

DEALING WITH AND PREVENTING STUDENT FRAUD

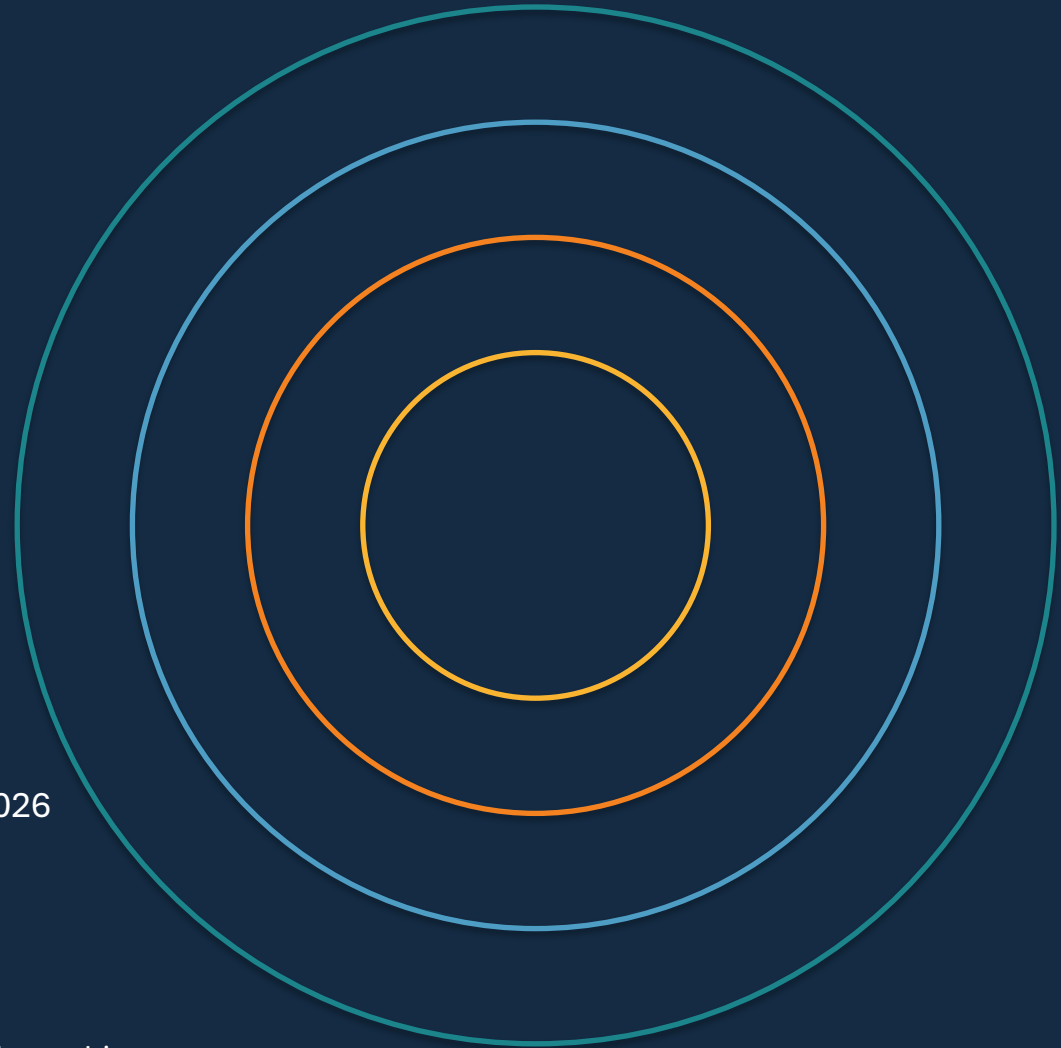
From first application to final collection

Cruisin' to Collections Student Financial Services Conference • 2026

Laurie Beets • Bursar / Director of Student Loans & Debt Management
Oklahoma State University

Tim Lehmann, Vice President Student Financial Services, Southern New Hampshire
University

