# BSA/AML/OFAC COMPLIANCE ESSENTIALS FOR FIDUCIARIES

TRI-STATE TRUST CONFERENCE

FARGO, ND – APRIL 24, 2025

PRESENTED BY

JEFFREY KROPSCHOT – PRESIDENT, KROPSCHOT CONSULTING PARTNERS

KROPSCHOT CONSULTING PARTNERS EXPERTISE PARTNERSHIP SOLUTIONS

## AGENDA

- Anti-Money Laundering History
- Anti-Money Laundering Program Requirements
- Customer Identification Program Requirements
- OFAC Regulations, Reporting and Compliance Program Expectations
- Suspicious Activity Monitoring
- Money Laundering Red Flags
- Suspicious Activity Reporting
- USA Patriot Act Section 314(a) – FinCEN Information Requests
- USA Patriot Act Section 314(b) - Voluntary Information Sharing
- BSA/AML/OFAC Fines and Penalties
- Questions

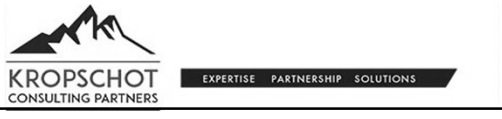
KROPSCHOT CONSULTING PARTNERS EXPERTISE PARTNERSHIP SOLUTIONS

## ANTI-MONEY LAUNDERING LAW HISTORY

- Bank Secrecy Act (1970) - 31 USC 5311 et seq
- Money Laundering Control Act (1986)
- Anti-Drug Abuse Act (1988)
- Annunzio Wylie Anti-Money Laundering Act (1992)
- Money Laundering Suppression Act (1994)
- Money Laundering and Financial Crimes Strategy Act (1998)
- USA Patriot Act (2001)
- Intelligence Reform & Terrorism Prevention Act (2004)
- Anti-Money Laundering Act (2020)


## ANTI-MONEY LAUNDERING PROGRAM REQUIREMENTS 31 CFR 1020.210 (Based on proposed regulatory updates)

- Must establish, implement, and maintain an effective, risk-based, and reasonably designed Anti-Money Laundering (AML)/Countering the Financing of Terrorism (CFT) program, which focuses attention and resources in a manner consistent with the institution's risk profile, which takes into account higher-risk and lower-risk customers and activities and must, at a minimum:
  - Establish a risk assessment process that serves as the basis for the AML/CFT program;
  - Reasonably manage and mitigate money laundering, terrorist financing, and other risks through internal policies, procedures, and controls commensurate with those risks and ensure compliance with the Bank Secrecy Act and related implementing regulations;
  - Designate one or more qualified individuals to be responsible for coordinating and monitoring day-to-day compliance;
  - Include an ongoing employee training program;
  - Include independent, periodic AML/CFT program testing to be conducted by a qualified internal or outside party; and
  - Include appropriate risk-based procedures for conducting ongoing customer due diligence.



# CUSTOMER IDENTIFICATION PROGRAM
# 31 CFR 1020.220 (a)(1)

- A bank required to have an AML/CFT program must implement a written Customer Identification Program (CIP) appropriate for the bank's size and type of business that, at a minimum, addresses each of the following:
  - Identity verification procedures
  - Recordkeeping
  - Comparison with government lists
  - Customer notice requirements
  - Reliance on another financial institution
- The CIP must be a part of the AML/CFT compliance program.


# CIP - IDENTITY VERIFICATION PROCEDURES
# 31 CFR 1020.220 (a)(2)

- The CIP must include risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable.
- The procedures must enable the bank to form a reasonable belief that it knows the identity of each customer.
- These procedures must be based on the bank's assessment of relevant risks
  - Various types of accounts maintained by the bank
  - Various methods of opening accounts provided by the bank
  - Various types of identifying information available
  - Bank's size, location, and customer base

## CIP - IDENTITY VERIFICATION PROCEDURES (Cont.) 31 CFR 1020.220 (a)(2)

- Annual BSA/AML risk assessment generally involves the identification of specific risk categories unique to the bank, which may include the following:
  - Products
  - Services
  - Customers
  - Geographic Locations

