Ghost Student Busters: Mitigating Fraudulent Application Risk

UNIVERSITY RISK MANAGEMENT & INSURANCE ASSOCIATION

Lizz Petroski, Executive Director of Student Financial Services, Excelsior University

Sarah Egerton, Director of Risk Management and Internal Audit, Excelsior University

TODAY'S ROADMAP

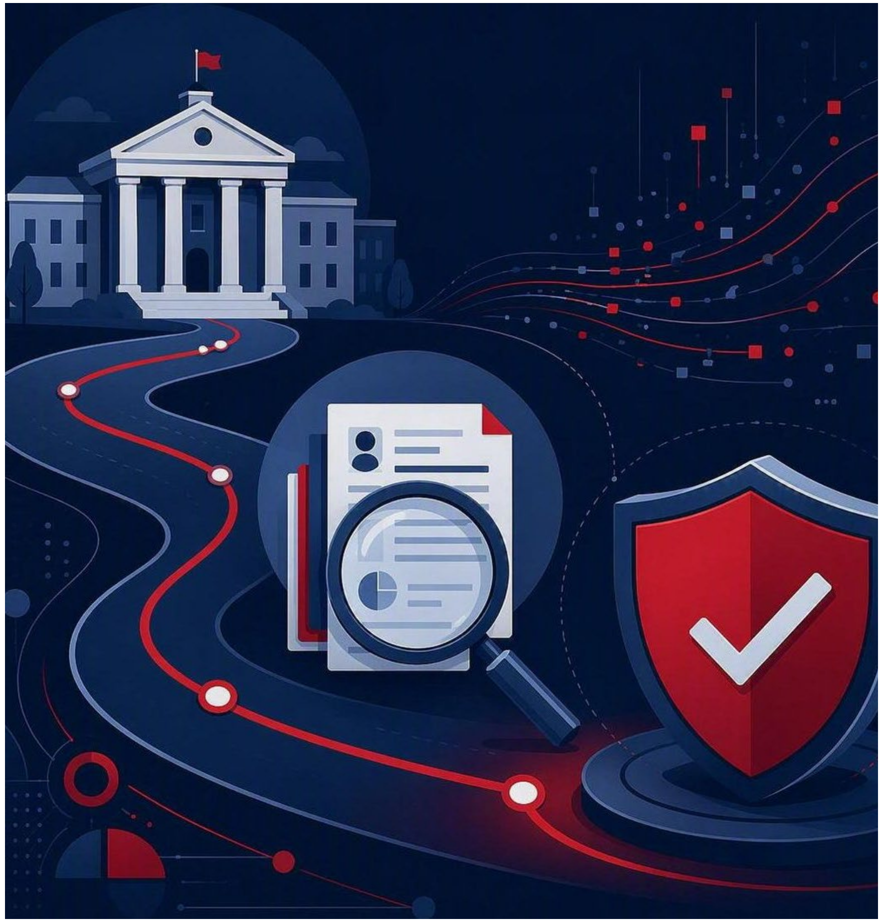
Agenda

01 What are ghost students?

02 The national risk landscape

03 Excelsior University Case Study

04 Results, lessons learned, and Q&A



What Is a Ghost Student?

The scheme in short

- Not a real learner, but a fabricated or stolen identity created to collect federal aid
- The scheme: enroll in online courses, stay active just long enough for aid to disburse, then disappear
- Victims are frequently real people whose stolen identities later surface as federal debt

The National Landscape

Fraud trends across U.S. higher education

THE NATIONAL LANDSCAPE IN FOUR NUMBERS

200+

Open federal investigations nationwide

$350M+

Ghost-student fraud investigated by federal authorities over the past five years

31.4%

Fraudulent applications reported by the nation's largest community college system

15,000+

Staff hours spent fighting enrollment fraud at Utah institutions alone

What changed

- COVID-19 pushed enrollment online, erasing in-person identity checks
- Generative AI mass-produces synthetic identities, essays, and even deepfake verification
- Open-access admissions let applications through with minimal proof