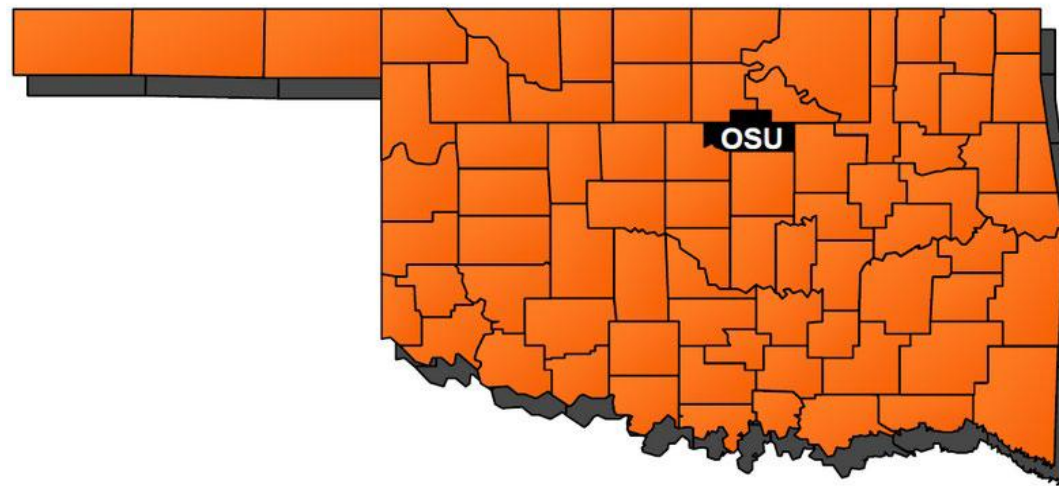
AWARENESS • CONNECTION • EARLY ACTION



About Oklahoma State University



- **Founded on Christmas Day in 1890**
- **Land-Grant Institution**
- Under the **governance** of the **Oklahoma A&M Board of Regents**
- **Five Campuses** – Stillwater (main), Oklahoma City, Tulsa, Center for Health Sciences (Tulsa), Institute of Technology (Okmulgee)
- **Location:** Stillwater, Oklahoma – 60 miles from Oklahoma City and Tulsa
- **Size:** 30,683 students
- **Famous Alumni:** Barry Sanders, T. Boone Pickens, Garth Brooks





Southern New Hampshire University

A private, nonprofit university serving more than 200,000 learners worldwide Founded 1932 · Private, nonprofit · Accredited by NECHE · 400,000+ alumni worldwide

285,000

Total learners

Enrolled across roughly 200 programs, certificate through doctorate

280,900

Online

98% of enrollment — learners worldwide, most of them working adults

4,100

On campus

300-acre residential campus in Manchester, New Hampshire

Who we serve

SNHU's population is overwhelmingly online and adult. Campus students account for roughly 2% of enrollment; the other 98% study at a distance, and the university's stated mission centers on working adults returning to higher education. Geographically distributed, nontraditional, and enrolling year-round.

Session Overview

Behind every enrollment number is a story but not all of them are real.

Schools are experiencing an influx of scammers, fraudulent applicants, and ghost students. Explore trends, real cases, and practical defenses.

AWARENESS • CONNECTION • EARLY ACTION

Behind every enrollment number is a story...

But not all of them are real.

The question is no longer simply:

“Did this student enroll?”

It is:

