OACC
OHIO ASSOCIATION OF COMMUNITY COLLEGES

Student-Level Fraud at Ohio Public Community Colleges and Universities

NOVEMBER 2025

Presented To

CHANCELLOR MIKE DUFFEY

Fraud Prevention Work Group Team Members

- **Melissa Amspaugh**, Senior Director Admissions & Enrollment Operations, Lakeland Community College
- **Tony Bourne**, Vice President of Enrollment Management, University of Toledo
- **Tony Box**, Director of Admissions, Marion Technical College
- **Sean Broghammer**, Vice President of Enrollment Management, Kent State University
- **Rob Callahan**, Assistant Vice President & Executive Direction, Enrollment Management, Ohio University
- **Nina Cooke**, Director of Enrollment Management, Cleveland State University
- **Val Fultz**, Director of Financial Aid, Lorain County Community College
- **Kim Everhart**, Director of Financial Aid, Wright State University
- **Dina Galley**, Interim Senior Director, Enrollment Services Operations, Columbus State Community College
- **Scott George**, Registrar, North Central State College
- **Brendan Greaney**, Vice President of Enrollment Management & Student Affairs, Rhodes State College
- **Jennifer Harpham**, Director of Student Financial Aid, University of Akron
- **Dave Hermann**, Vice President of Institutional Advancement, Washington State College
- **Sherri Jiannuzzi**, Director Student Financial Aid Operations, University of Toledo
- **Angela Johnson**, Vice President of Enrollment Management, Cuyahoga Community College
- **Sarah Morrision**, Dean of Enrollment Management, Central Ohio Technical College
- **Stephen Powell**, Chief of Staff, Hocking College
- **Emily Salvage**, Director of Operations, University of Toledo
- **Kevin Wesselman**, Assistant Director of Admissions, Cincinnati State University

Fraud Prevention Work Group Support Members

- **Katelyn Bowling**, Senior Director of Government Relations, Ohio Association of Community Colleges
- **Laura Rittner**, Vice President of Operations & Student Success, Ohio Association of Community Colleges
- **Stephanie M. Sutton**, Higher Education Consultant and Project Manager for Ohio Association of Community Colleges
- **Mike Suver**, Vice President of Operations, Inter-University Council of Ohio

Executive Summary

Ohio's public community colleges and universities are experiencing a dramatic surge in student-level fraud, with fraudulent applications representing one of the most urgent and complex challenges facing higher education in the state. Institutions have reported a marked increase in cases involving falsified admissions documents, synthetic identities, and coordinated fraud rings targeting financial aid systems. The open-access mission of Ohio's community colleges—characterized by open admissions, no application fees, and low-cost tuition—has made these institutions especially susceptible to exploitation by individuals seeking financial gain through fraudulent means.

In response to this growing crisis, the Ohio Association of Community Colleges (OACC) convened a Fraud Prevention Work Group at the request of the Chancellor of the Ohio Department of Higher Education (ODHE). OACC included the Inter-University Council of Ohio (IUC) to ensure that four-year public universities were also represented in the Work Group. This volunteer group conducted a comprehensive review of fraud trends and institutional vulnerabilities, documenting ten representative case studies (seven from community colleges and three from universities). These case studies reveal the sophisticated tactics used by fraudsters, including the use of stolen or fabricated identities, counterfeit transcripts, and manipulation of financial aid and refund processes. Institutions have also encountered organized rings submitting hundreds of fraudulent applications, often leveraging digital tools and third-party facilitators to bypass traditional safeguards.

To address these threats, the Work Group identified and shared a set of best practices, including the establishment of multidisciplinary fraud prevention teams, investment in advanced identity verification software, enhanced staff training, and robust collaboration with law enforcement. These strategies are designed to strengthen institutional defenses, protect legitimate students, and uphold the integrity of academic operations statewide.

This report concludes with targeted recommendations to the Chancellor of the ODHE, emphasizing the need for dedicated funding for fraud prevention and identity verification software, the creation of a centralized state-driven database for fraudulent applications, the formation of a cross-sectional statewide fraud prevention work group, and formalized collaboration with law enforcement agencies. By implementing these recommendations, Ohio's higher education community can more effectively combat the rising tide of fraudulent applications and safeguard the future of academic integrity across the state.

