on the banking agencies’ web sites.

(3) This Order shall be enforceable to the same extent and in the same manner as an effective and outstanding order that has been issued and has become final pursuant to 12 U.S.C. § 1818.

ARTICLE IV

ORDER FOR CIVIL MONEY PENALTY

Respondent consents to, and it is ORDERED that:

(1) Respondent shall pay a civil money penalty in the amount of two thousand five hundred dollars ($2,500), which shall be paid in full upon Respondent’s execution of this Order.
(2) Respondent shall make payment in full by cashier’s or certified check made payable to the Treasurer of the United States, and shall deliver the payment to: Office of the Comptroller of the Currency, P.O. Box 979012, St. Louis, Missouri 63197-9000. The docket number of this case (AA-EC-2015-92) shall be entered on the submitted payment.

(3) This Order shall be enforceable to the same extent and in the same manner as an effective and outstanding order that has been issued and has become final pursuant to 12 U.S.C. § 1818.

ARTICLE V

CLOSING

(1) By executing this Order, Respondent waives:

(a) the right to a Notice of Charges for Issuance of an Order to Cease and Desist and Notice of Civil Money Penalty Assessment under 12 U.S.C. § 1818(b) and (i);

(b) all rights to a hearing and a final agency decision pursuant to 12 U.S.C. § 1818(b) and (i) and 12 C.F.R. Part 109;

(c) all rights to seek judicial review of this Order;

(d) all rights in any way to contest the validity of this Order; and

(e) any and all claims for fees, costs, or expenses against the United States, the OCC, or any officer, employee, or agent of the OCC, related in any way to this enforcement matter or this Order, whether arising under common law or under the terms of any statute, including, but not limited to, the Equal Access to Justice Act, 5 U.S.C. § 504 and 28 U.S.C. § 2412.
(2) Respondent shall not cause, participate in, or authorize the Bank (or any subsidiary or affiliate of the Bank) to incur, directly or indirectly, any expense relative to the negotiation and issuance of this Order except as permitted by 12 C.F.R. § 145.121 and Part 359. In addition, Respondent shall not, directly or indirectly, obtain or accept any indemnification (or other reimbursement) from the Bank (or any subsidiary or affiliate of the Bank) with respect to such amounts except as permitted by 12 C.F.R. § 145.121 and Part 359; provided, however, Respondent may not obtain or accept such indemnification with respect to payment of the civil money penalty.

(3) Respondent acknowledges that he has read and understands the premises and obligations of this Order and declares that no separate promise or inducement of any kind has been made by the OCC or any officer, employee, or agent of the OCC to cause or induce Respondent to agree to consent to the issuance of this Order and/or to execute this Order.

(4) This Order constitutes a settlement of any proceedings arising out of the facts, omissions, or violations described in the Comptroller’s Findings (Article II of this Order). The OCC agrees not to institute the proceedings referenced in the first whereas clause of this Order for the specific acts, omissions, or violations described in Article II of this Order unless such acts, omissions, or violations reoccur. However, the specific acts, omissions, or violations described in Article II may be used by the OCC in future enforcement actions to establish a pattern of misconduct or the continuation of a pattern of misconduct.

(5) This Order shall not be construed as an adjudication on the merits and, except as set forth in paragraph (4) above, shall not inhibit, estop, bar, or otherwise prevent the OCC from taking any action affecting Respondent if, at any time, the OCC deems it appropriate to do so to fulfill the responsibilities placed upon the OCC by the several laws of the United States.
(6) Nothing in this Order shall preclude any proceedings brought by the OCC to enforce the terms of this Order, and nothing in this Order constitutes, nor shall Respondent contend that it constitutes, a waiver of any right, power, or authority of any other representatives of the United States or agencies thereof, including the Department of Justice, to bring other actions deemed appropriate.

(7) This Order is intended to be, and shall be construed to be, a final order issued pursuant to 12 U.S.C. § 1818, and expressly does not form, and may not be construed to form, a contract binding on the United States, the OCC, or any officer, employee, or agent of the OCC. Respondent expressly acknowledges that no officer, employee, or agent of the OCC has statutory or other authority to bind the United States, the United States Treasury Department, the OCC, or any other federal bank regulatory agency or entity, or any officer, employee, or agent of those entities, to a contract affecting the OCC’s exercise of its supervisory responsibilities.

(8) This Order is “issued with the consent of . . . the institution-affiliated party concerned,” pursuant to 12 U.S.C. § 1818(h)(2).

(9) The terms of this Order, including this paragraph, are not subject to amendment or modification by any extraneous expression, prior agreements, or prior arrangements between the parties, whether oral or written.