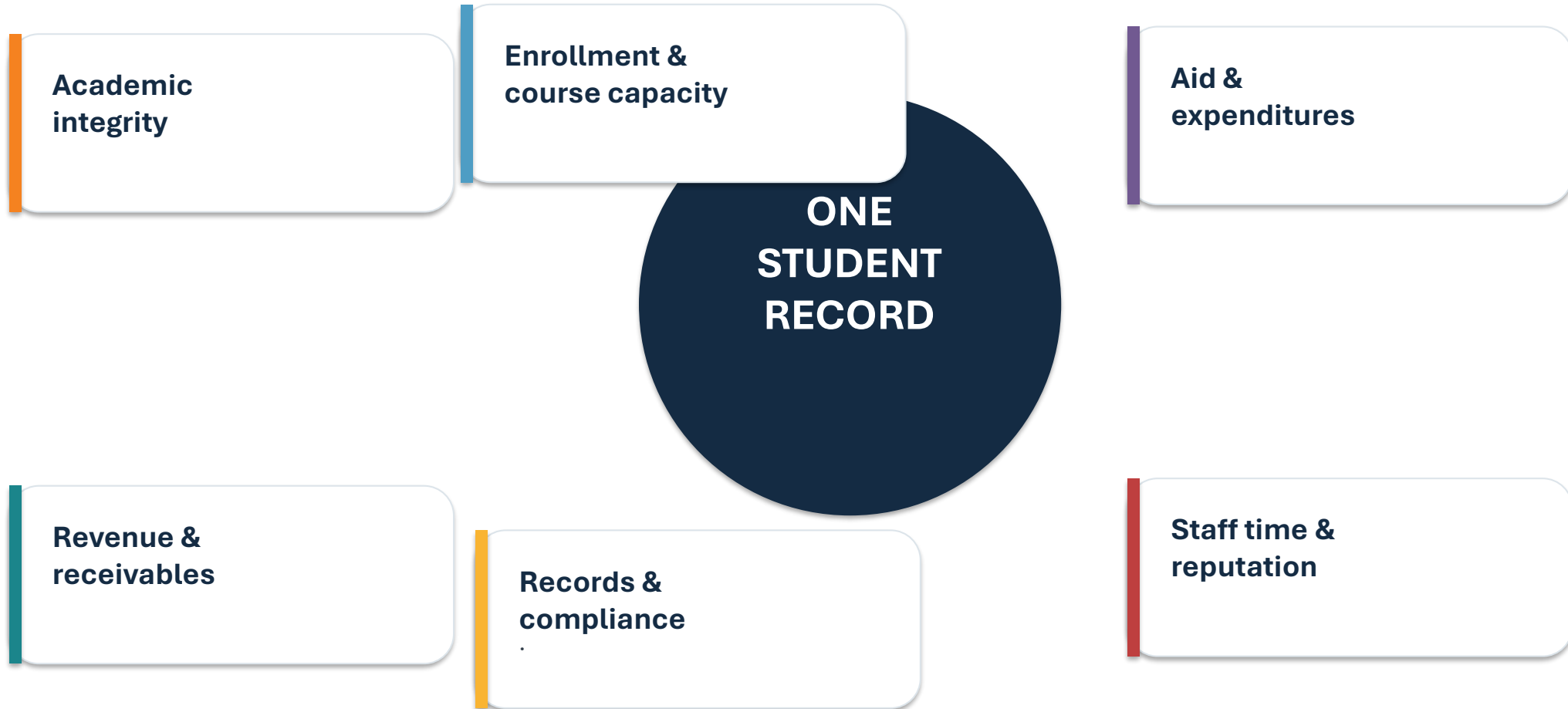
“What story is the activity across the University telling us?”



Why this matters

WHY

Student fraud creates risk long before a balance reaches collections. ***One activity can create downstream work in multiple offices.***



This is not simply a Bursar or Financial Aid issue.

The fraud landscape is broader than one scheme

Synthetic fraud, identity theft, and first-party fraud can contaminate the receivables pipeline.

S

Synthetic fraud

Name/DOB/SSN combination does not correspond to a single real person.

- First-party synthetic: applicant uses an SSN that does not belong to them or masks financial history.
- Third-party synthetic: identity elements are fabricated.

I

Identity theft

Real identity information is used by someone else.

- Name, DOB and SSN may all be real.
- Email and phone may connect to the perpetrator rather than the legitimate person.

F

First-party fraud

Applicant uses their own real identity with malicious intent.

Examples identified in the COHEAO material include ACH/check returns, money muling, credit washing, and boosted tradelines.

Key point: different fraud types can enter at different points—and become a collections problem later.