KROPSCHOT CONSULTING PARTNERS EXPERTISE PARTNERSHIP SOLUTIONS

## CIP - IDENTITY VERIFICATION PROCEDURES 31 CFR 1020.220 (a)(2)(i) AND (ii)

- The CIP must contain procedures for account opening, specifying information to be obtained from each customer. The following minimum information must be obtained, prior to account opening:
  - Name
  - Date of birth, for an individual
  - Address
  - Identification number
- The CIP must contain procedures for verifying the identity of the customer, using information obtained above, within a reasonable time after the account is opened. The procedures must describe when the bank will use documentary methods, non-documentary methods, or a combination of both methods

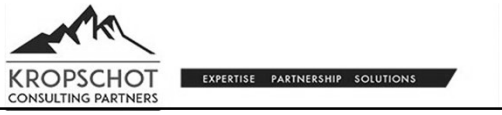
KROPSCHOT CONSULTING PARTNERS EXPERTISE PARTNERSHIP SOLUTIONS

## CIP - IDENTITY VERIFICATION PROCEDURES 31 CFR 1020.220 (a)(2)(iii)

- The CIP must include procedures for responding to circumstances in which the bank cannot form a reasonable belief that it knows the true identity of a customer. These procedures should describe:
  - When the bank should not open an account;
  - The terms under which a customer may use an account while the bank attempts to verify the customer's identity;
  - When the bank should close an account, after attempts to verify a customer's identity have failed; and
  - When the bank should file a Suspicious Activity Report in accordance with applicable law and regulation.


## CIP - IDENTITY VERIFICATION PROCEDURES PARTIES SUBJECT TO CIP

- Investment Management Agency or Investment Advisory Accounts
  - For individual(s) – Account owner(s)
  - For a trust – Trustee(s) and a trustee certification
  - For an entity – Entity and key individuals
- Employee Benefit Plan
  - Plan (not participants) – Entity and key Individuals
- IRAs and Custodial Accounts – Account owner(s)
- Revocable Trust
  - Trust, Grantor(s) and Trustee(s) other than own bank



## CIP - IDENTITY VERIFICATION PROCEDURES PARTIES SUBJECT TO CIP (Cont.)

- Irrevocable Trust
  - Trust, and Trustee(s) other than own bank
- Guardianship/Estates – Co-Guardian(s) and Co-Personal Rep(s)

KROPSCHOT CONSULTING PARTNERS EXPERTISE PARTNERSHIP SOLUTIONS

## OFFICE OF FOREIGN ASSETS CONTROL (OFAC) 31 CFR 500-599

- OFAC is an office of the Treasury that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted individuals and entities
- All U.S. persons, including U.S. banks, bank holding companies, and nonbank subsidiaries, must comply with OFAC's regulations
- The regulations that OFAC administers require banks to:
  - Block/freeze accounts/property of certain countries, entities, and persons
  - Prohibit or reject unlicensed transactions with specified countries, entities, and individuals
- Regulations outline reporting, procedures and penalties related to economic sanctions regulations

KROPSCHOT CONSULTING PARTNERS EXPERTISE PARTNERSHIP SOLUTIONS

## OFAC REPORTING

- Banks must report all blockings to OFAC within 10 business days of the occurrence and annually by September 30 concerning those assets blocked (as of June 30). Once assets or funds are blocked, they should be placed in a separate blocked account
- Prohibited transactions that are rejected must also be reported to OFAC within 10 business days of the occurrence
- Blocked property records must be kept for the period the property is blocked and five years thereafter. Must keep a record of each rejected transaction for five years.