(10) The provisions of this Order are effective upon issuance by the OCC, through the Comptroller’s duly authorized representative, whose hand appears below, and shall remain effective and enforceable, except to the extent that, and until such time as, any provisions of this Order shall have been amended, suspended, waived, or terminated in writing by the OCC, through the Comptroller’s duly authorized representative.
IN TESTIMONY WHEREOF, the undersigned has hereunto set his hand.

/s/ Charles Sanders       3/7/16

Charles Sanders

_____________________________
Date

_____________________________

IT IS SO ORDERED.

/s/ Michael R. Brickman      3/15/16

Michael R. Brickman
Deputy Comptroller for Special Supervision

_____________________________
Date
UNITED STATES OF AMERICA
DEPARTMENT OF THE TREASURY
FINANCIAL CRIMES ENFORCEMENT NETWORK

IN THE MATTER OF:   )
)  )  )  )  Number 2016-06
Bethex Federal Credit Union  )
Bronx, New York  )

ASSESSMENT OF CIVIL MONEY PENALTY

I. INTRODUCTION

The Financial Crimes Enforcement Network (FinCEN) has determined that grounds exist to assess a civil money penalty against Bethex Federal Credit Union (Bethex or the Credit Union), pursuant to the Bank Secrecy Act (BSA) and regulations issued pursuant to that Act.¹

FinCEN has the authority to investigate credit unions for compliance with the BSA pursuant to 31 C.F.R. § 1010.810, which grants FinCEN “[o]verall authority for enforcement and compliance, including coordination and direction of procedures and activities of all other agencies exercising delegated authority under this chapter.” As a credit union, Bethex was a “financial institution” and a “bank” within the meaning of the BSA and its implementing regulations during the time relevant to this investigation. 31 U.S.C. § 5312(a)(2)(E); 31 C.F.R. §§ 1010.100(d)(6) and 1010.100(t). The National Credit Union Administration (NCUA) was Bethex’s federal functional regulator and examines credit unions, including Bethex, for compliance with the BSA and its implementing regulations.

Bethex was a federally-chartered, low-income-designated, community development financial institution in the Bronx, New York. Since 2002, Bethex maintained internal controls specific to low and moderate-income clientele within its designated field of membership in New York City. In 2011, Bethex began providing banking services to a large number of wholesale, commercial money services businesses (MSBs). Many of these MSBs were located in high-risk jurisdictions outside New York and engaged in high-risk activity, including wiring millions of dollars per month to foreign jurisdictions at risk for money laundering. When Bethex expanded its customer base to include these MSBs, it did not take steps to update its anti-money laundering (AML) program. During this time, Bethex relied on a third party to conduct much of the due diligence and suspicious activity monitoring for these MSBs without appropriate verification or inspection of the third-party’s compliance activity. As a result, Bethex was unable to adequately monitor, detect, and report suspicious activity or mitigate the associated risks these MSBs posed, leaving the Credit Union particularly vulnerable to money laundering.

II. DETERMINATIONS

From January 1, 2011 through December 31, 2012, Bethex willfully violated the BSA’s AML program and reporting requirements. Bethex provided banking services to MSBs for which it did not adequately assess or mitigate the risks of money laundering and terrorist financing.

Bethex had a history of AML compliance deficiencies that led to egregious BSA failures starting in 2011. Systemic and continuing AML program deficiencies were cited in ten of the

---

2 In civil enforcement of the BSA under 31 U.S.C. § 5321(a)(1), to establish that a financial institution or individual acted willfully, the government need only show that the financial institution or individual acted with either reckless disregard or willful blindness. The government need not show that the entity or individual had knowledge that the conduct violated the BSA, or that the entity or individual otherwise acted with an improper motive or bad purpose.
thirteen examinations conducted on Bethex between 2005 and 2013. Without addressing its BSA deficiencies, Bethex brought on a substantial new business line devoted to wholesale MSBs. At the same time that Bethex’s wholesale MSB activity was increasing, Bethex continued to have internal control and independent testing deficiencies. In 2012, Bethex continued to have internal control deficiencies, as well as training, customer identification program, recordkeeping and reporting deficiencies, and failed to designate an appropriately competent compliance officer. Weaknesses in Bethex’s BSA/AML compliance program caused significant reputational and regulatory damage to the Credit Union, contributing in part to its eventual conservatorship by the NCUA in September 2015. The NCUA liquidated Bethex and discontinued its operations in December 2015.

As described in more detail below, Bethex failed to: (a) implement an adequate AML program, 31 U.S.C. § 5318(h); 31 C.F.R. § 1020.210; and (b) detect and adequately report suspicious transactions, 31 U.S.C. § 5318(g); 31 CFR § 1020.320.