Fraud can move through the full student lifecycle

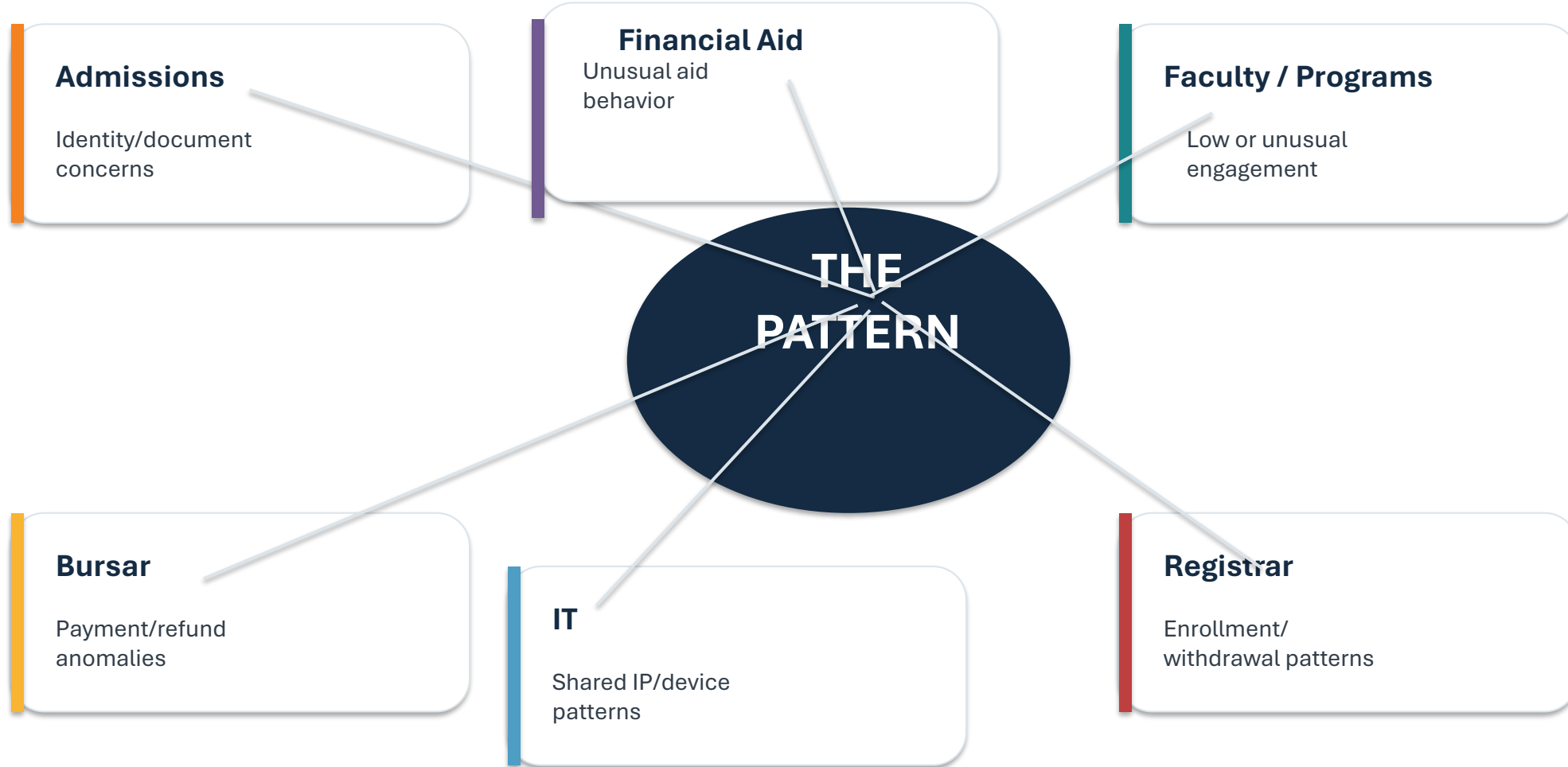
At each stage, there are opportunities for fraud to enter, change, or exploit the process.



Connect the dots across the University

CROSS-FUNCTIONAL

A fraudulent student may interact with multiple systems while each office sees only one piece.



Individually, an activity may not establish fraud. Collectively, the pattern may be significant.

One common pattern: value is extracted from the institution before meaningful academic participation occurs.



But fraud does not always follow this exact path.

Some individuals participate, earn passing grades, remain enrolled for multiple terms, or interact normally with offices.
Passing grades or office contact alone do not establish legitimacy.

Red flags: look for patterns, not proof

A red flag is a reason to pause, document, and connect information—not a finding of fraud.

