Collaborate with Confidence

Your Guide to 314(b) Collaboration

VERAFIN
A STEP AHEAD

Sections

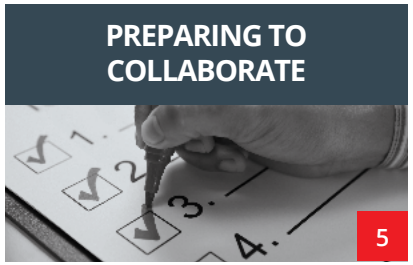


TABLE OF CONTENTS

Introduction

Banks and credit unions offer their customers a wide range of products from accounts to online services to meet their everyday banking needs. However, with the rapidly-progressing and ever-changing financial landscape also come evolving methods of financial crime.

Criminals take advantage of new products, services and technologies, and can target multiple institutions to conceal their illegal activities. By using several institutions to mask their activity, criminals make it difficult for institutions to detect suspicious activity and even harder to catch the "customers" who are perpetrating schemes that span institutions.

One of the best defenses that an institution has is simply reaching out to other institutions to collaborate and to share information.

Section 314(b) of the USA PATRIOT Act permits financial institutions to share information with one another. When institutions work together, they can learn more about their customers' activity across institutions, they can uncover more suspicious activity, and ultimately, they can prevent more losses for their institution.

SECTION 1

Information Sharing Encouraged

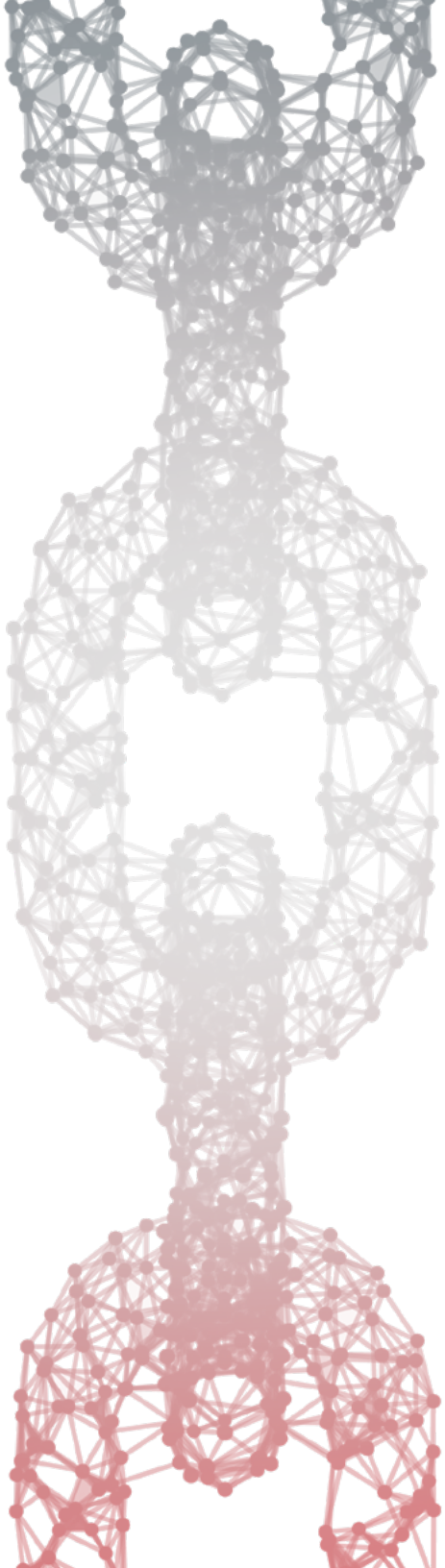
On January 1, 2021, the National Defense Authorization Act (NDAA) and the Anti-Money Laundering Act of 2020 became law. The AML Act may introduce profound changes to the BSA/AML regime, including important changes designed to reinforce information sharing.

