U.S. DEPARTMENT OF THE TREASURY

Resource Center

OFAC FAQs: Sanctions Compliance

Skip to the Following Topics:

Assessing OFAC Name Matches

Print this topic

5. How do I determine if I have a valid OFAC match?

Please take the following "due diligence" steps in determining a valid OFAC match.

If you are calling about a wire transfer or other "live" transaction:

Step 1. Is the "hit" or "match" against OFAC's Specially Designated Nationals (SDN) list, one of its other sanctions lists, or targeted countries, or is it "hitting" for some other reason (i.e., "Control List" or "PEP," "CIA," "Non-Cooperative Countries and Territories," "Canadian Consolidated List (OSFI)," "World Bank Debarred Parties," "Blocked Officials File," or "government official of a designated country"), or can you not tell what the "hit" is?

- If it's hitting against OFAC's SDN list, one of its other sanctions lists, or targeted countries, continue to 2 below.
- If it's hitting for some other reason, you should contact the "keeper" of whichever other list the match is hitting against. For questions about:
- The Denied Persons List and the Entities List, please contact the Bureau of Industry and Security at the U.S. Department of Commerce at 202-482-4811.
- The FBI's Most Wanted List or any other FBI-issued watch list, please contact the Federal Bureau of Investigation (http://www.fbi.gov/contact/fo/fo.htm).
- The Debarred Parties list, please contact the Directorate of Defense Trade Controls at the U.S. Department of State, 202-663-1282.
- The Bank Secrecy Act and the USA PATRIOT Act, please contact the Financial Crimes Enforcement Network (FinCEN), 1-800-949-2732.
- If you are unsure whom to contact, please contact your screening software provider which told you there was a "hit."
- If you can't tell what the "hit" is, you should contact your screening software provider which told you there was a "hit."

Step 2. Now that you've established that the hit is against one of OFAC's sanctions lists or targeted countries, you must evaluate the quality of the hit. Compare the name in your transactions with the name on the sanctions list. Is the name in your transaction an individual while the name on the sanctions list is a vessel, organization or company (or vice-versa)?

- If yes, you do not have a valid match.*
- If no, please continue to 3 below.

Step 3. How much of the listed entry's name is matching against the name in your transaction? Is just one of two or more names matching (i.e., just the last name)?

- If yes, you do not have a valid match.*
- If no, please continue to 4 below.

Step 4. Compare the complete sanctions list entry with all of the information you have on the matching name in your transaction. An entry often will have, for example, a full name, address, nationality, passport, tax ID or cedula number, place of birth, date of birth, former names and aliases. Are you missing a lot of this information for the name in your transaction?

- If yes, go back and get more information and then compare your complete information against the entry.
- If no, please continue to 5 below.

Step 5. Are there a number of similarities or exact matches?

- If yes, please call the hotline at 1-800-540-6322.
- If no, you do not have a valid match.*

If you are calling about an account:

Step 1. Is the “hit” or “match” against OFAC’s SDN list, one of OFAC's other sanctions lists or targeted countries, or is it “hitting” for some other reason (i.e., “Control List” or “PEP,” “CIA,” “Non-Cooperative Countries and Territories,” “Canadian Consolidated List (OSFI),” “World Bank Debarred Parties,” or “government official of a designated country”), or can you not tell what the “hit” is?

- If it’s hitting against one of OFAC’s sanctions lists or targeted countries, continue to 2 below.
- If it’s hitting for some other reason, you should contact the “keeper” of whichever other list the match is hitting against. For questions about:
- The Denied Persons List and the Entities List, please contact the Bureau of Industry and Security at the U.S. Department of Commerce at 202-482-4811.
- The FBI’s Most Wanted List or any other FBI-issued watch list, please contact the Federal Bureau of Investigation (http://www.fbi.gov/contact/fo/fo.htm).
- The Debarred Parties list, please contact the Directorate of Defense Trade Controls at the U.S. Department of State, 202-663-1282.
- The Bank Secrecy Act and the USA PATRIOT Act, please contact the Financial Crimes Enforcement Network (FinCEN), 1-800-949-2732.
- If you are unsure whom to contact, you should contact your screening software provider which told you there was a “hit.”
- If you can’t tell what the “hit” is, you should contact your screening software provider which told you there was a “hit.”

Step 2. Now that you’ve established that the hit is against one of OFAC’s sanctions lists or targeted countries, you must evaluate the quality of the hit. Compare the name of your customer with the name on the sanctions list. Is the name of your customer an individual while the name on the sanctions list is a vessel, organization or company (or vice-versa)?

- If yes, you do not have a valid match.*
- If no, please continue to 3 below.

Step 3. How much of the listed entry’s name is matching against the name of your account holder? Is just one of two or more names matching (i.e., just the last name)?

- If yes, you do not have a valid match.*
- If no, please continue to 4 below.

Step 4. Compare the complete entry with all of the information you have on the matching name of your account holder. An entry often will have, for example, a full name, address, nationality, passport, tax ID or cedula number, place of birth, date of birth, former names and aliases. Are you missing a lot of this information for the name of your account holder?

- If yes, go back and get more information and then compare your complete information against the entry.
- If no, please continue to 5 below.

Step 5. Are there a number of similarities or exact matches?

- If yes, please call the hotline at 1-800-540-6322.
- If no, you do not have a valid match.*

* If you have reason to know or believe that processing this transfer or operating this account would violate any of the Regulations, you must call the hotline and explain this knowledge or belief. [01-30-2015]

Strong and Weak Aliases

For additional information regarding strong and weak aliases on OFAC's sanctions lists, please see the following topic.