Table of Contents

Introduction

Student-level fraud at community colleges and universities across the United States, including in Ohio, is an escalating and multifaceted risk that threatens institutional finances, regulatory compliance, academic integrity, and campus trust. Digital access, economic pressures, and the rise of third-party facilitators have widened the range and sophistication of schemes fraudsters use to obtain financial benefits, academic advantage, or other services to which they are not legitimately entitled.

Community colleges are especially vulnerable because of their mission to make education accessible to all students — through practices such as open admissions, no application fees, and low-cost tuition that maximizes the amount of Pell grant and loan refunds a student can receive. According to Mark Kantrowitz, a nationally recognized expert on student financial aid, this makes them an attractive target (Swaak, 2024). In a survey administered to Ohio community colleges and universities in September 2025, all 27 respondents (18 community colleges and 9 universities) reported that they had experienced student-level fraud (see appendix A for survey summary and participating colleges).

At the request of ODHE Chancellor Mike Duffey of the Ohio Association of Community Colleges (OACC) convened a Fraud Prevention Work Group to produce a report to help mitigate student-level fraud. This cross-college group of leaders attended meetings, examined student-driven fraud trends, identified institutional vulnerabilities, and provided case studies, best practices and recommendations tailored to Ohio's state institutions of higher education.

Definition of Student-level Fraud

For the purposes of this report, student-level fraud refers to any instance in which individuals exploit institutional processes or resources for personal or financial gain. This encompasses both applicant-level fraud—which occurs during the admissions or onboarding phase through falsified documents, stolen identities, or fraudulent attempts to obtain aid—and fraud committed after enrollment, such as misuse of financial aid, unauthorized access to institutional systems, or falsification of academic records. In this context, an applicant is anyone who has submitted an admissions application but has not yet completed registration or identity verification, while a student is someone who has been officially admitted, registered, and granted access to institutional systems or services.

Fraud schemes take many forms. Common student-level fraud types include manipulation of financial aid and Free Application for Federal Student Aid (FASFA) submissions (false income or household data, forged tax transcripts, and fabricated or synthetic identities); identity theft and account takeover; false withdrawal or refund claims and collusion with staff to expedite payouts; misuse or resale of campus services and accounts (meal plans, bookstore credit, printing); academic-record manipulation and unauthorized grade changes; cheating rings and diploma/credential fraud; and cyber-enabled social engineering (phishing, SIM-swapping) to intercept MFA or reroute payments. Additional vectors include forgery of documents, exploitation of vendor or preparer services, and organized resale schemes that monetize institutional services.

These schemes often take advantage of everyday gaps that can exist in any campus environment — for example, identity checks that could be more rigorous, refund and withdrawal processes that use paper or involve multiple offices, limited information-sharing between units, early-stage analytics, vendor oversight that could be strengthened, and how student conduct cases are handled. Left unchecked, student-level fraud can lead to lost funds, repayments to state or federal programs, investigation and cleanup costs, reputational harm, and staff time diverted from supporting students. This report — developed alongside a statewide fraud-prevention effort — outlines common student-level frauds, how they occur, and straightforward steps campuses and state partners can take together to detect, reduce, and respond to them.

These schemes are enabled by weak identity-verification and account controls, paper-based or loosely governed refund and withdrawal processes, insufficient cross-office data sharing, limited behavioral analytics, lax vendor oversight, and gaps in student-conduct enforcement. If not detected and mitigated promptly, student-level fraud can produce direct financial losses, trigger federal or state claw backs, incur investigation and remediation costs, damage reputation, and divert staff time from essential educational functions. This report — informed by the OACC Fraud Prevention Work Group and prepared for consideration by the Chancellor and institutional leaders — focuses on identifying those fraud types, the mechanisms and enablers behind them, and practical steps colleges and universities can take to prevent, detect, and respond.

Types of Student-Level Fraud Encountered by Ohio Public Community Colleges and Universities

Fraud within higher education has evolved into a complex and organized threat, affecting admissions, enrollment, and financial aid systems across many institutions. Colleges and universities — particularly those with open-enrollment policies or fully online programs — continue to report widespread attempts to exploit weaknesses in identity verification, data monitoring, and refund disbursement processes. The following sections outline the main categories of student-level fraud and the ways they commonly appear.