Section 6002 of the AML Act defines the purpose of the Act:

"(1) To improve coordination and information sharing among the agencies tasked with administering anti-money laundering and countering the financing of terrorism requirements, the agencies that examine financial institutions for compliance with those requirements, Federal law enforcement agencies, national security agencies, the intelligence community, and financial institutions."

Financial institutions conducting AML/CFT investigations are strongly encouraged to engage in information sharing for efficient and effective investigations identifying a complete picture of potentially suspicious activity.

"The conference agreement also opens avenues for more data sharing among financial institutions and within financial institutions and their affiliates, while retaining key security safeguards, so that patterns of suspicious activities will be more easily identified, tracked, and shared appropriately." [1]



SECTION 2

USA PATRIOT Act & Section 314(b)

USA PATRIOT Act Section 314

According to the USA PATRIOT Act website, Section 314 is about **"Cooperative Efforts to Deter Money Laundering."**[2]

Both Section 314(a) and Section 314(b) are about information sharing:

Section 314(a) contains procedures for information sharing between law enforcement and financial institutions which allows them "to reach out to more than 34,000 points of contact at more than 14,000 financial institutions to locate accounts and transactions of persons that may be involved in terrorism or money laundering".[3]

Section 314(b) complements 314(a) by providing "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".[4]

By joining forces and collaborating, institutions who share information can identify and report suspicious activity. The ultimate goal of these cooperative efforts between regulators, law enforcement, and financial institutions is to detect and prevent financial crime.

Section 314(b): Intent to Engage

"To avail itself of this statutory safe harbor from liability, a financial institution or an association must notify FinCEN of its intent to engage in information sharing and that it has established and will maintain adequate procedures to protect the security and confidentiality of the information."[5]

What is safe harbor?

Safe harbor means protection under the law.

Section 314(b) protects financial institutions from civil liability and allows them to share information in conjunction with current laws.

The safe harbor does not extend to sharing information across international borders.

Under the safe harbor, an FI may share information related to transactions suspected to involve the proceeds of Specified Unlawful Activities (SUAs).[6]

SECTION 3

Notifying FinCEN

As stated on the Section 314(b) Fact Sheet,
"Participation in information sharing pursuant to Section 314(b) is voluntary, and FinCEN strongly encourages financial institutions to participate." [7]

Who can participate?

Financial institutions subject to an anti-money laundering program requirement under FinCEN regulations, and any association of such financial institutions, are eligible to share information under Section 314(b). According to FinCEN, an association of financial institutions is "a group or organization the membership of which is comprised entirely of financial institutions." [8]

Notification process

You must first notify FinCEN of your intention to participate in 314(b) information sharing. Notification can be completed online after first registering for FinCEN's Secure Information Sharing System (SISS).

Notification is simple.

After logging in to your FinCEN SISS account:

1. Select the 314(b) tab.
2. Click the *Opt In* button.
3. Complete the required fields.

You will need:

- ✓ Information about your financial institution including EIN and Federal Regulator.
- ✓ Your contact information as a 314(b) contact at your institution.

For audit/exam purposes:
Retain a copy of the email acknowledgment received from FinCEN to voluntarily share information.