Starting an OFAC Compliance Program

Print this topic

25. Does OFAC itself require that banks set up a certain type of compliance program?

No. There is no single compliance program suitable for every financial institution. OFAC is not itself a bank regulator; its basic requirement is that financial institutions not violate the laws that it administers. Financial institutions should check with their regulators regarding the suitability of specific programs to their unique situations. [09-10-2002]

---

27. What do I need to do to comply? Do I have to buy expensive software?

This is primarily a question for your regulator. What constitutes an adequate compliance program depends in large part on who your customers are and what kinds of business you do. Certain areas of bank operations, such as international wire transfers and trade finance, are at a higher risk than others. There are numerous interdiction software packages that are commercially available. They vary considerably in cost and capabilities. If your bank feels it needs to invest in software in its attempt to comply with OFAC regulations, OFAC recommends that you talk to your counterparts in other banks about the systems they have in place and contact vendors for an assessment of your needs. It should be noted that *.TXT and *.PDF versions of all of OFAC's sanctions lists can be manually scanned; OFAC also offers a free, online search engine at the following URL: https://sdnsearch.ofac.treas.gov [01-30-2015]

---

28. How often do I need to scan my customer database against OFAC's sanctions lists?

The frequency of running an OFAC scan must be guided by your organization's internal policies and procedures. Keep in mind, however, that if your organization fails to identify and block a target account (of a terrorist, for example), there could be serious consequences such as a transfer of funds or other valuable property to an Specially Designated National, an enforcement action against your organization, and negative publicity. [01-30-2015]

---

29. How do I setup a compliance program for my bank?

There is no prepackaged compliance program that fits the needs of every bank. Banks, obviously, range in size from small to some of the largest institutions in the world. A good starting point is to go to the OFAC website and look under "Regulations by Industry." Then read the brochure for the Financial Community. This brochure provides insight as to how your particular bank could set up a compliance program. There are also a number of articles written for banking industry publications available on OFAC's website. Banks should also review OFAC's Frequently Asked Questions, its SDN and other sanctions list pages and finally, OFAC's dedicated sanctions program pages. It may be helpful to contact your counterparts in other banks to see what they are doing and talk to your regulator. [01-30-2015]

---

30. How do I know if my compliance program is adequate?

The following information will provide you with areas to consider as you review your OFAC procedures. [09-10-2002]

---

31. What are the features and benefits that banks should be looking for when selecting an OFAC compliance software package?

There are a wide variety of software packages available to the financial community. The size and needs of each institution help to determine what to look for in a package. Some packages are used to interdict sanctioned countries and names on the Specially Designated Nationals or other sanctions lists in wire transfers. Others are used to check the names of new customers or to routinely filter the names of all account holders. One suggestion for finding the right software for your bank is to research what your peer banks are using and determine if the software package is working for them. Your bank also could talk to a variety of software vendors who can easily be located by doing an Internet search. [01-30-2015]

Blocking and Rejecting Transactions

Print this topic

32. How do I block an account or a funds transfer?

Once it has been determined that funds need to be blocked, they must be placed into an interest-bearing account on your books from which only OFAC-authorized debits may be made. The blocking also must be reported to OFAC Compliance within 10 business days. Some banks have opted to open separate accounts for each blocked transaction, while others have opted

for omnibus accounts titled, for example, "Blocked Libyan Funds." Either method is satisfactory, so long as there is an audit trail which will allow specific funds to be unblocked with interest at any point in the future. [09-10-2002]

---

33. How much interest do I have to pay on the blocked funds?

OFAC regulations require that funds earn interest at a commercially reasonable rate, i.e., at a rate currently offered to other depositors on deposits or instruments of comparable size and maturity. [09-10-2002]

---

34. Can my bank deduct service charges from the account?

Generally yes. In most cases (excluding Iraq, for instance) OFAC regulations contain provisions to allow a bank to debit blocked accounts for normal service charges, which are described in each set of regulations. The charges must be in accordance with a published rate schedule for the type of account in which the funds are maintained. [09-10-2002]

---

35. Do all OFAC programs involve blocking transactions?

No. OFAC regulations are tailored to further the requirements and purposes of specific Executive Orders or statutes which provide the basic outline of each program. In some cases, the President has determined that a comprehensive asset freeze is appropriate, and in others the President has determined that more limited restrictions (for example, import bans) are in order. The individual program web pages outline the restrictions for each program. Special attention should be given when reviewing sanctions list targets that are included on one of OFAC's non-Specially Designated Nationals sanctions lists. [01-30-2015]

---

36. I understand blocking a transaction, but what is meant by rejecting a transaction? When should a transaction be rejected rather than blocked?

In some cases, an underlying transaction may be prohibited, but there is no blockable interest in the transaction. In these cases, the transaction is simply rejected, or not processed. For example, a U.S. bank would have to reject a wire transfer between two third-country companies (non-SDNs) involving an export to a company in Sudan that is not subject to sanctions. Since there is no interest of the Government of Sudan or an SDN, there is no blockable interest in the funds. The U.S. bank cannot process the transaction because that would constitute a transaction in support of a commercial activity in Sudan, which is prohibited by the Sudanese Sanctions Regulations. Similarly, a U.S. bank could not be involved in the financing of a prohibited transaction. A U.S. bank cannot so much as advise a letter of credit if the underlying transaction is in violation of OFAC regulations.

The following examples may help illustrate which transactions should be blocked and which should be rejected.

- A U.S. bank interdicts a commercial payment destined for the account of XYZ Import-Export Co. at the Bank of XYZ in Sudan. The Bank of XYZ is wholly-owned by the Government of Sudan and, accordingly, is a Specially Designated National of Sudan. This payment must be blocked.
- A U.S. bank interdicts a commercial payment destined for the account of ABC Import-Export at Sudanese French Bank, Khartoum, Sudan. Unlike the Bank of XYZ, Sudanese French Bank, Khartoum is a private sector entity so there is no blockable interest in this payment. However, processing the payment would mean facilitating trade with Sudan and providing a service in support of a commercial transaction in Sudan, therefore the U.S. bank must reject the payment.

Rejected and blocked funds transfers must be reported to OFAC within 10 days. Questions about whether a transaction should be blocked or rejected should be directed to OFAC Compliance. [01-15-2015]

---

39. What do I do if I have a blocked account that needs to be escheated to the state?

You need to discuss this with your state authorities and with OFAC. For instance, the state of New York has a license to escheat blocked funds, pending OFAC approval of each transfer. Banks in New York should contact the State Banking Department for instructions on how to proceed. Banks in other states should contact OFAC directly for instructions on how to proceed. [09-10-2002]

---

41. Should an institution tell its customer that it blocked their funds, and, if so, how does the institution explain it to them?