Why it works

- Online courses need less activity to trigger aid disbursement
- Fraud rings deploy thousands of applications at once — often overnight, on weekends and holidays
- Manual, reactive review can't keep pace with automated attacks

Financial Loss

- Direct institutional losses
- Compliance and regulatory penalties
- Bad debt write-offs

Reputational Damage

- Reduced stakeholder trust
- Potential negative media attention

Operational Disruptions

- Wasted enrollment management resources
- Distorted enrollment reporting
- Ghost students occupying course seats

Strategic Impacts

- Misinformed decision-making
- Reduced institutional growth capacity
- Increased cybersecurity vulnerabilities

The Defense Framework: Prevent, Detect, Correct

Preventative

Stop fraud before enrollment

Detective

Identify risk early

Corrective

Recover and monitor

The Federal Response

Safeguards now in place

- Real-time fraud detection is now built into the FAFSA — every applicant screened with risk-based identity checks
- Higher-risk applicants must present government-issued ID before aid is released
- Resumed post-screening and Social Security death-record cross-checks close old gaps
- The “No Aid for Ghost Students Act” would write screening into law

$2B+ in disbursements prevented • 200+ open federal investigations

DESPITE IT ALL

Fraud keeps flourishing

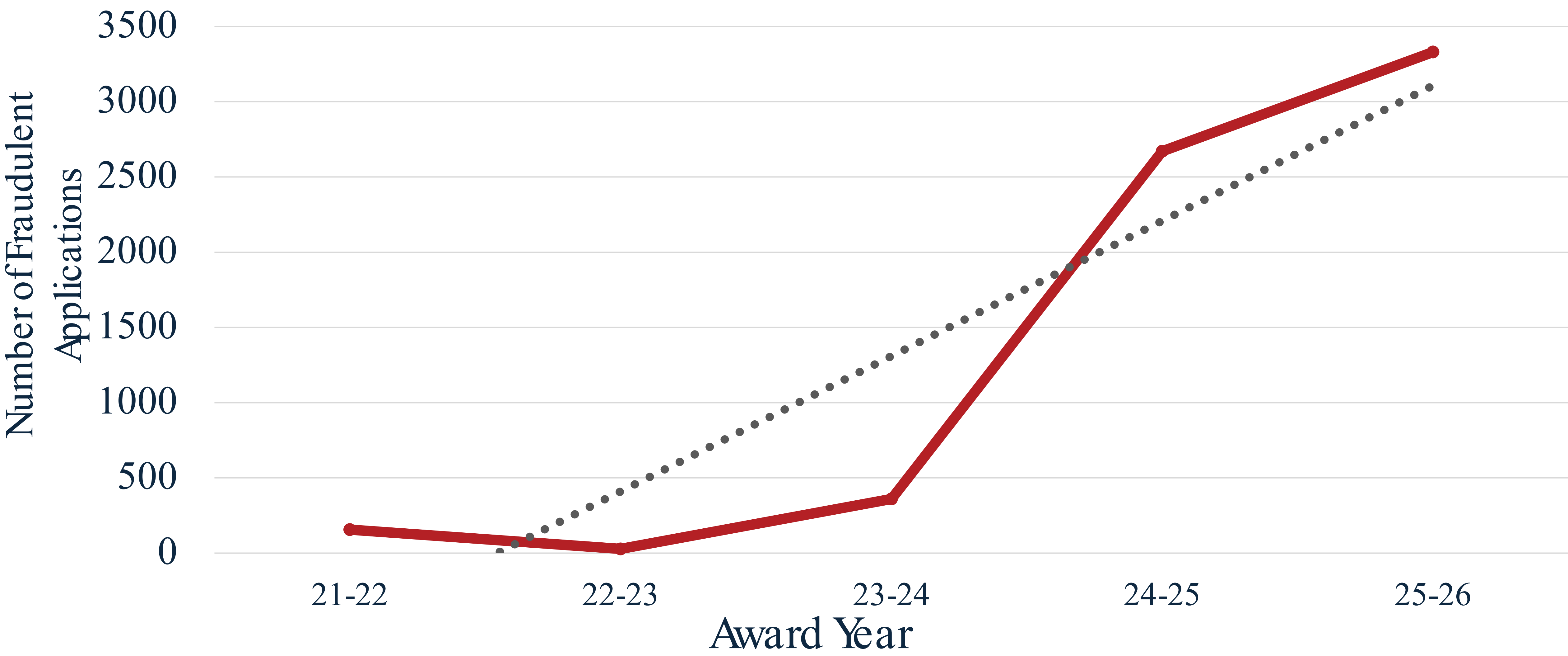
Every safeguard raises the bar — and the schemes keep finding a way over it