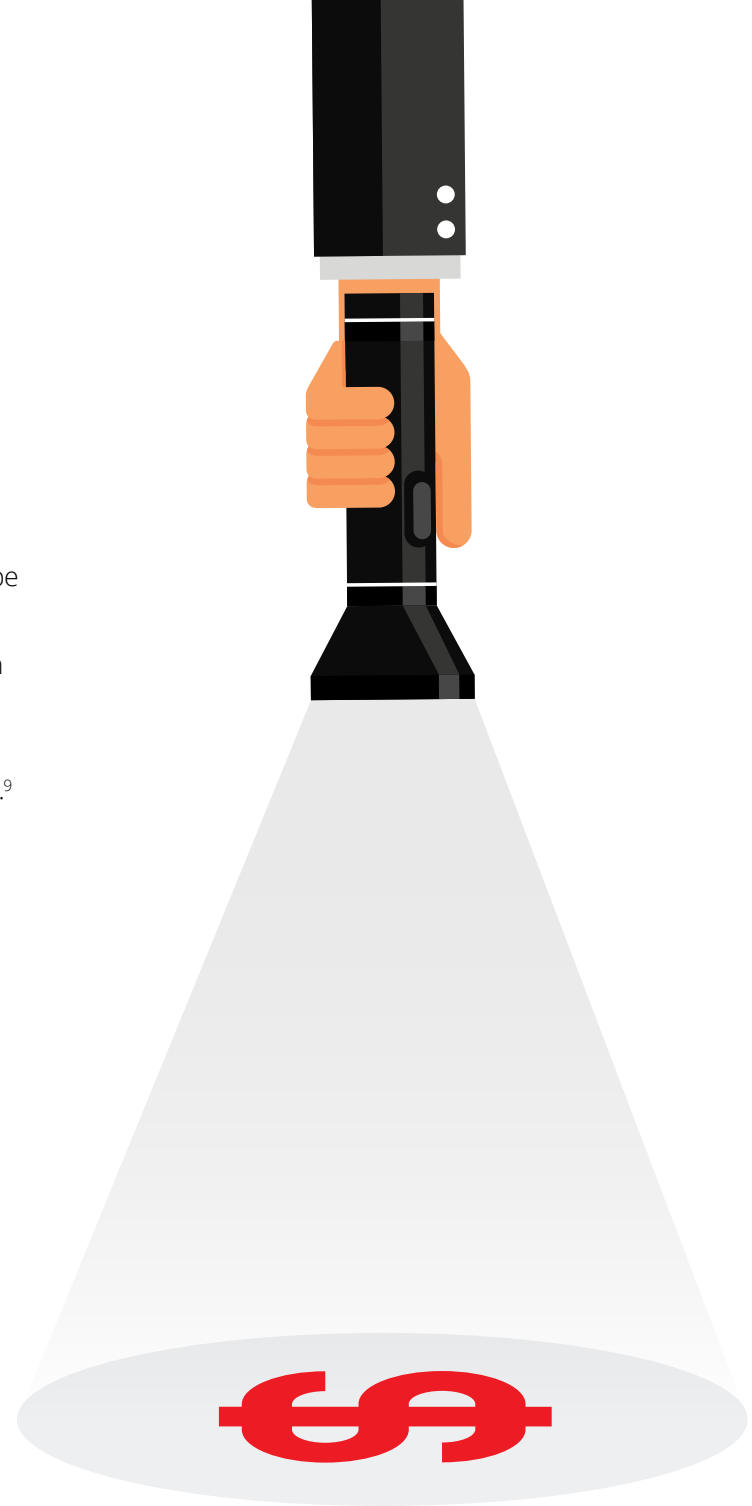
SECTION 3

Notifying FinCEN

Updated Fact Sheet - December 2020

The Fact Sheet was updated December 2020 to reflect several changes to FinCEN guidance, providing three clarifications on the Safe Harbor Provision:

1. A financial institution may share information relating to activities that are suspected to be terrorist financing or money laundering, even if it does not constitute a "transaction".[9]
2. An entity that operates as an association of a financial institution may share information under 314(b). This includes compliance service providers.[9]
3. An unincorporated association governed by a contract among the group of financial institutions that constitutes the institution's members may share information under 314(b).[9]



SECTION 3

Notifying FinCEN

How does my FI participate?

Financial institutions are permitted to share information upon providing notice to FinCEN. If a financial institution decides to participate in Section 314(b) information sharing, the institution must designate at least one person as the 314(b) contact. Multiple contacts can be added for the institution; however, each contact person must complete the notification process.

A contact person's notification is valid for a period of one year from the date on the notification form. 314(b) notification must be renewed every year.

Why participate?