An institution may notify its customer that it has blocked funds in accordance with OFAC's instructions. The customer has the right to apply for the unblocking and release of the funds.

To apply online to have the funds released, please go to our online application page. [3-16-2015]

---

42. What do I do if a person tries to open an account and the person's name is on OFAC's SDN list? Do I open the account and then block the funds?

A U.S. bank cannot open an account for a person named on the SDN list. This is a prohibited service. However, you should pay careful attention to be sure the person trying to open the account is the same person as the one named on OFAC's list. In many cases you may get a "false positive," where the name is similar to a target's name, but the rest of the information provided by the applicant does not match the descriptor information on OFAC's SDN list. If the bank does come into the possession or control of any property in which a blocked person has an interest, it is obligated to block that property. In other words, if you receive an application to open an account from a person who matches the information on the SDN list, together with an opening deposit, you are obligated to block the funds. The same is true for other banking transactions. If, for example, a customer asks if he or she is allowed to send money to a relative's account with Bank of XYZ in Sudan, the bank can say "no, that's illegal." If, on the other hand, a bank receives instructions from its customer to debit his or her account and send the funds to Bank of XYZ, the bank must act on the instructions by blocking the funds which contain a future interest of the Sudanese SDN bank. You might think of the analogy of a bouncing ball. Once the ball starts moving, you must stop it if it comes into your possession. [04-06-2005]

---

48. I just received an interdiction "alert." What do I do?

When your interdiction software or account holder checking service shows a potential match, OFAC recommends that you do an initial analysis prior to contacting OFAC. If you have a reasonably close match to a name on the Specially Designated Nationals (SDN) list (or one of OFAC's other sanctions lists) and your customer is located in the same vicinity as the SDN, feel free to contact OFAC. Computer software may flag some transactions that are not actually associated with OFAC targets. This is where human intervention becomes critical and some hands-on research may be necessary. Please look at the following "due dilligence" steps before calling OFAC. Unless you have an exact match or are otherwise privy to information indicating that the hit is a sanctions target, it is recommended that you do not actually block a transaction without discussing the matter with OFAC. [01-30-2015]

---

53. How do I differentiate between an "inquiry" and a "payment instruction" when a customer wants to send a wire transfer to a sanctioned party or country?

In those programs with blocking provisions, OFAC's regulations block all "property" in which a target has an interest. The term "property" is very broadly defined, including present, future or contingent interests. In the case of a wire transfer, the bank will be holding blocked property upon the receipt of concrete instructions from its customer to send the funds. In this case, the funds must be blocked and reported to OFAC within ten days. If, on the other hand, a customer simply asks "Can I send money to Cuba?" there is no blockable interest in the inquiry and the bank can answer the question or direct the customer to OFAC. The same logic applies to cases where the transaction would be required to be rejected under OFAC regulations. There is not technically a "reject" item until the bank receives instructions from its customer to debit its account and send the funds. [01-15-2015]

Filing Reports with OFAC

Print this topic

49. If I reject or block a transaction, when do I have to report the action to OFAC? How do I submit the report?

31 C.F.R. Parts §§501.603 and 501.604 require blocking and reject reports to be submitted to OFAC within 10 business days of the date of the action. Optional reporting forms are available at this link and complete information may be emailed to OFAC's Sanctions Compliance and Evaluation Division at ofacreport@treasury.gov. Blocking and reject reports must contain a copy of the original transfer instructions. [07-28-2017]

---

50. Is there a requirement for annual reporting of blocked property? Is there a required format?

Yes. A report of blocked property is to be submitted annually by September 30 to OFAC Compliance, Department of the Treasury, Washington, D.C., 20220. The standardized form can be accessed by visiting this link. If you wish to use a different format, please contact OFAC's Compliance Division at 202-622-2490. For Guidance on Filing the Annual Report of Blocked Property, visit this link. [06-30-2017]

Compliance for Internet, Web Based Activities, and Personal Communications

Print this topic

72. Can I send money to a sanctioned country using a third-country company's website? Can I buy gifts for someone in a sanctioned country over the internet? The websites tell me that it's ok because they themselves are not sanctioned parties.

You cannot do something indirectly that you would not be able to do directly. Therefore, these sites can be used to facilitate authorized transactions, but you cannot use them to perform a transaction which would be in violation of U.S. law. For example, the Cuban Assets Control Regulations authorize any U.S. person to send $2000 per quarter to any individual in Cuba. The U.S. remitter can use a third-country provider to send these funds to Cuba. If the person attempts to send more than $2000 per quarter to any one individual, however, he or she may be in violation of U.S. law and subject to penalties. Another example is booking unauthorized travel to Cuba using an internet travel service provider in a third country. Spending money on unauthorized travel-related transactions involving Cuba is prohibited by the CACR, regardless of how the travel is booked or how it is paid for. The fact that the trip was booked through a third-country company, either in person or over the internet, is irrelevant. [01-15-2015]

---

73. My company provides money remittance and account services via the Internet. Does OFAC have any compliance guidance for this type of business?

Complying with United States sanctions policy presents unique challenges to institutions that operate exclusively on the Internet. The Internet has often been thought of as an "anonymous venue" in that e-commerce transactions can be conducted in relative privacy with little or no face-to-face contact among the parties in a transaction. This anonymity creates a significant challenge for Internet businesses that wish to satisfy their due diligence requirements.

In order to be compliant with OFAC-governed sanctions regulations, US jurisdiction entities must ensure that they are not:

A. Engaging in trade or transaction activities that violate the regulations behind OFAC's country-based sanctions programs, and;

B. Engaging in trade or transaction activities with sanctions targets named on OFAC's list of Specially Designated Nationals and Blocked Persons (SDN's).

