SecurePoint USA

Whitepaper



OFAC sanctions screening best practices

Which lists to screen, how matching and review work, and the records to keep

OFAC · BIS · EU · UK · UN

A practitioner guide to sanctions and restricted-party screening for organizations that host visitors and work with vendors. It explains what a match on each major list means for a U.S. organization, how name matching and match review work, how the 50 Percent Rule reaches entities no list names, and which records show reasonable care.

Written for
Compliance teams, risk managers, counsel

Last reviewed
November 7, 2026

First published
March 18, 2026

Read online
securepointusa.com/resources/whitepapers/ofac-sanctions-screening

Informational only. Not legal, regulatory, export-control, or compliance advice. Not a substitute for review by qualified counsel or the compliance professionals who know your obligations.

Contents

1. Executive summary 3
2. Where screening fits in a sanctions program 3
3. Which lists to screen, and what a match means 4
4. How name matching works 6
5. Ownership and the 50 Percent Rule 8
6. Reviewing a possible match 9
7. Records that show reasonable care 10
8. Lessons from enforcement 11
9. Questions to ask of any screening tool 12

Sources and revision history 13

About SecurePoint USA 16

Key takeaways

- Screening is one internal control inside a risk-based sanctions program. It does not replace the program, and no tool makes an organization compliant.
- Each list has its own legal effect. An SDN match, an Entity List match and an INTERPOL Red Notice call for different responses.
- Name similarity only nominates a candidate. Dates of birth, nationality and other identifiers decide whether it is a match, and a person should make that call.
- An entity owned 50 percent or more by blocked persons is blocked even when no list names it.
- OFAC records must be kept for ten years (31 CFR 501.601).

Last reviewed November 7, 2026 against the sources listed at the end of this paper and against SecurePoint's product as it stood that day.

1. Executive summary

The Office of Foreign Assets Control (OFAC), part of the U.S. Department of the Treasury, administers and enforces economic sanctions against targeted countries and regimes and against individuals and entities such as terrorists, narcotics traffickers and proliferators of weapons of mass destruction. Its prohibitions apply to all U.S. persons wherever they are, and to anyone in the United States, so they reach defense contractors, universities and schools, hospitals and every other kind of organization, not only banks.

OFAC can impose civil penalties on a **strict liability** basis, so a dealing with a blocked person can be a violation even when nobody knew. Diligence still shapes the outcome. Under its Economic Sanctions Enforcement Guidelines, OFAC weighs whether conduct was willful or reckless, what the organization knew, the harm to the sanctions program, and the existence, nature and adequacy of the organization's compliance program.

Screening is how most organizations find out who they are dealing with. This paper covers which lists to screen and what each one means, how name matching and match review work, how ownership extends the SDN List beyond the names on it, which records let an organization show its decisions later, and what OFAC's screening cases teach.

2. Where screening fits in a sanctions program

OFAC's regulations do not require a formal compliance program, and OFAC does not prescribe lists, matching algorithms or match thresholds. Its Framework for OFAC Compliance Commitments, published in May 2019, strongly encourages a risk-based program, with screening tools calibrated to the organization's risk and tested routinely, and the Enforcement Guidelines weigh such a program when OFAC decides how to respond to an apparent violation. The Framework names five components.

Management commitment	Senior management approves the program, gives it resources and authority, and backs the people who run it.
Risk assessment	A documented view of where the organization's sanctions exposure sits: its customers, suppliers, visitors, products, geographies and payment flows. It decides who is screened, against what, and when.
Internal controls	Written policies and procedures, screening among them, that identify, escalate and report prohibited activity and keep a record of what was done.
Testing and auditing	Independent checks that the controls work as designed, including the screening tool's lists, settings and results.

Training	Role-based training for the people who run the controls, matched to the organization's risk.

Who to screen in a visitor and vendor program

- Visitors, when they pre-register and again at check-in.
- The companies visitors represent, and the vendors, contractors and service providers the organization pays.
- The owners of those companies, where the risk assessment calls for it (see section 5).
- Payors and other counterparties to incoming payments, for schools and other organizations that receive money from abroad.