Identity Theft and Synthetic Identities

A significant portion of student-level fraud involves the use of stolen or fabricated identities. Fraudulent actors employ genuine personal data from victims or create "synthetic" profiles by combining real and false information. These fabricated students often complete the FAFSA using stolen Social Security numbers or falsified tax documents to obtain Pell Grants and student loans. According to statewide survey findings, every participating institution reported encountering identity-based fraud. Some institutions noted clusters of applications sharing the same addresses, phone numbers, or internet protocol (IP) locations. In several cases, legitimate individuals later contacted institutions after discovering that student loans had been taken out in their names.

Fraudulent Admissions Applications and Documents

Institutions increasingly receive falsified or artificially generated admissions applications. Fraudsters often submit counterfeit transcripts, diplomas, or identification cards, and some use

third-party services to produce credible-looking academic records. These documents may contain fabricated residency details or minor name variations designed to evade detection. These fraudulent records may also include false SAT or ACT scores. The goal is typically to secure admission and gain access to financial aid with minimal oversight.

Financial Aid and Refund Scams

Financial aid and refund schemes are among the most frequently reported forms of institutional fraud. Individuals enroll in low-cost, online courses, complete minimal coursework, and withdraw after aid funds are disbursed. This tactic allows them to collect refunds without fulfilling academic requirements. Some cases involve manipulation of FAFSA data or rerouting of financial aid to alternate bank accounts. In one specific instance, perpetrators used stolen credit cards to pay tuition, dropped most courses, and waited for refund checks to be mailed. The institution later implemented procedures requiring refunds to be returned to the original payment source to reduce exposure. Fraudulent applicants are also completing the courses with passing grades to allow continued issuing of overage refunds without being caught by Satisfactory Academic Performance through Financial Aid.

Abuse of Institutional Email and Phishing Activity

Another form of fraud involves misuse of institutional email systems. Individuals apply for admission primarily to obtain a ".edu" email address, which can be used to access discounts or conduct phishing attacks against students and staff. This behavior can be a precursor to more complex financial aid scams. Automated application systems and open-enrollment environments have made such exploitation easier to carry out. One example of these attacks was students at a college being sent a phishing email about getting a job on campus at $25.00 an hour. All the students had to provide was their contact information and their Social Security number and date of Birth.

Credit Card Payment and Refund Fraud

Several institutions have reported incidents involving the use of stolen credit cards to pay tuition or fees. After completing payment, the fraudsters drop their courses except a single class to stay enrolled to trigger refunds, which they attempt to divert to alternative payment methods. Many institutions have since adopted policies requiring all refunds to be returned to the original payment method, thereby closing a common loophole.

Coordinated Fraud Rings and Organized Schemes

Institutions have identified organized groups submitting identical or related applications across multiple campuses. These fraud rings reuse personal information, essays, and contact details to exploit weaknesses in identity verification and data-sharing systems. When detected, such cases are often escalated to the U.S. Department of Education's Office of Inspector General or law enforcement agencies for further investigation.

Enrollment-Stage Fraud

Certain fraud schemes persist beyond admission, involving individuals who maintain active enrollment through minimal coursework or by hiring others to complete assignments. These efforts allow the scheme to continue long enough for repeated financial aid disbursements. Faculty have played a growing role in identifying these cases by recognizing similar

communication patterns, assignment styles, and email naming conventions among fraudulent accounts.

Transcript and Record Requests

Another growing concern involves fraudulent transcript or credential requests. Offenders often target records of former students, especially older files with limited verification protocols. These attempts undermine institutional record integrity and may enable individuals to fabricate academic histories for employment or further education purposes.

Institutional Responsibility for Reporting Fraud

Institutions of higher education have a legal responsibility in reporting student-level fraud, as outlined by federal guidance. Administrators must adhere to the Federal Student Aid (FSA) Handbook, which includes holding disbursements and conducting institution-level fraud queries when necessary. When fraud is suspected, it is essential to report these cases to the U.S. Department of Education's Office of Inspector General (ED-OIG) and to cooperate fully with auditors and law enforcement agencies. This proactive approach helps safeguard the integrity of student aid programs and ensures compliance with federal regulations.