A number of Internet-based financial service companies already developed Internet Protocol (IP) address blocking procedures. These companies use publicly available data to maintain tables of IP addresses based on geographic region. Users attempting to initiate an online transaction or access an account from a sanctioned country are blocked based on their IP address. While this approach is effective, it does not fully address an Internet firm's compliance risks. The fact that international distribution authorities can reassign IP blocks makes the geographic location of an IP potentially dynamic.

The anonymous character of Internet-based transactions often places obstacles in the path of rigorous compliance practices. Firms that facilitate or engage in e-commerce should do their best to know their customers directly. In order to minimize their liabilities, Internet remittance and account service firms should attempt to gather authentic identification information on their customers before a new account is opened or new transaction is initiated. This information will help confirm the customer's identity and help the e-commerce firm ensure it is not conducting business with a sanctions target. Currently many Internet remittance companies use credit card authentication as the primary method of confirming a customer's identity. While this method is technologically expedient, it does not meet the standards of due diligence normally found in the non-Internet-based financial community. A company cannot rely on another firm's compliance program in order to mitigate risk.

It is recommended that e-commerce firms gather and record "purpose of payment" information on each transaction they process. In the non-Internet sector, financial institutions are able to stop in-process transactions and gather more information on them. Due to the level of automation found within the Internet financial sector, this type of in-process information gathering is not always possible. Collecting information on the purpose of payments up front will allow Internet firms to better screen outgoing and incoming transactions for potential violations. [04-13-2004]

Cyber-related Sanctions and Executive Orders 13694 and 13757

For information regarding Cyber-related Sanctions and Executive Orders 13694 and 13757, please see the following topic.

Specific Software, Hardware, and Services Covered by General License D-1 for Iran and 31 CFR § 538.533 for Sudan (the "Personal Communications General Licenses") Print this topic

Effective January 17, 2017, the general license under the Sudanese Sanctions Regulations, 31 C.F.R. part 538 (SSR), authorizing the exportation, reexportation, or provision of certain services, software, and hardware incident to personal communications, 31 C.F.R. § 538.533, has been superseded by a broader general license under the SSR that authorizes all transactions prohibited under the SSR. See 31 C.F.R. § 538.540. As a result, for such exports and reexports to Sudan, U.S. persons may rely on the broader authorization in § 538.540 and do not need to abide by the narrower requirements of § 538.533. Section 538.540 only authorizes transactions prohibited under the SSR and does not affect Iran General License D-1.

434. Are all applications designed to run on mobile operating systems ("apps") covered by the Personal Communications GLs?

The exportation to Iran and Sudan of apps that are designated EAR99 or classified under export control classification number (ECCN) 5D992.c, as specified in category (8) of the Annex to GL D-1 and in Appendix A to § 538.533, respectively, is authorized under the Personal Communications GLs, including apps downloaded via online app stores. [02-17-2015]

435. Is the exportation of anti-virus, anti-malware, anti-tracking, and anti-censorship software authorized?

Yes. Paragraphs (a)(3) of GL D-1 and § 538.533 authorize the exportation of certain anti-virus, anti-malware, anti-tracking, and anti-censorship software, as specified in categories (6), (7), and (9) of the Annex to GL D-1 and Appendix A to § 538.533, respectively. [02-17-2015]

436. What do Secure Socket Layers (SSLs), listed in the Annex to GL D-1 and in Appendix A to § 538.533, encompass?

SSLs, as described in category (11) of the Annex to GL D-1 and Appendix A to § 538.533, respectively, encompass "provisioning and verification software for Secure Socket Layer (SSL) certificates designated EAR99 or classified under ECCN 5D992.c, and services necessary for the operation of such software." Additional provisioning and verification software not subject to the EAR may be included under the Personal Communications GLs' authorization for, in relevant part, software not subject to the EAR that is exported or reexported, directly or indirectly, by a U.S. person located outside the United States, that is of a type described in the Annex to GL D-1 and Appendix A to § 538.533, respectively, provided that it would be eligible for classification under an ECCN listed in the Annex or Appendix (here, ECCN 5D992.c), or designated as EAR99, if it were subject to the EAR. [02-17-2015]

437. Are mobile phone accessories and computer accessories and peripherals authorized for export under the Personal Communications GLs?

Yes. Accessories for use in conjunction with hardware specified in categories (1) and (5) of the Annex to GL D-1 and Appendix A to § 538.533, respectively, and peripherals for use in conjunction with hardware specified in category (5) of the same are authorized for export to Iran and Sudan under the Personal Communications GLs. Authorized accessories for mobile phones include headsets, cases, holsters, mounts, chargers, docks, display protectors, cables, adapters, and batteries. Authorized accessories for computers include keyboards and mice; authorized peripherals for computers include consumer disk drives and other data storage devices. As set forth in a note to the Annex to GL D-1 and Appendix A to § 538.533, respectively, for the purposes of the Annex and Appendix, the term "consumer" refers to items that are: (1) generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following: (a) over-the-counter transactions; (b) mail order transactions; (c) electronic transactions; or (d) telephone call transactions; and (2) designed for installation by the user without further substantial support by the supplier. [02-17-2015]

438. Is the exportation of parts or components for authorized hardware, such as microprocessors, authorized under the Personal Communications GLs?

No. While the exportation of certain accessories and peripherals specified in categories (1) and (5) of the Annex to GL D-1 and Appendix A to § 538.533, respectively, is authorized under paragraphs (a)(3) of the Personal Communications GLs, the exportation of hardware parts or components is not. Requests for specific licenses to export parts or components, including replacement parts, will be considered on a case-by-case basis. [02-17-2015]

439. Do the Personal Communications GLs authorize the export of bundled software that includes both software authorized by the Personal Communications GLs and software that is not authorized by the Personal

Communications GLs?