> **A clean result is dated**
>
> OFAC and the other publishing agencies add and remove names regularly, so a screening result is current only as of the moment it ran. Re-screen continuing relationships on a schedule your risk assessment sets, and screen again before a decision that matters.

3. Which lists to screen, and what a match means

A restricted-party list is not one thing. Each list comes from a different authority, and a match carries a different legal effect for a U.S. organization: some lists prohibit dealings outright, some require an export license, and some bind only people within another jurisdiction's reach. Knowing which is which decides what a reviewer does with a match.

Table 1. Major lists and what a match means for a U.S. organization

List	Published by	What a match means	In SecurePoint
SDN List	Treasury (OFAC)	U.S. persons may not deal with the listed person, or in its property or interests in property, without OFAC authorization. Property that comes into a U.S. person's possession must be blocked and reported.	On by default
Sectoral Sanctions Identifications List	Treasury (OFAC)	Russia's financial, energy and defense sectors, under directives issued under Executive Order 13662. A listing restricts specified dealings, such as new debt beyond set terms; it does not block the entity unless it is also on the SDN List.	On by default

List	Published by	What a match means	In SecurePoint
Entity List	Commerce (BIS)	Each entry sets a license requirement for exporting, reexporting or transferring items subject to the EAR to the listed party, usually reviewed under a presumption of denial. A visit is not itself prohibited, but releasing controlled technology during one can require a license.	On by default
Denied Persons List	Commerce (BIS)	The party's export privileges are denied, and no one may take part with it in a transaction involving items subject to the EAR.	On by default
DDTC debarred parties	State (DDTC)	Debarred parties may not take part, directly or indirectly, in activities the ITAR regulates.	Off until enabled
UK Sanctions List	UK government (FCDO)	Binds people and business within the UK's reach: UK nationals and companies anywhere, and conduct in the UK. For a U.S. organization with no UK subsidiary, branch, staff or business, a UK-only designation is a risk signal rather than an obligation.	On by default
EU Financial Sanctions Files	European Commission	Binds EU nationals and companies anywhere, and business done in the EU. The reasoning for the UK list applies.	On by default
UN Security Council Consolidated List	United Nations	Member states give UN designations effect in their own law. The United States does so largely through OFAC programs, so most UN-listed parties also appear on the SDN List.	On by default
SAM.gov exclusions	General Services Administration	Federal agencies may not award contracts to excluded parties, and the FAR restricts federal contractors from subcontracting with them.	Off until enabled
LEIE	HHS Office of Inspector General	Federal health care programs do not pay for items or services furnished by excluded individuals or entities. Relevant to health care employers and their contractors.	Off until enabled
FBI Most Wanted and INTERPOL Red Notices	FBI and INTERPOL	Not sanctions: a match creates no prohibition on dealing. It is a security matter for the facility to handle under its own procedures and, where appropriate, with law enforcement. A Red Notice is a request to locate a person, not an arrest warrant.	On by default

Which lists SecurePoint screens, and what a match does

Every screen searches all of an organization’s enabled lists in one pass. Beyond the lists in the table, SecurePoint screens the UFLPA Entity List, the Section 1260H list of Chinese military companies, Federal Reserve enforcement actions, France’s national asset-freeze register (DGT), Singapore MAS enforcement actions, World Bank and Inter-American Development Bank debarments, and the OpenSanctions dataset by default.

Lists differ in what a match does. A strong match on the SDN List, the UN, EU or UK lists, or the BIS Denied Persons List blocks check-in until a person decides. A match on the SSI List or France’s asset-freeze register is held for a reviewer and does not block on its own. The World Bank, IADB, Federal Reserve, Singapore MAS, UFLPA and Section 1260H lists are searched on every screen and affect the decision only when no other list matched.

The DDTC debarred list, SAM.gov exclusions, the LEIE and politically exposed persons stay off until an organization turns them on. By default, adverse media is recorded as review context and does not change the screening decision. Check which sources your own account has enabled rather than assuming every source named here is active.