1

Identity

Document inconsistencies
Unusual identity attributes

2

Contact

Shared addresses
Disposable email/phone

3

Technology

Shared IPs/devices
Unusual login patterns

4

Financial

Shared/unrelated bank accounts
Returned payments

5

Enrollment

Rapid add/drop
Multiple institutions

6

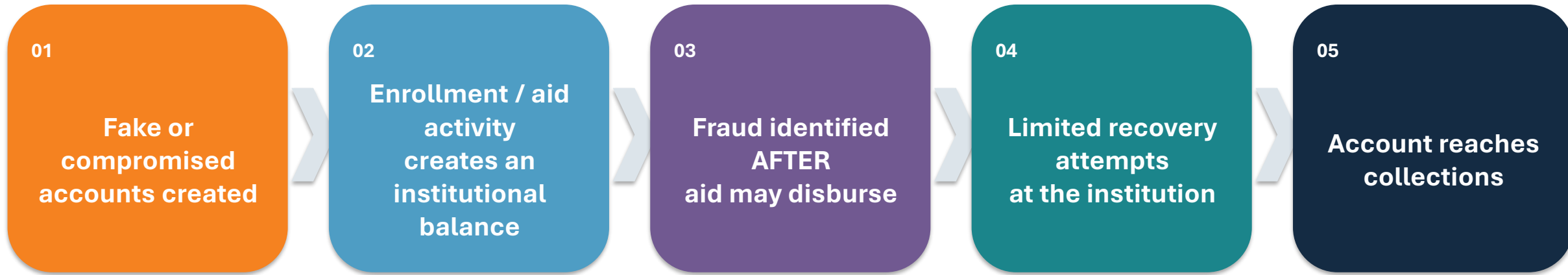
Academic

Minimal participation
Unusual course activity

The strongest signal may be the combination of otherwise ordinary events.

The fraud-to-default pipeline

Weak upstream controls can create downstream recovery problems.



**Collections
consequence**

Fraudulent debt can distort recovery analytics, liquidation performance, forecasting, placement strategy, and agency scorecards.

“Institutions cannot simply ‘place and forget.’”

Four fraud vectors that threaten collections

Ways upstream fraud can contaminate the recovery pipeline.

01

Synthetic identity & identity theft

Fraudulent accounts enter receivables with little or no recoverability and can create disputes and identity-theft claims.

02

Data integrity & contact degradation

Burner phones, fake addresses, disposable emails, VPNs and manipulated data reduce right-party contact and skip-tracing effectiveness.

03

Delayed detection & portfolio pollution

When fraud is identified only after aid, non-attendance or failed engagement, collections may receive an obligation that was never legitimate.

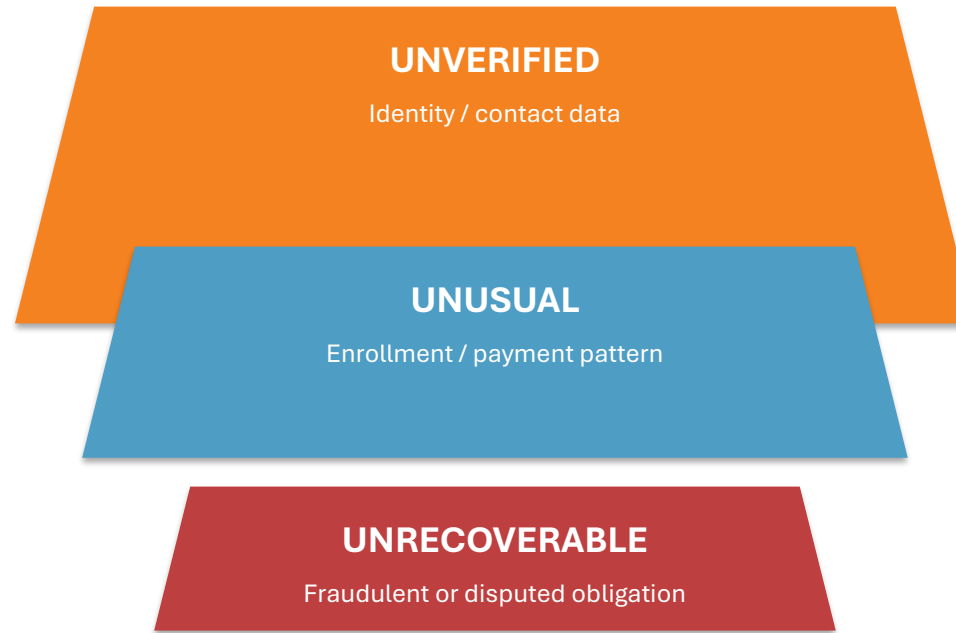
04

Regulatory, compliance & reputational risk

Pursuing fraudulent or identity-theft-related balances can create complaint, litigation, regulatory and trust risks.