Section 314(b) helps institutions comply with anti-money laundering/counter-terrorist financing (AML/CFT) requirements.

Open communication and collaboration between institutions helps increase awareness of suspicious activity that spans institutions.

SECTION 4

The Power of Collaboration

5 Benefits of 314(b) Collaboration

Here are 5 advantages of connecting with peers to communicate and collaborate. Working together under 314(b) can:

1. Increase compliance with AML/CFT requirements.
2. Help discover information about customers and transactions suspected of being related to money laundering, terrorist financing activity, and SUAs.
3. Give a better view of customer activity/transactions at your financial institution and an expanded view of customer activity that spans institutions.
4. Make more informed decisions, for example:
   - » Whether to establish a new account or to maintain an account.
   - » Whether the institution should engage in a transaction.
5. Assist an FI with investigations and with "SAR file" or "no file" decisions. In the case where an FI decides to file a SAR, their reports are stronger — the FI has more information about the customer/transactions/suspicious activity because of collaboration with another financial institution.

Power of communication: local groups & compliance meetings

Financial institutions often meet to collaborate about activity in their local area.

Representatives from each FI who participate in these local/compliance groups must individually send their notification for Section 314(b) so they can openly share and learn about local activity during group meetings.

There has been a 19.7% increase in the number of financial institutions filing SARs with 314(b) referenced in the narrative, increasing from 979 institutions in 2017 to 1,236 institutions in 2019. [10]

SECTION 4

The Power of Collaboration

Peer Perspective

"We had instances where **we were banking individuals without knowing that they were part of this crime ring,** but by sharing information with other institutions, we were able to figure out what was going on and **prevent further losses** — both for ourselves and others down the road.

These crime rings are successful because they are defrauding institutions of **small amounts over time** and are **hard to detect.** By collaborating through **Verafin** and putting all the pieces together, this particular crime ring proved to be **much larger than any of us thought."** [11]

Randolph-Brooks Federal Credit Union

Location: *Live Oak, TX*
Assets: *$13.3B*

SECTION 4

The Power of Collaboration

Peer Perspective

"We've developed relationships where we've been able to **advise other institutions about trends we're seeing in specific areas** and that's helped them stop criminal activity. And vice versa — they've communicated suspicious behavior, which has helped us i**dentify and stop very risky activity** on our side."

The team's use of **information sharing** recently enabled them to uncover another criminal enterprise — this time affecting multiple financial institutions. In this case, sharing information with other financial institutions **gave the institution access to a wealth of important information that ultimately helped put the criminals behind bars.**

"There was a crime ring involving a number of institutions spread throughout California where we had an unidentified primary suspect. **Through the use of Verafin's communication tools** we were able to identify them. Ultimately, they were arrested." [12]

Case Study from
Financial Institution in California

Assets: *$16.3B*

SECTION 5

Preparing to Collaborate

Policies and Procedures

To comply with Section 314(b), a financial institution must ensure that proper information sharing policies and procedures are in place.

Designate a point of contact.

The contact person is responsible for receiving and providing information. A financial institution can have more than one contact person. In fact, most institutions have at least two people — the primary and secondary contacts.

Document the institution's compliance with Section 314(b).

When your institution decides to partake in 314(b) collaboration, ensure that you update your BSA/AML policies and procedures.

Update your BSA training policy and implement ongoing training for employees.

Ongoing training ensures that employees are aware of the purpose of 314(b) information sharing and the designated contact person.

Establish a process for sending requests and receiving requests.

Make sure that this process includes checking that the other institution has sent their 314(b) notice to FinCEN.

Establish SAR filing decisions when information is learned from information sharing.

The institution must have processes for determining if a SAR will be filed from the information gathered through 314(b) information sharing. All SAR filing decisions and no file decisions must be tracked.

Ensure that all information shared (both requested and received) is safeguarded.