OFAC’s lists come from Treasury’s sanctions list service, the UN list from the United Nations, and the BIS lists through the Consolidated Screening List; the UK, EU, French, INTERPOL and several other lists come through OpenSanctions’ published copies of the official lists. OFAC SDN and SSI, the BIS Denied Persons List and the UK, EU and UN lists refresh daily; the BIS Entity List and most other sources refresh weekly.

4. How name matching works

Exact matching catches only the spellings a list already publishes as aliases. It misses true matches that differ in transliteration, word order or a typing error. The same Arabic name is written Muhammad, Mohammed or Mohamed. Russian names have several romanization systems. Chinese names appear in Pinyin, in older Wade-Giles spellings or in regional forms, with the family name first or last. Companies add and drop legal forms such as LLC, Ltd. and GmbH. Fuzzy matching scores how similar two names are, and a threshold decides which scores become candidates.

Exact match	Character-for-character comparison after normalizing case, accents and punctuation. Highest confidence, but it finds only direct hits.
Normalized match	Comparison after removing legal forms such as Inc., Ltd., GmbH and LLC, and standardizing spacing and punctuation. Catches variants of company names.
Jaro-Winkler	A similarity score that rewards shared characters and a shared beginning. Good at transposed letters, missing letters and short misspellings.

Levenshtein distance	The number of single-character edits that turn one name into another. Useful for typing errors.
Double Metaphone	Encodes how a romanized name sounds, so spellings such as Mohammed and Muhammad can share a code. It works on names already written in Latin letters and follows English pronunciation, so it does less for Chinese romanizations.
Trigram similarity	Compares the overlapping three-character pieces of two names. Useful for partial matches and reordered names.

Every threshold is a trade. Set it low and reviewers spend their time on namesakes; set it high and true matches pass. Secondary identifiers settle what similarity cannot: the date of birth, nationality, place of birth, addresses and identification numbers on the list entry. OFAC's guidance on assessing name matches (FAQ 5) tells screeners to compare those details before treating a name hit as a match, and notes that OFAC does not confirm or deny potential matches.

How SecurePoint scores a name

Sanctions screening in SecurePoint scores each candidate with Jaro-Winkler similarity, compares the name in several word orders so a surname-first entry still matches, and looks up each listed alias exactly. OFAC's own native-script spellings of SDN names are stored as aliases, and names entered in Cyrillic or Arabic script are transliterated before matching. Common names must clear a stricter minimum. The default match threshold is 0.75.

Candidates that screening rules dismiss, such as a common name whose country or date of birth does not match, are recorded in the decision trace rather than dropped, so a reviewer can see why a name did not match. The weighted combination of the six techniques above is used in three other places: to match owners in ownership records against the SDN List, to match names in adverse-media monitoring, and to score politically exposed persons where that screening is on.

When a screen cannot be completed

A screen that SecurePoint cannot complete is held for review rather than cleared. A search that did not finish, a clean result resting on a critical list (OFAC SDN, BIS, UN, UK or EU) more than twice past its refresh age, and a name in a script the matcher cannot read that returns no match are all held. Screens that ran on degraded data are queued and run again once the data is current. Each screen records the list versions and freshness it used.

5. Ownership and the 50 Percent Rule

Under OFAC's 50 Percent Rule, an entity owned 50 percent or more, directly or indirectly, individually or in the aggregate, by one or more blocked persons is itself blocked, whether or not it is named on any list. Many such entities never appear on the SDN List, so name screening alone cannot find them.

Indirect ownership counts only through entities that are themselves blocked (OFAC FAQ 401). A blocked company's stakes count in full toward the companies it invests in; a stake held through a company that is not blocked carries nothing forward.

A worked example

- Blocked Person X owns 50 percent of Company A. Company A is blocked.
- Company A owns 30 percent of Company B, and Blocked Person Y owns 20 percent of Company B. Blocked persons own 50 percent of Company B in the aggregate, so Company B is blocked.
- Blocked Person X owns 40 percent of Company C, which owns 60 percent of Company D. Company C is not blocked, so Company D is not blocked through it, although both call for caution.