**A. Violations of the Requirement to Establish and Implement an Effective Anti-Money Laundering Program**

Bethex failed to establish and implement an effective AML program. The BSA and its implementing regulations require all federally-chartered credit unions to establish and implement AML programs. 31 U.S.C. § 5318(h) and 31 C.F.R. § 1020.210. A federally-chartered credit union is deemed to have satisfied BSA/AML program requirements if it implements and maintains an AML program that complies with the applicable regulations of the NCUA, its federal functional regulator. 31 C.F.R. § 1020.210. The NCUA requires each credit union under its supervision to establish and maintain a written AML program that, at a minimum: (1) provides for a system of internal controls to assure ongoing compliance; (2) provides for independent testing for compliance to be conducted by bank personnel or by an outside party; (3)
designates an individual or individuals responsible for coordinating and monitoring day-to-day compliance; and (4) provides training for appropriate personnel. 12 C.F.R. § 748.2. Bethex failed to implement adequate internal controls or designate a qualified compliance officer.

1. Internal Controls

Bethex failed to implement an effective system of internal controls reasonably designed to ensure compliance with the BSA. In 2011, Bethex opened its doors to wholesale, commercial MSBs and, by the end of 2012, had established relationships with over 70 money transmitters and check cashing companies. Bethex’s MSB expansion resulted in an increase in volume from $657 million in transactions processed in 2010, all of which were domestic, to over $4 billion in domestic and international transactions processed in 2012 – an annual increase of more than 300%. Although the MSB program had grown to substantial volume and scope, Bethex failed to make commensurate changes in compliance controls to account for the money laundering and terrorist financing risks posed by those MSBs, many of which were located in high-risk jurisdictions overseas. For the level of funds transfer activity at Bethex, which generated significant fee income for the institution, it should have had a robust AML and transaction monitoring program. Instead, Bethex’s program remained tailored to primarily low and middle income individual account holders in New York.

a. Risk Assessment

From 2011 through 2012, Bethex failed to conduct a risk assessment that incorporated all of its products and services including wire transfers processed for its domestic and international MSB accounts. Bethex processed transactions for MSB customers in over 30 countries, including jurisdictions with high money laundering risks such as Mexico, Ghana, Bangladesh,
China, Pakistan, and South Korea. Bethex failed to conduct any risk assessment in 2011 and conducted an inadequate risk assessment in 2012 because it did not assess the risk of its MSB clients. An operational and organizational risk assessment is a vital part of a compliance program, as it permits the financial institution to assess the particular risks posed by its business lines, practices, and clientele and establish appropriate controls to mitigate those risks. Bethex’s failure to conduct an adequate risk assessment left Bethex ill-equipped to implement necessary AML controls when its MSB transaction activity nearly quadrupled from $1.3 billion in 2010, to $2.7 billion in 2011, and finally to $4.0 billion in 2012.

b. Due Diligence

Bethex did not perform the due diligence necessary on its MSBs to determine the money laundering risks or their expected volume and pattern of activity. Bethex failed to require and maintain documentation to identify the business type, use, and associated business partners of its MSBs and did not provide for annual or periodic monitoring and updating. For instance, Bethex maintained four MSB accounts that shared the same address in an office suite. Each of the accounts belonged to a U.S.-based shell company subsidiary of a Mexican MSB, but Bethex failed to appropriately identify and incorporate this information into its monitoring system. By not knowing its customers and their profiles, Bethex was incapable of understanding MSB transactional behavior and was unable to place them under appropriate monitoring for suspicious activities.

---

3 At the time of the MSB activity, Mexico, Ghana, Bangladesh, China, Pakistan, and South Korea were classified by the United States Department of State as “Countries of Primary Concern” or “Countries of Concern” in the 2012 United States Department of State International Narcotics Control Strategy Report, which classifies countries based on money laundering risk. See http://www.state.gov/documents/organization/185866.pdf.
c. Transaction Monitoring

Bethex failed to implement an effective suspicious activity monitoring system relative to the scale and scope of the currency and electronic funds transmission activity conducted on behalf of its MSBs. Bethex did not assign its MSB members a proper risk category. It failed to implement enhanced monitoring on higher risk entities to adequately monitor for and detect suspicious activity. These failures exposed the U.S. financial system to serious risks of money laundering.

Bethex also failed to maintain an adequate level of staffing to ensure it could effectively monitor its MSB customers. In 2011, Bethex had 22 full-time employees for the entire Credit Union, many of which Bethex assigned to handle the operational side of its wholesale MSB activity. Its independent auditor notified Bethex that 22 full-time employees were insufficient to handle the AML risks of processing the $657 million in transactions conducted during 2010. In response, Bethex increased its staff by four people. But, at the same time, transactions had increased annually from $657 million to over $4 billion, due in large part to transactions that Bethex processed for wholesale MSBs. Bethex failed to maintain sufficient staff necessary to monitor the significant amount of wholesale MSB transactions. At the same time, customers engaged in dramatically increasing volumes of transactions at increasing average amounts per transaction.