Your institution must have processes in place to keep shared information confidential. It is a good practice to maintain audit logs of all requests that are sent by your institution and the information received in return, and to also track all incoming requests and all your responses to incoming requests.

Ensure 314(b) Registration with other financial institutions.

Financial institutions should review the FinCEN 314(b)-registrants list to verify another institution is a valid participant prior to sending any information. The registrants list is updated in real-time by FinCEN.

SECTION 5

Preparing to Collaborate

What do I have to do *before* I can collaborate and share information?

- ✓ **Always check that the other financial institution(s) has filed 314(b) notification with FinCEN** — Before collaborating or sharing any information with another financial institution, you must verify (or make reasonable efforts to verify) that the other institution and their contact person has filed notification for Section 314(b). FinCEN maintains a list of 314(b) participants where you can check the contact person at another institution. Always check that the other institution has filed a notice to share before collaborating — that is, either sending requests or responding to requests.
- ✓ **Have internal policies in place** — A financial institution must have policies, procedures, and processes in place to document compliance with Section 314(b), have internal controls to maintain the security and confidentiality of shared information that was gained through collaboration, and provide ongoing training so that employees are aware of Section 314(b) and the main point of contact for information sharing.
- ✓ **Suspect that the customer or transaction is suspicious and that the activity is related to money laundering, terrorism financing, or SUAs** — The purpose of Section 314(b) information sharing is to identify activity related to money laundering, terrorist financing or specified unlawful activities. It cannot be used as a way to find out more information about a customer or transaction.

SECTION 6

Collaborate with Confidence

"Information sharing among financial institutions through 314(b) is critical to identifying, reporting, and preventing crime and bad acts.

It is an important part of how we protect our national security. It can also help financial institutions enhance compliance with their AML/CFT requirements". [13]

Kenneth A. Blanco
Former Director, Financial Crimes Enforcement Network

SECTION 6

Collaborate with Confidence

The information that can be shared:

- ✓ Information relating to transactions that the institution suspects may involve the proceeds of one or more specified unlawful activities (SUAs). [14]
- ✓ Information to identify and report activities that may involve terrorist activity or money laundering. [15]
- ✓ Information about individuals, entities, organizations, and countries related to money laundering and terrorist financing activity even if these activities do not constitute a "transaction". [16]
- ✓ If a financial institution shares information under Section 314(b) about the subject of a prepared or filed SAR, the information shared must be limited to the underlying transactions and customer information (not the SAR itself or existence of the SAR). [17]

The information that cannot be shared:

- × A Suspicious Activity Report (SAR) itself
- × The existence or non-existence of a SAR
- × The intent to prepare or to file a SAR
- × Information across international borders

The Money Laundering Control Act includes Specified Unlawful Activities (SUAs) (18 U.S.C. § 1956 and 1957) [18]

Some example SUAs are:

- **Bank Fraud:** defrauding a federally chartered or insured financial institution
- **Fraud and False Statements**: fraudulent bank entries, reports and transactions
- **Fraud and False Statements:** fraud and related activity in connection with identification documents

According to the *FFIEC BSA/AML Examination Manual*, information from another FI may be used to:

- ✓ Identify and, where appropriate, report on money laundering and terrorist activities, and the fraud tied to these criminal activities
- ✓ Determine whether to establish or maintain an account
- ✓ Engage in a transaction
- ✓ Assist in BSA compliance
- ✓ Determine whether to file a SAR

SECTION 6

Collaborate with Confidence

SAR: To file or not to file

The information shared under Section 314(b) can help a financial institution determine whether to file a SAR or not.

If SAR is filed:

If your financial institution decides to file a SAR based on the information learned from collaborating between institutions, ensure that the written SAR Narrative mentions that Section 314(b) information sharing was used and how it helped make the SAR file decision. Reports filed after sharing information are typically more detailed because the financial institution now has a better view of the suspicious activity and the customer/subject conducting or attempting to conduct the activity.