Case Study: Excelsior University

We ain't afraid of no ghosts!

THE PROBLEM, QUANTIFIED

Fraud Trend at Excelsior



The Challenge at Excelsior

Why identity is hard to verify

- A primarily adult, online student population means no single document or office can confirm identity
- We learned to see each student as the sum of their parts, layering data across admissions, financial aid, IT, and academics
- Early reviews were manual: validating high-school completion, comparing signatures, and hunting inconsistencies
- Many cases traced back to stolen identities the victims were unlikely to detect
- COVID-19 and AI made the risk faster-moving and impossible to manage by hand

A Layered, Three-Part Approach

1

Multi-Factor Authentication

Catches invalid emails and phone numbers at application, before enrollment

2

Predictive Risk Model

Turns known fraud behaviors into a risk score, easing reliance on manual review

3

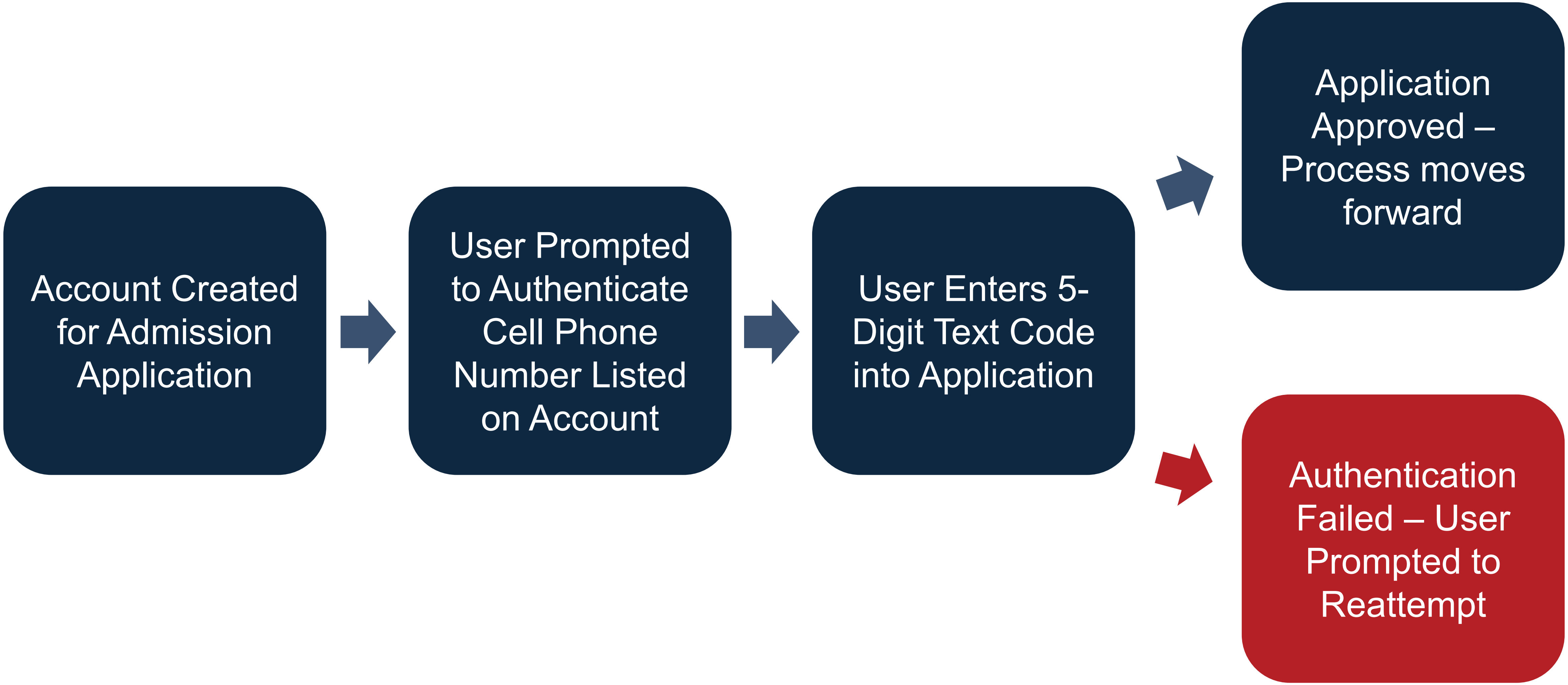
Third-Party Identity Screening

Automates checks across sources like email-creation history and prior identity theft

The strength is in how the layers work together — a wide net early, and deep review only where it is warranted.

LAYER 1 IN ACTION

Multi-Factor Authentication Process



LAYER 2

The Predictive Risk Model

What it does

- Converts the behaviors and characteristics of known fraud into a risk score
- Helps frontline admissions teams flag risk earlier, without manually connecting every data point
- Frees staff to redirect time toward real students who need support

96.57%

model accuracy

Automated Risk-Based Screening

One screen, calibrated by risk

- Every applicant moves through the same risk-based screening, applying consistent standards for all
- Low risk: no disruption to the enrollment experience
- Medium risk: prompted for additional identity confirmation