No. To qualify for the Personal Communications GLs, all individual software items in a bundled package must fall within one of the Personal Communications GL authorizations. If some software in a bundled package is authorized by the Personal Communications GLs, but other software is not, the portion of the software falling outside the authorizations in the Personal Communications GLs would need to be otherwise exempt or authorized or would require a specific license for export. For example, a bundle of software that included exclusively software authorized by GL D-1 and by 31 CFR § 560.540 could be exported. [02-17-2015]

---

440. Do the Personal Communications GLs authorize the exportation to Iran and Sudan of fee-based desktop publishing software and productivity software suites used to publish documents, presentations, spreadsheets, charts, music, movies, and digital images?

Yes. Fee-based desktop publishing software and productivity software suites have been determined to fall within the scope of fee-based software necessary to enable services incident to the exchange of personal communications as described in paragraphs (a)(2) of the Personal Communications GLs, provided that the software meets the additional criteria in those paragraphs (e.g., for software subject to the EAR, the software is designated EAR99 or is classified by the U.S. Department of Commerce on the Commerce Control List, 15 CFR part 774, supplement No. 1 ("CCL") under ECCN 5D992.c). By contrast, enterprise management software has been determined not to fall within the scope of fee-based software necessary to enable services incident to the exchange of personal communications as described in paragraphs (a)(2) of the Personal Communications GLs. [02-17-2015]

---

441. Do the Personal Communications GLs authorize the exportation of fee-based cloud computing services to Iran and Sudan

Yes. Paragraphs (a)(1) of the Personal Communications GLs authorize the exportation to Iran and Sudan of fee-based cloud computing services incident to the exchange of personal communications over the Internet. In addition, paragraphs (a)(2)(i) and (a)(3) authorize software necessary to enable such services, provided that such software is designated EAR99 or classified by the U.S. Department of Commerce on the CCL under ECCN 5D992.c or, in the case of software that is not subject to the EAR, would be designated EAR99 if it were located in the United States or would meet the criteria for classification under ECCN 5D992.c if it were subject to the EAR. [02-17-2015]

---

442. For purposes of category (5) of the Annex to GL D-1 and Appendix A to § 538.533, respectively, what would be considered "software required for effective consumer use" of personal computing devices, laptops, and tablets?

"Software required for effective consumer use" consists of software essential to the operation of the hardware listed in category (5) of the Annex to GL D-1 and Appendix A to § 538.533, respectively, including, for example, drivers and patches. Operating systems are separately authorized in category (5) of the Annex to GL D-1 and Appendix A to § 538.533. [02-17-2015]

---

443. What are "residential consumer" satellite terminals and transceiver equipment?

Satellite terminals and other equipment listed in category (4) of the Annex to GL D-1 and Appendix A to § 538.533, respectively, shall be deemed "residential consumer" if the equipment is designated EAR99 or classified under ECCN 5A992.c, 5A991.b.2, or 5A991.b.4 or, in the case of equipment that is not subject to the EAR, would be designated EAR99 if it were located in the United States or would meet the criteria for classification under ECCN 5A992.c, 5A991.b.2, or 5A991.b.4 if it were subject to the EAR. [02-17-2015]

Compliance for the Insurance Industry

Print this topic

61. State insurance statutes regulate an insurer's ability to withhold claim payments, cancel policies or to decline to enter into policies. In some cases, insurers must commit an ostensible violation of state insurance regulations to comply with OFAC regulations. Does OFAC have a position as to whether OFAC regulations preempt state insurance regulations in this context?

OFAC's regulations under the Trading with the Enemy Act and the International Emergency Economic Powers Act are based on Presidential declarations of national emergency and preempt state insurance regulations. OFAC regulations are not federal

insurance regulations, they are regulations promulgated under the President's exercise of foreign-affairs and national emergency powers. [09-10-2002]

---

62. At what point must an insurer check to determine whether an applicant for a policy is a Specially Designated National (SDN) or is on one of OFAC's other sanctions lists?

If you receive an application from an SDN for a policy, you are under an obligation not to issue the policy. Remember that when you are insuring someone, you are providing a service to that person. You are not allowed to provide any services to an SDN. If the SDN sends a deposit along with the application, you must block the payment. If you receive an application from a party on one of OFAC's other sanctions lists, please review the specific treatment prohibitions associated with that list carefully before taking any action. [09-10-2002]

---

63. What should an insurer do if it discovers that a policyholder is or becomes a Specially Designated National (SDN)--cancel the policy, void the policy ab initio, non-renew the policy, refuse to pay claims under the policy? Should the claim be paid under a policy issued to an SDN if the payment is to an innocent third-party (for example, the injured party in an automobile accident)?

The first thing an insurance company should do upon discovery of such a policy is to contact OFAC Compliance. OFAC will work with you on the specifics of the case. It is possible a license could be issued to allow the receipt of premium payments to keep the policy in force. Although it is unlikely that a payment would be licensed to an SDN, it is possible that a payment would be allowed to an innocent third party. The important thing to remember is that the policy itself is a blocked contract and all dealings with it must involve OFAC. [09-10-2002]

---

64. A workers' compensation policy is with the employer, not the employee. Is it permissible for an insurer to maintain a workers compensation policy that would cover a person on the Specially Designated Nationals (SDN) List, since the insurer is not transacting business with the SDN, but only with his/her employer?

If an insurer knows that a person covered under the group policy is an SDN, that person’s coverage is blocked, and if he or she makes a claim under the policy, the claim cannot be paid. If an insurer does not know the names of those covered under a group policy, it would have no reason to know it needed to block anything unless and until an SDN files a claim under that policy. At that point its blocking requirement would kick in.

If an insurer knows that a person covered under a group policy is on one of OFAC's other sanctions lists, a different set of restrictions may apply. The insurer should contact OFAC if a claim is filed by an individual on one of the other sanctions lists. [01-30-2015]

---

65. How frequently is an insurer expected to scrub its databases for OFAC compliance?

That is up to your firm and your regulator. Remember that a critical aspect of the designation of a Specially Designated National (SDN) is that the SDN's assets must be frozen immediately, before they can be removed from U.S. jurisdiction. If a firm only scrubs its database quarterly, it could be 3 months too late in freezing targeted assets. Although the prohibitions and treatments for individuals and entities on OFAC's other sanctions lists are different from those on the SDN list, there may be similar consequences if your firm takes a long time in recognizing a sanctions list match.