If no SAR is filed:

Information sharing can also help you determine that a SAR is not deemed necessary. Information sharing and collaboration can help you verify whether something is or is not suspicious. However, ensure that the use of Section 314(b) is also documented in the "no file" decision.

Feedback from FinCEN Outreach Meetings

"Banks found the 314(b) process very useful from an investigative perspective. Several banks noted that they often use the 314(b) process throughout the course of a SAR investigation, before filing a SAR, or making a decision to close an account." [19]

Don't divulge the intent to prepare or file a SAR.

Also, don't disclose the existence or non-existence of a SAR and never share a SAR.

SECTION 7

How to request information

The importance of the initial request

When initiating a collaboration request, remember that a strong overall collaboration begins with an informative request.

By providing details and quality information in your outgoing collaboration request, you are increasing the likelihood, speed, and quality of collaboration responses from the other institution.

Remember to:

- ✓ **Provide details** for the entity you are requesting information about.
- ✓ **Be specific** with your questions.
- ✓ **Include the reason** why you are requesting information.
- ✓ **Specify what information** you are looking to learn.

SECTION 7

How to request information

The 5 Ws of requesting information

When reaching out to another institution about an entity, consider the five Ws for starting a strong collaboration.

WHY?

Outline the reasons why you think their activity or transactions are unusual.

Consider the following questions:
Is there any unusual activity or reason for concern? Has an activity or transaction prompted you to start an inquiry or to begin to investigate the customer? If so, what type of investigation have you started?

WHO?

Provide identifying information for the entity.

Consider including the following information:
Individual's name or the name of the business, Tax ID (SSN/EIN), date of birth, occupation, account type and history, and how long they have been a customer.

WHERE?

Indicate the type of activity you are investigating and what you are hoping to learn.

If you are collaborating on a transaction or suspected activity, include relevant information about activities you suspect involve the proceeds of a specified unlawful activity (SUA).

If you are inquiring about an account, provide the account information at your institution.

WHEN?

Provide a brief timeline for the customer's activity.

By providing specific details of when transactions or suspicious activity occurred, the other institution will have a better understanding of the activity you are inquiring about.

WHAT?

Include any information you know about the suspected illicit activity at your institution.

You should ask the other institution additional questions to help clarify the destination or source of the funds.

SECTION 7

How to request information

Sample request for information

Pursuant to Section 314(b) of the USA PATRIOT Act, National Bank would like to initiate a sharing of information request with Red, White & Blue Bank. Lisa Stacks is 314(b) contact at National Bank.

I am requesting information regarding multiple wires from our customer, Andrew Cullum, to a single customer at Red, White & Blue Bank.

Details:

Sender Name: Andrew Cullum
Sender Acct #: a3344-0055-0667
Recipient Name: Lee DeFranco
Receiver Acct # c5566-0044-2345
Wire Amounts: $6500; $8500; $4500
Wire Dates: Jun-1 2015; Jun-2 2015; Jun-4 2016

We are investigating a high volume of wires as listed above, totaling nearly $20,000 transferred to a single receiver. This type of activity is unusual for the customer, and we are investigating this as potential money laundering activity.

Our specific questions are:

- Can you provide any details about the destination or use of funds transferred?
- Do you have any BSA/AML concerns, current or prior, with the receiving customer, or activity being conducted on the account?

TIP: *Consider stating that you are requesting information under Section 314(b) of the USA PATRIOT Act.*

Who?

What?
When?
Where?

Why?