KROPSCHOT CONSULTING PARTNERS EXPERTISE PARTNERSHIP SOLUTIONS

## OFAC COMPLIANCE PROGRAM

- While not required by specific regulation, but as a matter of sound banking practice and in order to mitigate the risk of noncompliance with OFAC requirements, banks should establish and maintain an effective, written OFAC compliance program that is commensurate with their OFAC risk profile (based on products, services, customers, and geographic locations).
- The compliance program should identify higher-risk areas and provide for the following:
  - A risk assessment process that serves as the basis for the OFAC compliance program;
  - Internal policies, procedures, and controls commensurate with those risks and ensure compliance with applicable laws and regulations;
  - One or more qualified individuals to be responsible for coordinating and monitoring day-to-day compliance;
  - An ongoing employee training program; and
  - Independent, periodic compliance testing to be conducted by a qualified internal or outside party.

KROPSCHOT CONSULTING PARTNERS EXPERTISE PARTNERSHIP SOLUTIONS

# SUSPICIOUS ACTIVITY MONITORING

- Know your customer (Benchmarking to know what is "normal")
  - Age, health and lifestyle
  - Risk tolerance
  - Client needs, wants and preferences
  - Family relations
  - Geographic location
  - Employment
  - Challenges (addictions, criminal past, money issues)
- Expected transactions
  - Frequency
  - Amount
  - Purpose


# SUSPICIOUS ACTIVITY MONITORING (CONT.)

- Must use available resources to monitor account activity to identify patterns of unusual volume, size, pattern or type of transactions. Resources used may include the following:
  - Suspicious activity reports (large one-day transactions, as well as frequency and velocity alerts)
  - Daily transaction reports
  - Wire transfer activity reports
  - Administrative accounts reviews
  - Investment account reviews
  - Regular calls and communication with clients.
- When the trust company or trust department identifies what it deems to be unusual account activity, the transactions will be reviewed in the context of other account activity to determine whether a transaction cannot be explained or is suspicious in nature

## MONEY LAUNDERING RED FLAGS

- The client exhibits unusual concern about the firm's compliance with government reporting requirements and the firm's AML policies, particularly on his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspect identification or business documents
- The client wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the client's stated business or investment strategy
- The client causes difficulties and delays in obtaining copies of governing documents or other documents of incorporation


## MONEY LAUNDERING RED FLAGS (Cont.)

- Upon request, the client refuses to identify or fails to indicate any legitimate source for his or her funds and other assets
- The information provided by the client that identifies a legitimate source for funds is false, misleading, or substantially incorrect
- The client (or a person publicly associated with the client) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations
- The client has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry

## MONEY LAUNDERING RED FLAGS (Cont.)

- The client conducts multiple and/or separate transactions for less than $10,000 despite a clear relationship to one another
- The client deposits money and purchases long-term investments, but shortly thereafter submits a request to liquidate the position and/or deplete the account and transfer the proceeds out of the account, especially when directed to a third party and/or foreign country
- The client's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity

KROPSCHOT CONSULTING PARTNERS EXPERTISE PARTNERSHIP SOLUTIONS

## MONEY LAUNDERING RED FLAGS (Cont.)

- The client's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
- The client's account has wire transfers that have no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven
- The client's account indicates large or frequent wire transfers, immediately withdrawn without any apparent business purpose
- The client makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose

KROPSCHOT CONSULTING PARTNERS EXPERTISE PARTNERSHIP SOLUTIONS

## MONEY LAUNDERING RED FLAGS (Cont.)

- The client requests that a transaction be processed to avoid the firm's normal documentation requirements
- The client's account shows an unexplained high level of account activity with very low levels of securities transactions
- The client's account has inflows of funds or other assets well beyond the known income or resources of the customer

KROPSCHOT CONSULTING PARTNERS EXPERTISE PARTNERSHIP SOLUTIONS

## SUSPICIOUS ACTIVITY REPORTING - GENERAL 12 CFR 21.11 (OCC) AND 12 CFR 353 (FDIC)

- An institution shall file a suspicious activity report (SAR) with the appropriate federal law enforcement agencies and the Treasury in the following circumstances:
  - Insider abuse involving any amount
  - Transactions aggregating $5,000 or more where a suspect can be identified
  - Transactions aggregating $25,000 or more regardless of potential suspects
  - Transactions aggregating $5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act.

