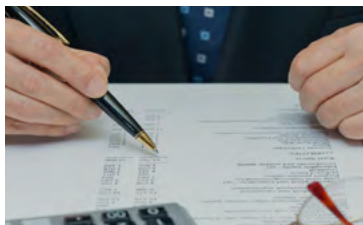


WHITE PAPER

Factors to Consider When Developing Procedures for FinCEN 314(a) Requests



Succeed. Transform. Compute. Perform.



The USA PATRIOT Act requires risk identification, measurement, monitoring, controlling and reporting. Section 314(a) mandates information sharing between law enforcement agencies and financial institutions through the Financial Crimes Enforcement Network, or FinCEN.

Factors to Consider When Developing Procedures for FinCEN 314(a) Requests

OVERVIEW

Many financial institutions continue to be challenged in developing robust policies, procedures and systems of internal control to meet specific requirements as outlined by the competent authorities in support of BSA/AML Compliance. Regulators continue to focus their attention on key areas of the BSA/AML Compliance Program to ensure that such risks are adequately identified, measured, monitored, controlled and reported. One such area of focus is Section 314(a) of the USA PATRIOT Act, Information Sharing between federal law enforcement agencies and financial institutions.

Section 314(a) of the USA PATRIOT Act and 31 C.F.R. Part § 1010.520 grant the Financial Crimes Enforcement Network ("FinCEN") the authority to require that each financial institution, expeditiously search its records to determine whether it maintains or has maintained any accounts for, or engaged in specified transactions with, each individual entity or organization named in FinCEN's request. A federal law enforcement agency investigating terrorist activity or money laundering may request that FinCEN solicit, on the investigating agency's behalf, certain information from financial institutions. Upon receiving the requisite certification from the requesting federal law enforcement agency, FinCEN may require the financial institution to search its records to determine whether it maintains or has maintained an account for, or has engaged in a transaction with, any specified individual, entity or organization.

DESIGNATION OF CONTACT PERSON

Each financial institution must have designated points of contact regarding Section 314(a) requests ("FinCEN 314(a) Requests") and provides FinCEN with the name, title, mailing address, e-mail address, telephone number and facsimile number for registration purposes. The institution should also promptly notify FinCEN of any changes to such designation or contact information.

NOTIFICATION OF FINCEN 314(A) REQUEST

The designated points of contact at the institution, as registered users, are notified by FinCEN of all FinCEN 314(a) Requests via the Secure Information Sharing System ("SISS"). Once notified, designated contact

person or other registered representative of the institution accesses the SISS website (<https://www.fincen.gov/314a/>) and downloads the current FinCEN 314(a) Request. Since FinCEN normally transmits FinCEN 314(a) Requests every other Tuesday, the designated contact person or other registered representative of the institution should access the SISS at least once every two weeks regardless of whether FinCEN notifies the financial institution that a FinCEN 314(a) Request is available.

RECORD SEARCH

Upon receipt of a FinCEN 314(a) Request, financial institutions are normally required to conduct a one-time search of its records to identify any current account, or any account maintained in the last twelve (12) months, for a named suspect and to identify any transaction conducted outside of an account by or on behalf of a named suspect during the preceding six (6) months. The records that must be searched are specified in the FinCEN 314(a) Request, and the financial institution should perform the search according to the specified parameters if different from those normally utilized.

REVIEW OF POTENTIAL MATCHES

In order to determine whether a potential hit is a false positive or a positive match, the institution should consider all relevant information related to the customers, including, but not limited to: name, street address, city, state, country, and any unique identifiers (i.e., social security number, employer identification number, tax identification number, passport number, etc.). The institution may utilize certain rules to determine the appropriate classification of any potential hit related to an entity or organization.

REPORTING POSITIVE MATCHES TO FINCEN

Positive matches must be sent to FinCEN using the SISS on or before the designated response date, which is normally fourteen (14) calendar days after the request is transmitted.

As a prudent internal control measure, the institution should confirm that all searches have been completed prior to reporting positive matches to FinCEN because the SISS does not permit edit responses once they are submitted. The institution should retain a confirmation and a FinCEN 314(a) Search Self-Verification from the SISS that it has responded to the FinCEN 314(a) Request and that the response was made in a timely manner. Once the confirmation and self-verification from the SISS has been obtained, the institution should also notify management, (i.e. Chief Compliance Officer) that the institution has responded to the FinCEN 314(a) Request.

ESCALATION OF POTENTIAL MATCHES FOR INVESTIGATION

If the institution reports a positive match to a FinCEN 314(a) Request, it should also escalate the positive match information and all relevant information to management, typically the Chief Compliance Officer.

CONFIDENTIALITY OF FINCEN 314(A) REQUESTS

Financial Institutions are prohibited from using information provided by FinCEN for any purpose other than:

- Reporting to FinCEN as provided in this section;
- Determining whether to establish or maintain an account, or to engage in a transaction; or
- Assisting the institution in complying with any requirement of 31 C.F.R. Part 103.

Therefore, the persons responsible for reviewing the lists and following up on potential matches should use discretion to maintain the confidentiality of FinCEN 314(a) Requests. In order to protect the confidentiality of the FinCEN 314(a) Requests, all search results, the FinCEN 314(a) Log and any supporting documentation should be stored either in a protected folder, if stored electronically, or in a secured file location, if retained in physical files.

DOCUMENTATION AND RECORD RETENTION

The financial institution should document the results of all searches utilizing the FinCEN 314(a) Log, which contains the tracking number, the date of the search, any potential hits identified during the search, the resolution of any potential hits, the number of positive matches identified and the date reported to FinCEN.

While there are no specific recordkeeping requirements concerning 314(a) Requests, appropriate documentation of the request and record search should be maintained for a reasonable time period to provide for an effective and thorough audit trail. In accordance with Bank Secrecy Act record retention requirements and the recommended retention period indicated in FinCEN 314(a) FAQs, institutions should maintain all FinCEN 314(a) Request files for five (5) years.