REMEMBER *to specify what information you want to learn.*

Collaboration Checklist

Information sharing checklist

- **Do select** a point of contact and have that individual send notice to FinCEN for Section 314(b) information sharing.
- **Do remember** to resend your 314(b) notification every year. A notice is effective for one year.
- **Do consult** the 314(b) participant list and ensure your point of contact is listed prior to collaborating.
- **Do safeguard** information and use it only for reporting anti-money laundering, counter-terrorism financing, and specified unlawful activities.
- **Do remember** that the information shared must relate to individuals, entities, organizations, or countries suspected of possible money laundering or terrorist financing activity.
- **Do implement** policies and procedures for information sharing.
- **Do note** the use of 314(b) collaboration in the SAR narrative section if you decide to file a SAR.
- **Do train** your employees about 314(b) and make sure they know the designated contact person responsible for sending and receiving information requests.
- **Do follow** best practices when preparing your initial request for information, remembering to be specific and include details on the *who*, *what*, *where*, *when* and *why* of the customer or activity.

Resources & References

References

1 National Defense Authorization Act's (NDAA) accompanying Joint Explanatory Statement
https://docs.house.gov/billsthisweek/20201207/116hrpt617-JointExplanatoryStatement.pdf?source=email

2 USA PATRIOT Act on FinCEN website
https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act

3 Section 314(a) Fact Sheet
https://www.fincen.gov/sites/default/files/shared/314afactsheet.pdf

4, 7, 16 Section 314(b) Fact Sheet
https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf

5, 17 FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual – Voluntary Information Sharing
Section 314(b) of USA PATRIOT Act (31 CFR 1010.540)
https://www.lexissecuritiesmosaic.com/gateway/OCC/Bulletin/other-publications-reports_ffiec-bsa-aml-examination-manual.pdf

6, 14 Guidance on the Scope of Permissible Information Sharing Covered by Section314(b) Safe Harbor of the USA PATRIOT Act
https://www.fincen.gov/sites/default/files/shared/fin-2009-g002.pdf

8 Administrative Ruling Regarding the Participation of Associations of Financial Institutions in the 314(b) Program
https://www.fincen.gov/sites/default/files/shared/FIN-2012-R006.pdf

9 FinCEN Director Emphasizes Importance of Information Sharing Among Financial Institutions
https://www.fincen.gov/news/news-releases/fincen-director-emphasizes-importance-information-sharing-among-financial

10 314(b) Participation and Reporting
https://www.fincen.gov/sites/default/files/shared/314bparticipationinfo.pdf

11 Verafin Case Study, Partners in Fighting Crime, Randolph-Brooks Federal Credit Union
https://download.verafin.com/wp-content/uploads/2021/06/randolph-brooks-case-study-verafin-20210604.pdf

12 Verafin Case Study, California Financial Institution
https://download.verafin.com/wp-content/uploads/2021/06/success-story-california-fi-case-study-verafin-20210604.pdf

13 Kenneth A. Blanco, Former Director, Financial Crimes Enforcement Network
https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-virtually-american-bankers

15 FinCEN Section 314(b) webpage
https://www.fincen.gov/section-314b

18 Specified Unlawful Activities
https://www.justice.gov/sites/default/files/criminal-afmls/legacy/2015/04/24/statutes2015.pdf

19 Financial Institutions Outreach Initiative - Report on Outreach to Large Depository Institutions
https://www.fincen.gov/sites/default/files/shared/Bank_Report.pdf

Verafin is the industry leader in enterprise Financial Crime Management solutions, providing a cloud-based, secure software platform for Fraud Detection and Management, BSA/AML Compliance and Management, High-Risk Customer Management and Information Sharing.

Over 3000 banks and credit unions use Verafin to effectively fight financial crime and comply with regulations. Leveraging its unique big data intelligence, visual storytelling and collaborative investigation capabilities, Verafin significantly reduces false positive alerts, delivers context-rich insights and streamlines the daunting BSA/AML compliance processes that financial institutions face today.

Verafin is the exclusive provider for Texas Bankers Association, Western Bankers Association, Florida Bankers Association, Massachusetts Bankers Association, and CUNA Strategic Services, with industry endorsements in 48 U.S. states.

Updated: July 2021

For more information, contact us today.

Visit **www.verafin.com,**
email **info@verafin.com**
or call **866.781.8433**

VERAFIN
A STEP AHEAD