KROPSCHOT CONSULTING PARTNERS EXPERTISE PARTNERSHIP SOLUTIONS

## SUSPICIOUS ACTIVITY REPORTING - GENERAL 12 CFR 21.11 (OCC) AND 12 CFR 353 (FDIC) (Cont.)

- Must file a SAR no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for its filing
- If no suspect was identified on the date of detection of the incident requiring the filing, an institution may delay filing a SAR for an additional 30 calendar days to identify a suspect. In no case shall reporting be delayed more than 60 calendar days
- An institution shall maintain a copy of any SAR filed and any supporting documentation for five years from the SAR filing date
- Management shall promptly notify its board of any SAR filed; SARs are confidential


## USA PATRIOT ACT SECTION 314(a)

- The Financial Crimes Enforcement Network (FinCEN) receives requests from law enforcement and upon review, sends notifications to designated contacts within financial institutions across the country every 2 weeks informing them new information has been made available via a secure website
- The requests contain subject and business names, addresses, and as much identifying data as possible to assist the financial industry in searching their records
- Financial institutions must query their records for data matches, including accounts maintained by the named subject during the preceding 12 months and transactions within the last 6 months
- Institutions generally have 2 weeks to respond with any positive matches

## USA PATRIOT ACT SECTION 314(b)

- Section 314(b) provides financial institutions with the ability to share information with one another, under a safe harbor that offers protections from liability, in order to better identify and report activities that may involve money laundering or terrorist activities
- Participation in information sharing is voluntary
- To rely on the safe harbor, an institution need not have specific information indicating that the activity directly relates to money laundering or terrorist activities, nor have reached a conclusive determination that the activity is suspicious. A reasonable belief that the information shared relates to activities that may involve money laundering or terrorist activity is sufficient.


## BSA/AML/OFAC FINES AND PENALTIES

- **2022-03-17** – USAA Federal Savings Bank (FSB) ordered to pay $140 million as part of two separate consent orders reached with the Financial Crimes Enforcement Network (FinCEN) and Office of the Comptroller of the Currency (OCC) for the bank's "willful" failure to implement and maintain a Bank Secrecy Act/anti-money laundering (BSA/AML) compliance program.
- USAA FSB admitted it willfully failed to implement and maintain an AML program that met the minimum requirements of the BSA. Inadequacies included:
  - Internal controls and risk management practices
  - Suspicious activity identification, evaluation, and reporting
  - Staffing and training
  - Third-party risk management

## BSA/AML/OFAC FINES AND PENALTIES

- **2024-10-10** – TD Bank was ordered to pay more than $3 billion in combined penalties levied by the US Department of Justice, Financial Crimes Enforcement Network, Office of the Comptroller of the Currency and the Federal Reserve. Specifically, TD Bank failed to develop and provide for the continued administration of a BSA/AML Program reasonably designed to assure and monitor compliance with the Bank Secrecy Act and its 2 implementing regulations.

- Deficiencies in the Bank's BSA/AML Program included:
  - Internal controls and risk management practices, including risk assessments
  - Customer due diligence and customer risk ratings
  - Suspicious activity identification, evaluation, and reporting
  - Governance
  - Staffing, independent testing and training



## KEY BSA/AML/OFAC LAWS AND REGULATIONS

- Bank Secrecy Act (31 USC 5311- 5330)
- USA Patriot Act (various sections of USC)
- OCC Rules (12 CFR 21 and 163)
  - BSA/AML compliance program requirement (12 CFR 21.21)
  - Suspicious Activity Reports (12 CFR 21.11 and 163.180)
- FinCEN Rules (31 CFR 1010 and 1020 et.al.)
  - Anti-money laundering programs (31 CFR 1020.210)
  - Customer identification programs (31 CFR 1020.220)
  - Suspicious Activity Reports (31 CFR 1020.320)
- Office of Foreign Assets Control (31 CFR 500)