OFAC's sanctions lists may be updated as frequently as a few times a week or as rarely as once in a month. [01-30-2015]

---

66. Is it sufficient if my company screens life insurance policies only prior to policy issuance?

That is up to your firm and your regulators. Conducting screening only before policy issuance is critical but would not likely achieve your desired level of compliance. After the policy issuance, the U.S. Government may designate an existing policyholder or a named beneficiary as a Specially Designated National or Blocked Person ("SDN"), or it may expand sanctions with respect to a particular country, or impose sanctions against a new country. If an existing policyholder or a named beneficiary became an SDN or otherwise subject to U.S. sanctions, the insurer may be required to "block" the policy, report such blocking to OFAC within 10 days of the SDN designation, place any future premiums into a blocked, interest-bearing account at a U.S. financial institution, and seek an OFAC license before making any payments under the policy. Other restrictions may apply if a policyholder or a named beneficiary is added to one of OFAC's other sanctions lists. Consequently, routinely screening all policies against OFAC’s sanctions lists, as frequently updated, would enable the insurer to comply with the applicable OFAC regulatory requirements. It also is important to screen the policyholder and beneficiary prior to paying a claim. [01-30-2015]

---

68. If my screening efforts uncover a policyholder who became a Specially Designated National after policy issuance, can I notify the policyholder that the policy is "blocked"?

Yes, the insurer may notify the policyholder that the policy is blocked, without obtaining a specific license from OFAC. [05-01-2003]

---

69. In my letter to the policyholder whose policy is "blocked," may I also instruct the policyholder not to send any more premium or that we will not accept additional premium under this account?

The insurer may instruct the policyholder as follows: "If you send any more premium, we are required under applicable U.S. laws and regulations to place such funds in a blocked account. If you have any questions, please contact the U.S. Department of Treasury's Office of Foreign Assets Control." [05-01-2003]

---

102. How can an insurer participate in worldwide insurance markets through global insurance policies if, by definition, coverage extends to potential risks in sanctioned countries?

The best and most reliable approach for insuring global risks without violating U.S. sanctions law is to insert in global insurance policies an explicit exclusion for risks that would violate U.S. sanctions law. For example, the following standard exclusion clause is often used in open marine cargo policies to avoid OFAC compliance problems: "whenever coverage provided by this policy would be in violation of any U.S. economic or trade sanctions, such coverage shall be null and void." The legal effect of this exclusion is to prevent the extension of a prohibited service (insurance or risk assumption) to sanctioned countries, entities or individuals. It essentially shifts the risk of loss for the underlying transaction back to the insured - the person more likely to have direct control over the economic activity giving rise to the contact with a sanctioned country, entity or individual. [11-16-2007]

---

103. What if the commercial setting and/or market circumstances of a global insurance policy does not permit the use of an OFAC exclusion such as the one noted above?

OFAC recognizes that U.S. insurers often compete in international markets where non-U.S. insurers are willing and able to issue global insurance policies without a U.S. sanctions exclusion. In cases where such an exclusion is not commercially feasible, the insurer should apply for a specific OFAC license for the global insurance policy. In making a licensing determination, OFAC will review the facts and circumstances of each global insurance policy, including both risk frequency and risk severity, to assure that issuance of the policy will not undermine U.S. foreign policy goals. A separate license would be required for the insurer to pay claims arising under any authorized global insurance policy. [11-16-2007]

---

104. Can an insurer offer global travel insurance and worldwide travel assistance without violating U.S. sanctions?

The provision of all travel related services are authorized for all OFAC country sanctions programs (including Burma, Iran and Sudan) except Cuba. Travel related services may only be provided in Cuba pursuant to a valid general or specific OFAC license. If the traveler is a U.S. person traveling to Cuba pursuant to a valid OFAC license, travel insurance may be issued to the traveler by a U.S. insurer without a separate license. Similarly, the issuance or provision of coverage for global health, life, or travel insurance policies for individuals ordinarily resident in a country outside of Cuba who travel to or within Cuba is authorized by general license, as is the servicing of such policies and payment of claim arising from events that occurred while the individual was traveling in, or to or from, Cuba. Additionally, insurers should check OFAC's list of Specially Designated Nationals and other sanctions lists to ensure that no prohibited services are rendered to persons or entities on those lists. [01-15-2015]

Sanctions Relating to Insurance, Reinsurance, or Underwriting and the Iran Freedom And Counter-Proliferation Act of 2012

For additional information regarding insurance, reinsurance, and underwriting activities in Iran, please see the following topic.

Additional Questions from Financial Institutions

Print this topic

40. If my financial institution receives a wire going to an embassy in a sanctioned country, can we process the transaction?

This depends on the program. If you have a payment involving an embassy in a targeted country, please contact OFAC Compliance for directions (1-800-540-6322). [09-10-2002]

---

43. Does a financial institution need to scan names against OFAC's list of targets upon account opening or can it wait for 24 hours to receive a report from its software vendor on whether or not there is a hit?

There is no legal or regulatory requirement to use software or to scan. There is a requirement, however, not to violate the law by doing business with a target or failing to block property. OFAC realizes that financial institutions use software that does not always provide an instantaneous response and may require some analysis to determine if a customer is indeed on OFAC's Specially Designated Nationals List (or any of OFAC's other sanctions lists). The important thing is not to conclude transactions before the analysis is completed. [09-10-2002]

---

44. Is there a dollar limit on which transactions are subject to OFAC regulations?

There is no minimum or maximum amount subject to the regulations. [09-10-2002]

---

45. Does my bank need to check the OFAC list when selling cashier's checks and money orders? In the case of cashier's checks, do I need to check both the purchaser and the payee? As a mortgage lender, do I need to check both the purchaser and the seller's name against the Specially Designated Nationals list? Do I need to check their names against all of OFAC's other sanctions lists?