The rule turns on ownership, not control. An entity that blocked persons control but own less than 50 percent of is not blocked by the rule, though OFAC may designate it, and OFAC urges caution with entities in which blocked persons hold significant ownership or control (FAQ 398). Finding these entities takes ownership data, such as company registers and beneficial-ownership disclosures, and it is only as complete as that data.

> **The BIS Affiliates Rule**
>
> Separately, BIS has stayed its Affiliates Rule, which applies Entity List and Military End-User List restrictions to entities owned 50 percent or more by listed parties, through January 10, 2027, as published in the Federal Register; it is scheduled to take effect January 11, 2027 absent further BIS action. Confirm its status at bis.gov before relying on it. A match against the BIS Entity List or Military End-User List is held for manager review, and reaching a scheduled date does not change that.

How SecurePoint checks ownership

SecurePoint checks the ownership of entities, such as vendors and other counterparties, submitted through the screening API or the compliance team's ownership lookup. Individual visitors are screened by name; ownership analysis does not run on them at check-in.

It traces ownership chains up to ten levels deep (the compliance lookup defaults to five) through ownership records drawn from OpenSanctions and Wikidata relationship data, so coverage and currency are limited to what those records hold. Stakes held by parties on the SDN List are added together, and a stake passes through an intermediate company only when that company is itself blocked, the way FAQ 401 counts it. An unknown stake, or a chain cut at the depth limit, is reported as unresolved, not as zero.

By default the ownership result is recorded with the screening result and does not change the decision. An organization can turn enforcement on: an entity at or above 50 percent is then blocked pending review, and an entity the ownership records do not cover is held for review instead of approved. Either way, the owners and their attributed stakes are recorded with the result.

6. Reviewing a possible match

Screening produces candidates; review decides what they are. A workable process clears what rules can clear, holds real ambiguity for a trained person, and records both, so reviewers spend their time on the cases that need judgment. OFAC's FAQ 5 sets out the sequence.

1. **Identify the list**
   Confirm which list the candidate comes from. A match on a list another agency publishes follows that agency's rules (see section 3).
2. **Compare the full entry**
   Compare the entry's date of birth, nationality, identification numbers, addresses and aliases with what you know. If the details rule the match out, record why and proceed.
3. **Escalate a likely match**
   If several details agree, or the match cannot be ruled out, escalate under your procedures and check whether an OFAC license or exemption applies.
4. **Stop, block or reject**
   Do not proceed with a confirmed match. Where property or a transaction is involved, OFAC's rules require the property to be blocked or the transaction rejected. Involve counsel.
5. **Report and record**
   Report blocked property and rejected transactions to OFAC within 10 business days (31 CFR 501.603 and 501.604), and keep a complete record of the review. SecurePoint does not file these reports; your organization does.

How SecurePoint decides and holds

Two numbers decide a screen. A listed name becomes a candidate when its similarity is 0.75 or higher, and higher for common names. The screen's risk score then sets the outcome. Under 0.40 it is approved automatically unless your organization turns automatic approval off (it is on by default) or the visit is flagged as export-control relevant. From 0.40 up to 0.90 it is held for a reviewer. A result at 0.90 or above blocks check-in until a person decides. A screen with no candidate is approved, and a weak candidate on a list outside the SDN, UN, EU, UK and BIS Denied Persons lists with no country to corroborate it can score into the approval band; it is recorded in the decision trace. No rule issues a final denial.

The reviewer sees the decision trace: the screened name, each candidate's list, program, country and similarity score, and why other candidates were dismissed. The reviewer approves, denies, escalates for senior review, or marks the result as not a match. A not-a-match decision always needs a note. Clearing a candidate that scored 90 percent or more, or one on the SDN List, the BIS Entity or Denied Persons List or the ITAR debarred list, needs a reason chosen from a fixed list; at 95 percent or more it also needs a recorded date-of-birth or ID mismatch, or a second reviewer. Approving a real match needs the license, exemption or legal approval reference and who issued it. Denials and escalations require a reason code, a decision on a case that changed after the reviewer opened it is refused, and the decision, the reviewer and the reason are written to the audit log.

