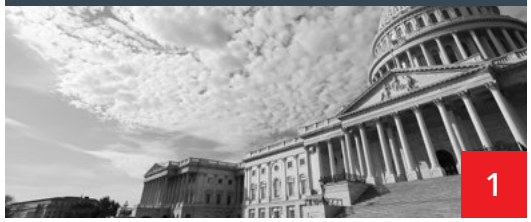
Collaborate with Confidence

Your Guide to 314(b) Collaboration

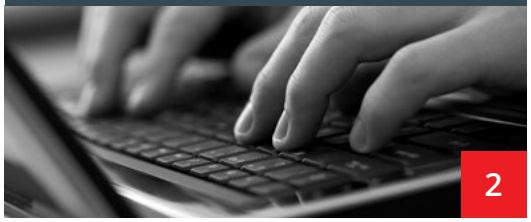
VERAFIN
A STEP AHEAD.

Sections

USA PATRIOT ACT & SECTION 314(b)

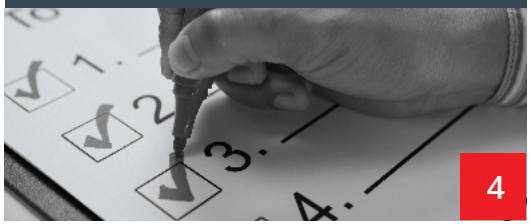


NOTIFYING FinCEN

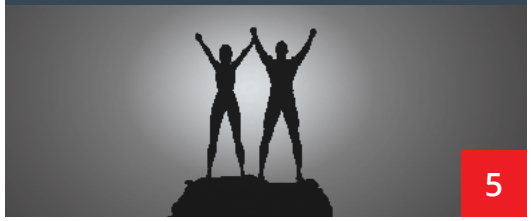


THE POWER OF COLLABORATION

PREPARING TO COLLABORATE



COLLABORATE WITH CONFIDENCE



HOW TO REQUEST INFORMATION

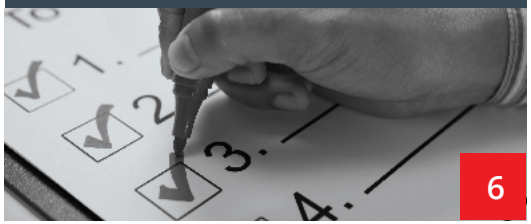


TABLE OF CONTENTS

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 services/technologies and also 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 in the end, they can prevent more losses for their institution.

SECTION 1

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."**[1]

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 "to identify, disrupt, and prevent money laundering and terrorist activity."[2]

Section 314(b) complements 314(a) by allowing voluntary information sharing between financial institutions and associations of financial institutions.

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.

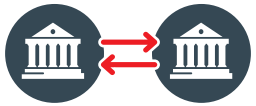
Section 314(b) — What is it?

"Section 314(b) of the USA PATRIOT Act 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 potential money laundering or terrorist activities." [3]

"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." [4]

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).[5]

SECTION 2

Notifying FinCEN

As stated on the Section 314(b) Fact Sheet, **"314(b) information sharing is a voluntary program, and FinCEN strongly encourages information sharing through Section 314(b)."** [6]

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." [7]

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 acknowledgement received from FinCEN to voluntarily share information.

SECTION 2

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 2

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 FI.

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.

SECTION 2

The Power of Collaboration

Peer Perspective

"We were investigating a new business member **due to some large volumes of cash and their nature of business** didn't seem to be fitting their activity. I had noticed they had deposited a large check from another credit union.

I contacted the 314(b) contact at that credit union and found out that they had closed out their accounts due to it being a marijuana business. He also mentioned that they deposited a large check from another credit union so I contacted the 314(b) rep from the other credit union and found out they had also closed out their accounts for the same reason.

This collaboration was key to validating our suspicion and it was also valuable to have a network of local 314(b) participants to share this information with so we could also warn others to watch out for them."

Lynn Searcey
Compliance Analyst
Bellco Credit Union

SECTION 3

The Power of Collaboration

Peer Perspective

"I was alerted of a new member with a **high frequency of wire transfer in and wire transfer out**. The individual was transferring his funds from his old institution into ours. Then he transferred the funds to a "charity" in Africa. The individual claimed to be the director of a charity that built schools in Africa. Despite being a noble cause, I had my doubts so I created Red Flag Alerts for any future transactions. Sure enough multiple wires transfers came in from **different originators at different institutions**.