2. Designation of BSA Compliance Officer

A credit union is required to designate a person responsible for ensuring day to day compliance with BSA requirements. 31 C.F.R. § 1020.210. Bethex failed to designate a person who was technically competent to oversee ongoing compliance efforts for the risks and scope of the products and services it provided and the customers it served.
Bethex failed to ensure that its BSA officer had sufficient experience, authority, and resources to ensure day-to-day compliance with the BSA. From 2011 to 2012, Bethex’s designated BSA compliance officer maintained multiple different roles at the Credit Union including its Chief Operating Officer and business manager of the MSB relationship and funds transfer operations. While having a BSA compliance officer fill multiple roles in a smaller institution is not a violation, as the amount of transactions grew to over $4 billion annually, Bethex’s BSA compliance officer was unable to adequately fulfill his multiple responsibilities to assure BSA compliance. Despite receiving repeated notification from independent auditors and the NCUA of deficiencies in its AML program, Bethex did not take steps to address its deficiencies until years after the fact. For example, Bethex’s own annual independent BSA audit in March 2011 identified lack of internal controls to detect structuring, an overdue BSA risk assessment, insufficient know your customer or customer due diligence policies for Bethex-serviced MSBs, and no written process to determine high-risk accounts. Its August 2012 audit identified those same deficiencies over a year later. This audit also put Bethex on notice that it had failed to develop adequate written procedures for wire transfers and lacked protocols to detect and report illicit wire transactions. These items continued to remain outstanding several months later when the NCUA conducted its examination of Bethex. For over two years, Bethex’s leadership allowed significant AML compliance concerns to persist without taking sufficient steps to address the deficiencies.

In addition, given Bethex’s reliance on the proceeds generated by the MSB business and the BSA compliance officer’s additional role as business manager of the MSB customers, a conflict of interest that was not sufficiently mitigated degraded the BSA compliance officer’s ability to evaluate whether clients were engaged in reportable suspicious activity, including
layering and structuring. For example, Bethex employees’ willingly disregarded internal controls in order to complete transactions for large, revenue generating customers over which the BSA officer was the business manager. Specifically, Bethex had written controls that limited the value of wire transfers conducted on behalf of a customer in a business day. To avoid these limits for its high-revenue generating customers, Bethex would send multiple wires below its internal control limit from the same originator to the same beneficiary on the same day.

B. Suspicious Activity Reporting Violations

The BSA and its implementing regulations impose an obligation on financial institutions to report transactions that involve or aggregate to at least $5,000, that are conducted by, at, or through the institution, and that the institution “knows, suspects, or has reason to suspect” are suspicious. 31 U.S.C. § 5318(g) and 31 C.F.R. § 1020.320. A transaction is “suspicious” if the transaction: (1) involves funds derived from illegal activities or is intended or conducted to hide or disguise funds or assets derived from illegal activities; (2) is designed to evade any requirement in the BSA or regulations implementing the BSA; or (3) has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including background and possible purpose of the transaction. 31 C.F.R. §§ 1020.320(a)(2)(i)–(iii).

Bethex failed to timely detect and report suspicious activity to FinCEN. In 2013, Bethex late-filed 28 SARs as a result of a look back. The look-back covered the period from January 2010 to March 2013. The majority of the suspicious activity underlying these SARs involved high-volume, large amount transfers by MSBs capable of exploiting Bethex’s AML weaknesses.
Some MSB customers also wired large volumes of funds to foreign jurisdictions with a high risk of money laundering, terrorism or drug trafficking, including Mexico, Pakistan and Yemen.4

In addition, the majority of the 28 late-filed SARs were inadequate. The SARs contained short, vague narratives that broadly summarized multiple and unrelated instances of suspicious activity. For example, one SAR described suspicious transactions involving amounts that aggregated to over $906 million. The overuse of boilerplate language and lack of sufficient detail in this SAR provided little benefit to law enforcement investigations. Broad summary SARs with poor-quality narratives such as these, reduce the value of the suspicious activity reporting.

III. CIVIL MONEY PENALTY

FinCEN has determined that Bethex willfully violated the program and reporting requirements of the BSA and its implementing regulations, and that grounds exist to assess a civil money penalty for these violations. 31 U.S.C. § 5321 and 31 C.F.R. § 1010.820. FinCEN has determined that the appropriate penalty in this matter is $500,000.

/s/                       12/14/16
Jamal El-Hindi          Date
Acting Director
FINANCIAL CRIMES ENFORCEMENT NETWORK
U.S. Department of the Treasury

---

4 At the time of the MSB activity, Mexico, Pakistan, and Yemen were classified by the United States Department of State as “Countries of Primary Concern” or “Countries of Concern” in the 2012 United States Department of State International Narcotics Control Strategy Report, which classifies countries based on money laundering risk. See http://www.state.gov/documents/organization/185866.pdf.