- High risk: rigorous review, including live photo or video verification when needed
- The shift: from reactive cleanup to proactive, measured prevention

Initial Intervention Results

22.8%
of Admitted Applications were deemed fraudulent in the most recent 170 days WITHOUT interventions.

8.60%
of Admitted Applications were deemed fraudulent in the most recent 170 days WITH interventions.

Dropped to **12.6%** in the 79 days with just MFA

Dropped to just **4.5%** in the 91 days we've had both interventions

Day -170
Truncated Data for Comparison

Day 0
MFA Introduced

Day 79
Predictive Model Launched

Day 170
Available data at time of analyses

Reporting Suspected Financial Aid Fraud

U.S. Dept. of Education — Office of Inspector General (OIG)

- Report suspected aid fraud — ghost students, fraud rings, and stolen identities
- Online (preferred): oig.ed.gov/oig-hotline
- Phone: 1-800-MIS-USED (1-800-647-8733)
- Fax: (202) 245-7047
- Mail: OIG Hotline, U.S. Dept. of Education, 400 Maryland Ave. SW, Washington, DC 20202-1500

On Campus: Who to Contact — and When

- Notify your Financial Aid Director and General Counsel
- Document everything: names, dates, application details, and how the fraud was flagged

WHAT TO REMEMBER

Key Takeaways

Five things to carry forward

- Ghost-student fraud is a national, AI-accelerated threat — no institution is immune
- No single checkpoint solves it; a layered defense is essential
- Shared responsibility across departments beats routing everything to financial aid
- Data reveals what individual offices cannot see alone
- Protect the integrity of aid while preserving access for the students we serve

LET'S DISCUSS

Questions?

THANK YOU

Thanks for attending!

Please reach out with any questions:

Lizz Petroski
Executive Director, Student Financial Services
Excelsior University

Sarah Egerton
Director, Risk Management & Internal Audit
Excelsior University