By default an AI provider named on the Subprocessors page also writes a summary of each screened name for the reviewer, labelled as AI-generated. The summary is shown with the result; it does not change the risk score or the decision.

7. Records that show reasonable care

Every person engaging in a transaction subject to OFAC's regulations must keep a full and accurate record of it for ten years (31 CFR 501.601). OFAC extended the period from five years, effective March 12, 2025. Screening records are what let an organization show, years later, what it knew and what it did.

What to be able to show

- Who or what was screened, against which lists, and how current each list was at the time.
- The matching method and threshold in force.
- The full result, including the candidates found and why each was cleared or held, not only pass or fail.
- Who decided each held result, when, and the reason they recorded.
- Where software or AI suggested a decision, what it suggested and whether a person accepted or overrode it.
- Screening at each point the program requires, such as pre-registration and check-in.
- An audit trail that shows whether a record changed after the fact.
- Retention for at least the period each applicable regime requires.

What SecurePoint records

Screening completions and review decisions are written to an append-only, hash-chained audit log that application users cannot edit or delete, with a verifier that checks the chain. Each entry's SHA-256 hash covers its sequence, action, actor, subject, organization and time and includes the previous entry's hash, so the verifier can detect a removed or reordered entry. Audit logs, screening results and review decisions are kept for ten years.

Evidence and report exports cover screening activity, review decisions and the audit trail, with a SHA-256 checksum recorded for each export so a recipient can confirm a file has not changed.

8. Lessons from enforcement

Each of these OFAC settlements turned on screening or due diligence: a filter too weak to flag close matches, a missed spelling, a slow list update, an owner nobody traced, or data the company held but did not screen. The figures are the amounts OFAC announced. SecurePoint does not claim any tool would have prevented them.

Table 2. OFAC settlements that turned on screening and due diligence

Case	Settlement	What OFAC described	The lesson
Bank of America (2026)	$11,662,930	475 apparent violations across programs including Russia, Iran and Burma, involving payments with blocked banks, slow watchlist updates, and alerts that gave low priority to customers matching blocked persons by name and date of birth.	A match on name and date of birth is a high-priority alert, and list updates have to reach the screening tool quickly.
Extreme Networks (2026)	$1,529,685	Between 2018 and 2022 it shipped hardware and services nine times to a Russian defense manufacturer that was blocked because a designated company owned a majority of it, before the manufacturer was listed in its own name. OFAC treated the case as voluntarily self-disclosed and egregious.	An unlisted company can be blocked through its owner. Vendor and customer screening needs ownership, not names alone.
Pegasus Worldwide Logistics (2026)	$175,015	A freight forwarder helped import a machine from a blocked supplier. The supplier's new name produced no hit, while the phone number and email address on the SDN entry still appeared on the shipping papers.	Names change. Compare the identifiers on the list entry, not the name alone.

Case	Settlement	What OFAC described	The lesson
IMG Academy (2026)	$1,720,000	A Florida sports boarding school signed tuition agreements with, and accepted payments from, two parents on the SDN List designated under the Kingpin Act. OFAC said minimal due diligence would have revealed they were sanctioned.	Schools and other non-financial organizations are in scope. Screen the people who pay, not only the people who attend.
Payoneer (2021)	$1,385,901.40	2,220 apparent violations. Weak algorithms let close matches to SDN entries go unflagged, flagged payments were released automatically during backlogs, and location data was not used to catch sanctioned regions.	Tune and test the matching, and never let a backlog release held items.
BitPay (2021)	$507,375	Screened its merchant customers against the SDN List but not the location data, including IP addresses, it held about those merchants' buyers, who were apparently in Crimea, Cuba, Iran, North Korea, Sudan and Syria.	Screen the data you already hold, not only the names you are given.
Amazon.com (2020)	$134,523	Its screening did not flag orders to addresses such as "Yalta, Krimea" or to Iran's embassies, and in some cases missed correctly spelled SDN names and addresses.	Screen addresses and spelling variants of sanctioned places as well as names.
Apple (2019)	$466,912	Its screening tool did not match "SIS DOO" in Apple's records to "SIS d.o.o." on the SDN List, and Apple did not screen the account's administrator, who was also designated.	Normalize legal forms and case before comparing, and screen the individuals behind an account.