Every transaction that a U.S. financial institution engages in is subject to OFAC regulations. If a bank knows or has reason to know that a target is party to a transaction, the bank's processing of the transaction would be unlawful. [09-10-2002]

---

46. If a loan meets underwriting standards but is a true "hit" on OFAC's Specially Designated Nationals (SDN) list, what do we use as a denial reason on the adverse action notice?

If you have confirmed with OFAC that you have a "good hit" on the SDN list or one of OFAC's other sanctions lists, there is no reason not to explain that to the customer. The customer can contact OFAC directly for further information. [09-10-2002]

---

47. Through corporate giving programs, many banks contribute toward charities and other non-profits. To what extent does a bank need to review the recipients of these gifts or the principals of the charities?

Donations to charitable institutions must be handled as any other financial transaction. The donating bank or institution should crosscheck the recipient names against OFAC's sanctions lists and assure that the donations are in compliance with OFAC sanctions programs. [09-10-2002]

---

52. Can U.S. financial institutions open correspondent accounts for Iraqi financial institutions, or process funds transfers to and from Iraqi financial institutions?

Yes, U.S. financial institutions are authorized to open correspondent accounts for, and process funds transfer to or on behalf of Iraqi financial institutions. [07-27-2004]

---

95. Does a financial institution have the obligation to screen account beneficiaries for compliance with OFAC regulations?

"Property," as defined in OFAC regulations, includes most products that financial institutions offer to their clients. "Property interest," as defined by OFAC, includes any interest whatsoever, direct or indirect, present, future or contingent. Given these definitions and as a matter of sound banking practice, it is prudent for financial institutions to screen account beneficiaries upon account opening, while updating account information, when performing periodic screening and, most definitely, upon disbursing funds. Where there is a property interest of a sanctions target under a blocking program, the property must be blocked. Beneficiaries include, but are not limited to, trustees, children, spouses, non-spouses, entities and powers of attorney. [12-04-2006]

---

116. On February 14, 2008, OFAC issued guidance stating that the property and interests in property of an entity are blocked if the entity is owned, directly or indirectly, 50% or more by a person whose property and interests in property are blocked pursuant to an Executive Order or regulations administered by OFAC. We act as an intermediary bank in wire transfers between other banks. Does OFAC expect banks that are acting as financial intermediaries to research

non-account parties that do not appear on the SDN List, but are involved with or referenced in transactions that are processed on behalf of correspondents?

A wire transfer in which an entity has an interest is blocked property if the entity is 50% or more owned by a person whose property and interests in property are blocked. This is true even in instances where such a transaction is passing through a U.S. bank that (1) is operating solely as an intermediary, (2) does not have any direct relationship with the entity (e.g., the entity is a non-account party), and (3) does not know or have reason to know the entity's ownership or other information demonstrating the blocked status of the entity's property. In instances where all three conditions are met, notwithstanding the blocked status of the wire transfer, OFAC would not expect the bank to research the non-account parties listed in the wire transfer that do not appear on the SDN List and, accordingly, would not pursue an enforcement action against the bank for having processed such a transaction.

If a bank handling a wire transfer currently has information in its possession leading the bank to know or have reason to know that a particular individual or entity involved with or referenced in the wire transfer is subject to blocking, then the bank will be held responsible if it does not take appropriate steps to ensure that the wire transfer is blocked.

OFAC expects banks to conduct due diligence on their own direct customers (including, for example, their ownership structure) to confirm that those customers are not persons whose property and interests in property are blocked.

With regard to other types of transactions where a bank is acting solely as an intermediary and fails to block transactions involving a sanctions target, OFAC will consider the totality of the circumstances surrounding the bank's processing of the transaction, including the factors listed above, to determine what, if any, enforcement action to take against the bank. [01-15-2015]

Securities Industry (Print)

---

335. Firms operating in the securities industry as custodians and securities intermediaries often face the question of how to accurately identify the beneficial owner of assets within an account or transaction. What can these firms do to protect themselves from the risk of directly or indirectly providing services to—or dealing in property in which there is an ownership or other interest of—parties subject to sanctions?

OFAC encourages firms operating in the securities industry, including securities intermediaries and custodians, to implement measures that mitigate the risk of providing services to, or dealing in property in which there is an ownership or other interest of, parties subject to U.S. sanctions. Such measures should be tailored to and commensurate with the sanctions risk posed by a firm's business activities. Best practices include:

- Making customers aware of the firm's U.S. sanctions compliance obligations and having customers agree in writing not to use their account(s) with the firm in a manner that could cause a violation of OFAC sanctions. Sanctions may be implicated when the United States is the jurisdiction of issuance or custody of an underlying security or when a U.S. person acts as a custodian or other service provider.
- Conducting due diligence, including through the use of questionnaires and certifications, to identify customers who do business in or with countries or persons subject to U.S. sanctions. Such customers may warrant enhanced due diligence because of an increased risk that they will use their accounts to hold assets or conduct transactions for third parties subject to sanctions.
- Imposing restrictions and heightened due diligence requirements on the use of certain products or services by customers who are judged to present a high risk from an OFAC sanctions perspective. Restrictions might include limitations on the use of omnibus accounts, where a lack of transparency can be exploited in order to circumvent OFAC regulations.
- Making efforts to understand the nature and purpose of non-proprietary accounts, including requiring information regarding third parties whose assets may be held in the accounts. Red flags may arise relating to geographic areas or the nesting of third-party assets.
- Monitoring accounts to detect unusual or suspicious activity – for example, unexplained significant changes in the value, volume, and types of assets within an account. These types of changes may indicate that a customer is facilitating new business for third parties that has not been vetted for possible sanctions implications. [01-23-2014]

Additional Iran-related Questions from Financial Institutions

For additional information regarding Iran, please see the following topic.

Questions on Virtual Currency

Print this topic

559. For purposes of OFAC sanctions programs, what do the terms "virtual currency," "digital currency," "digital currency wallet," and "digital currency address" mean?

Virtual currency is a digital representation of value that functions as (i) a medium of exchange; (ii) a unit of account; and/or (iii) a store of value; is neither issued nor guaranteed by any jurisdiction; and does not have legal tender status in any jurisdiction.

