

WHITEPAPER

The New Education Compliance Reality in 2026

Why sanctions screening, payment-chain review, and audit-ready documentation can no longer be treated as optional campus controls.

Prepared for: School heads, CFOs, business officers, general counsel, compliance leaders, admissions teams, finance teams, and trustees

\$1.72M

OFAC Settlement

\$5.2B

Foreign Funding

8,300+

Transactions

90 Day

Action Plan

OFAC

Section 117

Education

SecurePoint USA

securepointusa.com

Originally published: 2026-03-12 | Last reviewed: 2026-05-10

March 2026

01 Executive Summary

For years, many schools assumed sanctions compliance was mainly a banking problem. That assumption no longer holds.

In February 2026, OFAC announced a \$1.72 million settlement with IMG Academy tied to sanctions compliance failures involving tuition payments and enrollment relationships.

Around the same time, the U.S. Department of Education released 2025 foreign funding disclosures showing more than 8,300 transactions worth over \$5.2 billion in reportable foreign gifts and contracts, reinforcing that foreign-source oversight in education is now a matter of public accountability and national-security attention.

- International enrollment creates sanctions and counterparty risk
- Tuition and donor relationships can create hidden exposure
- Foreign funding oversight is under brighter federal scrutiny
- Institutions are expected to show process, documentation, and repeatable controls

02 The 2026 Shift

1. OFAC Enforcement Reached Education

The February 2026 OFAC settlement involving IMG Academy changed the conversation. The case showed that educational institutions are not outside the reach of sanctions enforcement merely because they are schools. Schools with international touchpoints must stop assuming that sanctions risk belongs somewhere else.

2. Federal Visibility Into Foreign Funding Is Increasing

On February 11, 2026, the U.S. Department of Education released 2025 Section 117 foreign funding data showing over \$5.2 billion in reportable foreign gifts and contracts across more than 8,300 transactions. For institutions, this means: know who is paying, know who is sponsoring, know who is connected to the transaction, and be able to show what was reviewed and when.

3. Compliance Is Moving Closer to Operations

The old model was policy on paper. The new model is operational: screening, review, escalation, documentation, and retained evidence built into the workflow. Regulators and auditors do not only ask whether a policy exists. They ask whether the institution can show what it actually did.

03 Where Schools Are Exposed

A lot of education leaders still think only about the student name. That is too narrow. The real exposure often lives in the full relationship and payment chain.

- **Tuition & Fee Payments**

Funds from parents, sponsors, corporate payers, third-party senders, or overseas remitters. Risk can sit with the source of funds, not only the enrolled student.

- **Enrollment Agreements**

Contractual or financial relationships entered before screening has happened.

- **Donations & Sponsorships**

International donors, family foundations, or intermediaries with limited screening.

- **Visiting Scholars & Vendors**

International visitors, research partners, and vendors creating sanctions or export-control implications.

- **Refunds & Disbursements**

Returning money is not automatically risk-free. Refunds can create additional exposure if counterparties are restricted.

A common — and costly — misconception: "We use Blackbaud / Flywire, so we're covered."

In our conversations with school CFOs, business officers, and general counsel, two vendor names come up repeatedly as the assumed compliance answer: Blackbaud and Flywire. Both are widely deployed in education, both handle money or constituent data, and both are strong at what they do. Neither is positioned by its own vendor as a sanctions-screening or OFAC-adjudication tool for the institution. The category mismatch is what creates exposure.

Blackbaud

Primarily a fundraising, constituent-relationship-management, financial accounting, and tuition-payment platform. Products such as Raiser's Edge, Financial Edge, and Blackbaud Tuition Management are built to manage donor relationships, fund accounting, and payment collection. Blackbaud's own product documentation does not position the platform as a sanctions-screening, beneficial-ownership-analysis, or OFAC-adjudication tool. Using Blackbaud well still leaves the institution responsible for screening the parties it transacts with.

Flywire

A cross-border payment processor specializing in international tuition payments. Flywire performs KYC/AML on payors as part of its own regulatory obligations as a licensed money-services business. That program runs on Flywire's books, satisfying Flywire's regulator. It is not the school's screening program, and a cleared Flywire payment is not the school's documented OFAC review of the payor relationship for the school's own compliance file.

Why this matters: OFAC and Section 117 disclosure obligations attach to the institution. A vendor running its own compliance program for its own business does not transfer the school's screening, adjudication, and evidence-retention obligation. A processor's "the payment cleared" log is a different artifact than the school's screening decision, reviewer identity, decision rationale, and timestamped audit trail of why a payor, sponsor, or donor was approved.

This is consistently where we see the most preventable exposure in education compliance reviews. Treat Blackbaud and Flywire as the excellent payment and CRM tools they are — and run institutional sanctions screening alongside them, not instead of them.

04 The 5 Compliance Failures That Keep Showing Up

1. Screening Only the Student

The institution screens the applicant, but not the parent, sponsor, donor, beneficial payer, or wire originator.

2. Screening Only Once

A one-time check at admission is not enough. Lists change. People change. Relationships change.

3. No Documented Adjudication

Potential matches handled informally through email or hallway discussion. Weak evidence and inconsistent decisions.

4. No Retained Audit Package

Even when staff make the right call, many schools cannot later prove what was screened, who reviewed it, and why.

5. Disconnected Ownership

Admissions, finance, advancement, and compliance operate in separate lanes. Risk moves between lanes faster than accountability.