9. Questions to ask of any screening tool

Whatever tool an organization uses, these are the questions an examiner, an auditor or opposing counsel will ask about the screening behind a decision.

- Which lists does it screen by default, which are optional, and can you see when each was last refreshed?
- What matching method and threshold does it use, and is a change to them recorded?
- Does it use dates of birth, nationality and other identifiers, or names alone?
- When it dismisses a candidate, does it record why?
- What happens when a search fails or a list is out of date: is the result held, or cleared?
- Who decides a held result, and does the record show their reasoning?

- Does it check the ownership of entities, and where does its ownership data come from?
- Can its audit trail show that a record has not been changed, and can you export a complete case file for an examiner?

Sources and revision history

First published March 2026. Last reviewed November 7, 2026 against the sources below and against SecurePoint's product as it stood that day. The sources are listed for traceability, not as endorsements. Confirm current text with the issuing agency before relying on a citation.

[1] **OFAC: A Framework for OFAC Compliance Commitments (May 2019)**
https://ofac.treasury.gov/media/16331/download
The five components of a sanctions compliance program, and the root causes of breakdowns OFAC has seen, including outdated lists and missed spelling variants.

[2] **31 CFR Part 501, Appendix A: Economic Sanctions Enforcement Guidelines**
https://www.law.cornell.edu/cfr/text/31/appendix-A_to_part_501
The general factors OFAC weighs in an apparent violation, including willfulness, awareness and the compliance program.

[3] **OFAC FAQ 5: Assessing a potential name match**
https://ofac.treasury.gov/faqs/5
The steps for verifying or ruling out a potential match, updated September 9, 2026.

[4] **OFAC FAQ 398: Control under the 50 Percent Rule**
https://ofac.treasury.gov/faqs/398
The rule turns on ownership, not control.

[5] **OFAC FAQ 401: The 50 Percent Rule**
https://ofac.treasury.gov/faqs/401
Aggregate and indirect ownership, including that an interest passes only through entities that are themselves blocked.

[6] **31 CFR § 501.601: Records and recordkeeping requirements**
https://www.ecfr.gov/current/title-31/section-501.601
Ten-year record period, effective March 12, 2025.

[7] **31 CFR §§ 501.603 and 501.604: Reports of blocked property and rejected transactions**
https://www.law.cornell.edu/cfr/text/31/501.604
Reports due to OFAC within 10 business days.

[8] **BIS Affiliates Rule: 90 FR 47201, its suspension at 90 FR 50857, and the extension in FR Doc. 2026-22793**
https://www.federalregister.gov/documents/2025/11/12/2025-19846/one-year-suspension-of-expansion-of-end-user-controls-for-affiliates-of-certain-listed-entities
BIS filed an extension of the stay through January 10, 2027 on November 5, 2026, effective November 9, 2026.

[9] **OFAC Enforcement Release: Extreme Networks, Inc. (October 27, 2026)**
https://ofac.treasury.gov/recent-actions/20261027
$1,529,685 settlement; exports to a Russian defense manufacturer blocked through its majority owner.

[10] **OFAC Enforcement Release: Pegasus Worldwide Logistics (October 9, 2026)**
https://ofac.treasury.gov/recent-actions/20261009
$175,015 settlement; an import from a blocked supplier.

[11] **OFAC Enforcement Release: Payoneer Inc. (July 2021)**
https://ofac.treasury.gov/media/911571/download
$1,385,901.40 settlement of 2,220 apparent violations.

[12] **OFAC Enforcement Release: BitPay, Inc. (February 18, 2021)**
https://ofac.treasury.gov/recent-actions/20210218
$507,375 settlement of 2,102 apparent violations.

[13] **OFAC Enforcement Release: Amazon.com, Inc. (July 2020)**
https://ofac.treasury.gov/media/44311/download
$134,523 settlement.

[14] **OFAC Enforcement Release: Apple Inc. (November 2019)**
https://ofac.treasury.gov/media/25931/download
$466,912 settlement.