Digital currency includes sovereign cryptocurrency, virtual currency (non-fiat), and a digital representation of fiat currency.

A digital currency wallet is a software application (or other mechanism) that provides a means for holding, storing, and transferring digital currency. A wallet holds the user's digital currency addresses, which allow the user to receive digital currency, and private keys, which allow the user to transfer digital currency. The wallet also maintains the user's digital currency balance. A wallet provider is a person (individual or entity) that provides the software to create and manage wallets, which users can download. A hosted wallet provider is a business that creates and stores a digital currency wallet on behalf of a customer. Most hosted wallets also offer exchange and payments services to facilitate participation in a digital currency system by users.

A digital currency address is an alphanumeric identifier that represents a potential destination for a digital currency transfer. A digital currency address is associated with a digital currency wallet. [03-19-2018]

---

560. Are my OFAC compliance obligations the same, regardless of whether a transaction is denominated in digital currency or traditional fiat currency?

Yes, the obligations are the same. U.S. persons (and persons otherwise subject to OFAC jurisdiction) must ensure that they block the property and interests in property of persons named on OFAC's SDN List or any entity owned in the aggregate, directly or indirectly, 50 percent or more by one or more blocked persons, and that they do not engage in trade or other transactions with such persons.

As a general matter, U.S. persons and persons otherwise subject to OFAC jurisdiction, including firms that facilitate or engage in online commerce or process transactions using digital currency, are responsible for ensuring that they do not engage in unauthorized transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property, or engaging in prohibited trade or investment-related transactions. Prohibited transactions include transactions that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate prohibitions imposed by OFAC under various sanctions authorities. Additionally, persons that provide financial, material, or technological support for or to a designated person may be designated by OFAC under the relevant sanctions authority.

Persons including technology companies; administrators, exchangers, and users of digital currencies; and other payment processors should develop a tailored, risk-based compliance program, which generally should include sanctions list screening and other appropriate measures. An adequate compliance solution will depend on a variety of factors, including the type of business involved. There is no single compliance program or solution suitable for every circumstance. [03-19-2018]

---

561. How will OFAC use its existing authorities to sanction those who use digital currencies for illicit purposes?

The United States' whole-of-government strategies to combat global threats such as terrorism, transnational organized crime, malicious cyber activity, narcotics trafficking, weapons of mass destruction (WMD) proliferation, and human rights abuses include targeting an array of activities, including the use of digital currencies or other emerging payment systems to conduct proscribed financial transactions and evade U.S. sanctions. The strategies draw from a broad range of tools and authorities to respond to the growing and evolving threat posed by malicious actors using new payment mechanisms. OFAC will use sanctions in the fight against criminal and other malicious actors abusing digital currencies and emerging payment systems as a complement to existing tools, including diplomatic outreach and law enforcement authorities. To strengthen our efforts to combat the illicit use of digital currency transactions under our existing authorities, OFAC may include as identifiers on the SDN List specific digital currency addresses associated with blocked persons. [03-19-2018]

---

562. How will OFAC identify digital currency-related information on the SDN List?

OFAC may add digital currency addresses to the SDN List to alert the public of specific digital currency identifiers associated with a blocked person. OFAC's digital currency address listings are not likely to be exhaustive. Parties who identify digital currency identifiers or wallets that they believe are owned by, or otherwise associated with, an SDN and hold such property should take the necessary steps to block the relevant digital currency and file a report with OFAC that includes information about the wallet's or address's ownership, and any other relevant details. [03-19-2018]

---

563. What is the structure of a digital currency address on OFAC's SDN List?

Digital currency addresses listed on the SDN List include their unique alphanumeric identifier (up to 256 characters) and identify the digital currency to which the address corresponds (e.g., Bitcoin (XBT), Ethereum (ETH), Litecoin (LTC), Neo (NEO), Dash (DASH), Ripple (XRP), Iota (MIOTA), Monero (XMR), and Petro (PTR)). Each digital currency address listed on the SDN list will have its own field: the structure will always begin with “Digital Currency Address”, followed by a dash and the digital currency’s symbol (e.g., “Digital Currency Address - XBT”, “Digital Currency Address - ETH”). This information is followed by the unique alphanumeric identifier of the specific address. [06-06-2018]

---

594. Is it possible to query a digital currency address using OFAC’s Sanctions List Search tool?

No, it is not currently possible to query for digital currency addresses using OFAC’s Sanctions List Search tool. Alternatively, OFAC’s SDN List and other OFAC sanctions lists are available in a number of file formats and downloads, which can be used to identify and screen for listed digital currency addresses. Additional information on OFAC list file formats and downloads, can be accessed here. [06-06-2018]

---

646. How do I block digital currency?

Once it has been determined that your institution is holding digital currency that is required to be blocked pursuant to OFAC’s regulations, you must ensure that access to that digital currency is denied to the blocked person and that your institution complies with OFAC regulations related to blocked assets. Institutions may choose, for example, to block each digital currency wallet associated with the digital currency addresses that OFAC has identified as being associated with blocked persons, or opt to use its own wallet to consolidate wallets that contain the blocked digital currency (similar to an omnibus account) titled, for example, “Blocked SDN Digital Currency.” Each of these methods is satisfactory, so long as there is an audit trail that will allow the digital currency to be unblocked only when the legal prohibition requiring the blocking of the digital currency ceases to apply. The institution is not obligated to convert the blocked digital currency into traditional fiat currency (e.g., U.S. dollars). Blocked digital currency must be reported to OFAC within 10 business days. Questions about whether a transaction should be blocked should be directed to OFAC at 202-622-2490 or ofac_feedback@treasury.gov. [11-28-2018]

---

647. Should an institution tell its customer that it blocked access to their digital currency and, if so, how does the institution explain it to the customer?

An institution may notify its customer that it has blocked digital currency pursuant to OFAC regulations. The customer has the right to apply for the unblocking and release of the digital currency.

To apply online to have the virtual currency released, please go to OFAC’s online application page. [11-28-2018]

Return to the OFAC FAQ Index