What collections may see—after the fact

By the time an account reaches collections, upstream warning signs may have been separated across systems.



The earlier the signal is connected, the more options the University has.

PREVENT → DETECT → RESPOND → RECOVER

The goal is not a single “fraud office.” It is a connected operating model.

PREVENT

Identity verification
Process controls
Clear escalation paths

DETECT

Exception reporting
Cross-system analytics
Human review

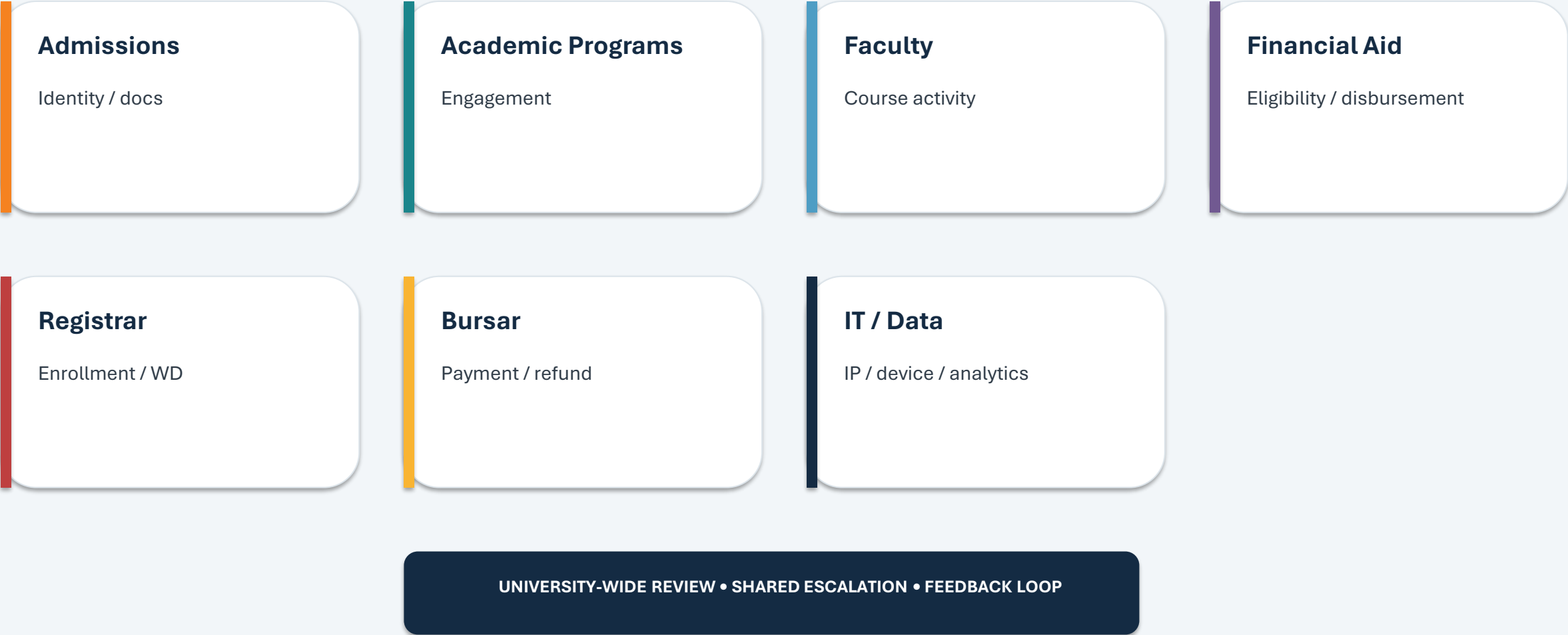
RESPOND

Pause / hold when
appropriate
Share information
appropriately
Document decisions

No single office sees the whole picture. The process has to connect the picture.

Build a University-wide fraud conversation

Awareness is the first control: know what to look for, where to send it, and who needs to connect the dots.