[15] **OFAC Enforcement Release: Bank of America, N.A. (October 13, 2026)**
https://ofac.treasury.gov/recent-actions/20261013_33
$11,662,930 settlement of 475 apparent violations across several sanctions programs.

[16] **OFAC Enforcement Release: IMG Academy, LLC (February 12, 2026)**
https://ofac.treasury.gov/recent-actions/20260212
$1,720,000 settlement of 89 apparent violations of the Kingpin Act regulations.

[17] **15 CFR Part 744: Control Policy, End-User and End-Use Based (Entity List)**
https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-744
The Entity List is Supplement No. 4 to Part 744.

[18] **Consolidated Screening List (International Trade Administration)**
https://www.trade.gov/consolidated-screening-list
Combined Commerce, State, and Treasury lists, including the Entity List and the Denied Persons List.

[19] **UK Sanctions List (Foreign, Commonwealth & Development Office)**
https://www.gov.uk/government/publications/the-uk-sanctions-list
The only source of UK sanctions designations since OFSI closed its Consolidated List on January 28, 2026.

[20] **European Commission: EU sanctions and the Financial Sanctions Files**
https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/overview-sanctions-and-related-resources_en
Overview of EU restrictive measures and the consolidated list of persons, groups, and entities subject to EU financial sanctions.

Revision history

November 7, 2026 Rewritten so the web page and the PDF carry the same text. Added what a match on each list means for a U.S. organization, OFAC's steps for assessing a name match, the 10-business-day reports for blocked property and rejected transactions, and a worked example of indirect ownership. Corrected the account of automatic approval (on by default below a risk score of 0.40), stated which lists block and which only hold for review, and described when a screen is held because it could not be completed. Replaced four bank and export-evasion cases with OFAC settlements that turned on screening, including Extreme Networks and Pegasus Worldwide Logistics (October 2026), and removed an adverse-media source description the product does not deliver.

October 23, 2026 Renamed the UK source to the UK Sanctions List, the only UK source since OFSI closed its Consolidated List on January 28, 2026, and corrected the EU list's name to the Financial Sanctions Files. Added OFAC's October 2026 Bank of America settlement, which turned on watchlist updates and alert priority, and replaced an unsourced transliteration figure with examples.

October 17, 2026 Updated how the paper states the status of the BIS Affiliates Rule.

September 27, 2026 Replaced the source count with the name of each list screened, corrected product, regulatory and enforcement statements, and stated OFAC's ten-year recordkeeping period.

About SecurePoint USA

SecurePoint USA builds visitor management and restricted-party screening software for defense contractors, manufacturers, research facilities and schools. It screens visitors and other parties against government sanctions and restricted-party lists, holds possible matches for a person to decide, issues badges once a site's required evidence is in place, and keeps an append-only, hash-chained audit log that application users cannot edit or delete, with a verifier that checks the chain. SecurePoint does not file with OFAC, BIS or DDTC, and it does not make an organization compliant: it supplies records for the program your organization runs.

See a screening decision from start to finish.

Request a demo to watch a visitor screened, a possible match held for review, and the decision recorded in the audit log, using demonstration data.

- Request a demo: securepointusa.com/request-demo
- Read this paper online: securepointusa.com/resources/whitepapers/ofac-sanctions-screening
- All whitepapers: securepointusa.com/resources/whitepapers

This whitepaper is provided for general informational purposes only and does not constitute legal, regulatory, export-control, or compliance advice.

It is not a substitute for review by qualified counsel, or by the compliance, security, export-control or assessment professionals familiar with your organization, its contracts, facilities and obligations.

Regulatory citations, enforcement examples, and statistics reflect publicly available information believed to be accurate as of the "Last reviewed" date on the cover page. Regulations and enforcement priorities change; consult primary sources before acting on anything in this document.

Statements about SecurePoint USA capabilities describe product behavior as of the "Last reviewed" date, not a contractual commitment. Capability fit for any specific environment must be confirmed during scoping.

© 2026 SecurePoint USA LLC. All rights reserved.