05 Audit-Ready Program Framework

Institutions do not need a giant bureaucracy. They need a practical operating model built on five pillars.

Pillar 1: Define Who Gets Screened

- Students and applicants
- Parents and guardians
- Tuition payors
- Scholarship sponsors
- Donors and foundations
- Visiting faculty, vendors

Pillar 2: Define When Screening Happens

- Pre-enrollment review
- Admission or enrollment
- Tuition payment setup
- International fund receipt
- Refund processing
- Periodic re-screening

Pillar 3: Human-Reviewed Adjudication

- System screens against lists
- Hits routed to review queue
- Staff review context
- Decision and rationale logged
- Evidence preserved

Pillar 4: Preserve Evidence

- Screening date/time
- Lists screened
- Match details
- Reviewer identity
- Decision rationale

- Exportable evidence

Pillar 5: Assign Ownership

- CFO or business officer
- Controller or student accounts lead
- General counsel
- Admissions operations leader

06 90-Day Action Plan

Days 1-15: Foundation

- Assign program ownership
- Map tuition and sponsorship chain
- Identify departments touching international funds
- Define who must be screened

Days 16-30: Policy & Process

- Write a short screening policy
- Define review triggers and escalation paths
- Standardize decision states
- Start screening high-risk relationships

Days 31-60: Scale

- Batch screening for existing rosters
- Build repeat screening cadence
- Train admissions, finance, advancement
- Establish retained evidence procedures

Days 61-90: Operationalize

- Test workflow with sample cases
- Review response times and documentation
- Report to senior leadership or board
- Move from ad hoc to stable process

07 Questions Trustees Should Be Asking

- > **Do we know every party connected to incoming tuition and donation flows?**
- > **Are we screening only students, or the full payment chain?**
- > **Can we prove what we reviewed six months from now?**
- > **Who owns sanctions and counterparty screening at our institution?**
- > **If regulators ask for documentation, how fast can we produce it?**

> **Are our current processes policy-deep but workflow-thin?**

08 How SecurePoint Education Fits

SecurePoint Education is built around the idea that educational screening needs to be operational, documented, and easy to defend.

- Screening for students, tuition payors, sponsors, faculty, and institutional vendors
- Batch roster imports and continuous monitoring workflows
- Structured review and adjudication for potential matches
- Immutable audit logs tied to case and organization identifiers
- Evidence packs and exports with timestamps and integrity-friendly records
- One shared screening and audit architecture across products

The key question is not "does it screen?" The key question is: can our institution run a real workflow and prove what happened later?

Final Takeaway

The institutions that respond well will not be the ones with the most complicated policy manuals. They will be the ones with a simple, enforced workflow: screen the right parties, review potential hits with human judgment, document every decision, keep evidence ready.

SRC Sources & Notes

The references below are the primary sources used in this paper. They are listed for traceability and verification — they are not endorsements, and SecurePoint USA does not represent any source as exhaustive. Confirm current text and guidance with the source itself before relying on any citation.

[1] OFAC Recent Actions — IMG Academy LLC settlement (Feb 2026)

<https://ofac.treasury.gov/recent-actions>

Settlement reference. Verify the linked enforcement notice for current penalty amount and program citation.

[2] U.S. Department of Education — Section 117 Foreign Gift and Contract Reporting

<https://sites.ed.gov/foreigngifts/>

Source for aggregate Section 117 disclosure totals. Numbers cited reflect the most recent published dataset; reconfirm with the live disclosure portal.

[3] 20 U.S.C. § 1011f — Disclosures of foreign gifts

<https://www.law.cornell.edu/uscode/text/20/1011f>

Statutory basis for Section 117 reporting referenced in the paper.

[4] 31 CFR Parts 500–599 — OFAC sanctions regulations

<https://www.ecfr.gov/current/title-31/subtitle-B/chapter-V>

Primary regulatory framework for the OFAC obligations described.

[5] Blackbaud product overview (Raiser's Edge NXT, Financial Edge NXT, Blackbaud Tuition Management)

<https://www.blackbaud.com/products>

Referenced to establish vendor product positioning. Blackbaud positions itself as a fundraising, CRM, financial accounting, and tuition-payment platform; it does not position itself as an institutional sanctions-screening or OFAC-adjudication tool. The "common misconception" callout reflects this product positioning, not a critique of Blackbaud.

[6] Flywire — Education payments product page and Compliance & Risk Management overview

<https://www.flywire.com/industries/education>

Referenced to establish vendor product positioning. Flywire positions itself as a cross-border payment processor that performs KYC/AML on payors as part of its own regulatory obligations as a licensed money-services business; it does not position itself as the school's institutional sanctions-screening program. The "common misconception" callout reflects this product positioning, not a critique of Flywire.

Originally published: 2026-03-12 Last reviewed: 2026-05-10

From Ad Hoc to Audit-Ready

See how SecurePoint Education provides screening, adjudication, and evidence in one workflow — built for the way schools actually operate. Whether the program is a lift-and-shift of existing manual checks or a greenfield build, scoping is environment-specific.

Request an Education Demo

securepointusa.com/request-demo

SecurePoint USA | securepointusa.com

(c) 2026 SecurePoint USA. All rights reserved. Last reviewed: 2026-05-10

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, a C3PAO, your Facility Security Officer (FSO), an export-control or empowered official, sanctions counsel, or other advisor familiar with your specific 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 current product behavior, not a contractual commitment. Capability fit for any specific environment must be confirmed during scoping.