Illustrative scenario: the clues arrive separately

The value of cross-functional review is seeing the sequence—not assuming any one clue proves fraud.

Admissions

Questionable identity/document pattern

Financial Aid

Aid activity inconsistent with other information

Faculty

Little or no meaningful academic engagement

Bursar

Payment returned; refund activity

IT

Common IP/device pattern across multiple accounts

Registrar

Rapid schedule change / withdrawal

Question for the room: Which office sees the first clue? Who connects the dots?

Recognizing potential red flags is a shared responsibility

Prevention and recovery integrity require coordinated stewardship.

01

Shared fraud detection & early warning

Develop fraud indicators and escalation triggers across the student lifecycle.

02

Shared accountability for data integrity

Validate identity, enrollment activity and borrower information before placement; maintain accuracy through servicing.

03

Shared compliance & consumer protection

Align fraud review, dispute handling and escalation processes.

04

Shared investment in analytics & strategy

Use portfolio analysis, recovery trends and fraud patterns to improve decisions.

Fraud management cannot be siloed.
Fraud is no longer isolated to one point in the student experience.

A practical conversation starter for your campus.

- 1 **Fraud can begin before enrollment—and continue after withdrawal.**
- 2 **No single red flag has to tell the whole story.**
- 3 **The strongest signal may be the combination of ordinary events.**
- 4 **Early information-sharing can protect students, programs and resources.**
- 5 **Collections is downstream—but fraud prevention starts upstream.**

Let's connect the dots

The goal is not to create suspicion—it is to create awareness, appropriate escalation and shared responsibility.



What fraud signals are you seeing first—and in which office?



Where does information currently stop?



Which red flags could be shared through an existing process?



What would help your team recognize a cross-system pattern earlier?



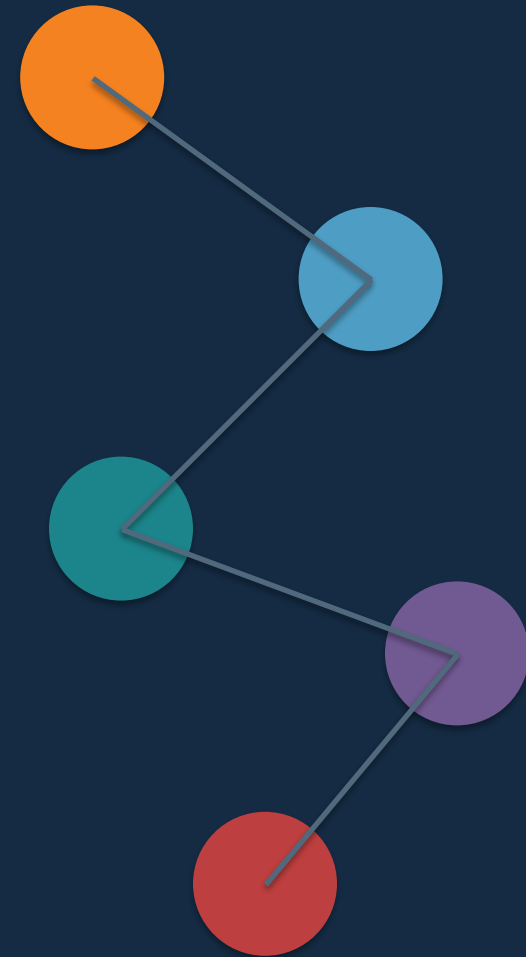
How can collections help feed information upstream?

Awareness → Connection → Early action → Better outcomes

STUDENT FRAUD IS A UNIVERSITY-WIDE ISSUE

The earlier we connect the dots, the more opportunities we have to protect our students, academic programs, and University resources.

**MORE AWARENESS.
BETTER CONNECTION.
EARLIER ACTION.**



QUESTIONS & DISCUSSION

Let's connect the dots

The goal is not to create suspicion—it is to create awareness, appropriate escalation and shared responsibility.



What fraud signals are you seeing first—and in which office?



Where does information currently stop?



Which red flags could be shared through an existing process?



What would help your team recognize a cross-system pattern earlier?



How can collections help feed information upstream?

Awareness → Connection → Early action → Better outcomes

THANK YOU

Questions?