I used 314(b) to reach out to the institutions' respective contact person. I explained my situation and concerns and asked them to review their member's wire transfer request. Later that day one institution called me back and stated that their member was conducting the wire transfer to invest in a company and not as a charitable donation. **Everything fell into place after that**.

Fortunately, we subscribed to 314(b) and had this resource so we could contact the right people to resolve this scenario."

Julian Guzman
Compliance Specialist II
LBS Financial Credit Union

SECTION 4

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.

SECTION 4

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 5

Collaborate with Confidence

"...I'd like to emphasize the need for information sharing across financial institutions.

The 314(b) safe harbor provisions permit financial institutions to share information under the 314(b) program as it relates to transactions involving proceeds of foreign corruption offenses and other specified unlawful activities (SUAs), the predicate offenses for money laundering, if the financial institution suspects there is a nexus between the suspected foreign corruption, or other SUA, and possible money laundering or terrorist financing activity." [8]

Jennifer Shasky Calvery
Former Director of FinCEN
2014 Bank Secrecy Act Conference, Nevada

SECTION 5

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).[9]
- ✓ Information to identify and report activities that may involve terrorist activity or money laundering.[10]
- ✓ Information about individuals, entities, organizations, and countries related to money laundering and terrorist financing activity.[11]
- ✓ 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).[12]

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)[13]

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 5

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." [14]

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 6

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 6

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 actvity you are investigating and what you are hoping to learn.

If you are collaborating on a transaction,
include relevant information including the date, amount and recipient of the transaction.

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 occurred, the other institution will have a better understanding of the activity you are inquiring about.

WHAT?

Include any information you know about the movement of funds at your institution.

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

SECTION 6

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

3, 6, 11 Section 314(b) Fact Sheet
http://www.fincen.gov/statutes_regs/patriot/pdf/314bfactsheet.pdf

4, 12 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.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014.pdf

5, 9 Guidance on the Scope of Permissible Information Sharing Covered by Section314(b) Safe Harbor of the USA PATRIOT Act
http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2009-g002.pdf

7 Administrative Ruling Regarding the Participation of Associations of Financial Institutions in the 314(b) Program
http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2012-R006.pdf

8 Prepared Remarks of Jennifer Shasky Calvery, Director of FinCEN, 2014 Bank Secrecy Act Conference, Las Vegas, NV
Conference sponsored by the State Bar of Nevada's Gaming Law Section, the American Gaming Association, and University of Nevada, Las Vegas (UNLV) International Gaming Institute.
https://www.fincen.gov/news/speeches/prepared-remarks-jennifer-shasky-calvery-director-financial-crimes-enforcement-1

10 FinCEN Section 314(b) webpage
http://www.fincen.gov/statutes_regs/patriot/section314b.html

31 CFR 1010.540 Voluntary information sharing among institutions
http://www.gpo.gov/fdsys/pkg/CFR-2011-title31-vol3/pdf/CFR-2011-title31-vol3-sec1010-540.pdf

The 314(b) Program – A Decade of Information Sharing: Stronger Than Ever
http://info.verafin.com/rs/verafin/images/FinCEN-The-314b-Program-A-Decade-of-Information-Sharing.pdf

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

14 Financial Institutions Outreach Initiatve - Report on Outreach to Large Depository Institutions
http://www.fincen.gov/news_room/rp/reports/pdf/Bank_Report.pdf

Verafin is an industry leader in cross-institutional Fraud Detection and Anti-Money Laundering (FRAMLx) collaboration software with a customer base of 1400 financial institutions across North America.

Its solution uses advanced behavior-based analytics that help financial institutions stay a step ahead of numerous types of fraud as well as the BSA, USA PATRIOT Act, and FACTA compliance landscape.

Verafin is the exclusive provider of fraud detection and BSA/AML software for the California Bankers Association, Florida Bankers Association, Massachusetts Bankers Association, Illinois Bankers Association, CUNA Strategic Services, a preferred service provider of the Independent Community Bankers of America, and has industry endorsements in 44 states across the U.S.

Updated: November 2016

For more information, contact us today.

1.877.368.9986
info@verafin.com
www.verafin.com/FRAMLx

VERAFIN
A STEP AHEAD.