Institutions are also encouraged to engage campus-wide stakeholders—including the registrar, IT, business office, and academic leaders—to strengthen internal processes. Improving identity verification, monitoring for red flags, documenting findings, and updating policies and training are all vital steps in preventing and addressing fraud. By fostering collaboration and maintaining robust procedures, colleges and universities can better detect and report fraudulent activities, ultimately protecting both their students and institutional resources.

Ohio Public Community College and University Case Studies

The following section presents ten case studies of student-level fraud, compiled and written by volunteers from the Fraud Prevention Work Group. These case studies were developed to illustrate the diverse and evolving nature of fraud affecting Ohio's public higher education institutions. Of the ten cases, seven originate from Ohio community colleges and three from universities, offering a comprehensive look at the challenges faced across different institutional settings. Each case highlights specific fraud schemes, detection methods, institutional responses, and key lessons learned, providing valuable insights for strengthening fraud prevention efforts statewide. These case studies collectively demonstrate the evolving and sophisticated nature of student-level fraud in Ohio's higher education system. Institutions have responded with a combination of policy changes, technology investments, staff training, and cross-departmental collaboration. See Appendix B for the complete Case Studies.

1. Application Fraud by Multiple Organized Rings

A large spike in fraudulent applications was detected, with over 700 records submitted using stolen personal information. These "ghost students" registered for courses to access

financial aid, sometimes completing coursework to remain eligible for future disbursements. Detection involved identifying patterns in transcripts, addresses, and student IDs. The institution responded by deregistering affected students, blocking aid, and launching a cross-departmental investigation. Key lessons included the need for automated validation technology, ongoing staff training, and a dedicated fraud prevention committee.

2. Student-level Credit Card Fraud
A coordinated scheme involved 65 fake student accounts using stolen credit cards to pay tuition, then withdrawing to trigger refunds. Institutional safeguards required refunds to be returned to the original payment method, preventing financial loss. A similar attempt using stolen checking account information was also thwarted by holding refunds for 21 days. Lessons learned emphasized strict refund policies, data monitoring, cross-departmental collaboration, and staff training.

3. Suspicious Admission Activity: Over 300 Fraudulent Applications
Admissions staff identified multiple applications sharing phone numbers and suspicious IP addresses. Fraudulent applicants focused on obtaining financial aid and used fabricated transcripts. Four students were dismissed after being found in violation of conduct policies. The institution formed a Suspected Fraud team to improve identification and response, including technical and manual review processes and monthly meetings to address evolving threats.

4. Application Fraud for Financial Aid Refunds
Fraudulent applicants enrolled in courses and received financial aid refunds by either attending briefly or completing minimal coursework. Detection involved freezing financial aid and requesting identity verification, which was not provided. The real victims of identity theft contacted the institution for resolution. The college now uses both automated and manual review processes and involves all departments in fraud prevention.

5. Stolen Credit Card Refunds
Fraudsters registered for classes, paid with stolen credit cards, and dropped most courses to create refunds. The institution froze accounts upon notification from the bank and reviewed payment methods for similar activity. Lessons included monitoring for multiple accounts paid by a single credit card and ensuring refunds are returned to the original payment method.

6. New Student Application, Identity, and Financial Aid Fraud
Suspicious activities included altered SAT scores, repeated use of mailing addresses, and applications from disposable email domains. Less than a dozen fraudulent applicants received aid and refunds before being identified and removed. Detection relied on manual review and research methods such as reverse phone lookups and collaboration with campus departments. Steps taken included requiring in-person identity verification and training staff to identify fraudulent transcripts.

7. Returning Student Phishing Fraud
Fraudulent returning student applications allowed access to student portals, enabling phishing for personal data. Detection involved blocking suspicious email domains and manual review of applications. Consequences included occupying class seats and diverting staff resources. The institution responded by training staff, placing holds on student records, and upgrading fraud detection capabilities.

8. Application Fraud: Returned Mail Leads to Falsified Transcript
An applicant was removed from classes after submitting a fraudulent transcript. AI-based fraud detection flagged the application as medium risk, prompting further scrutiny. Returned acceptance letters triggered investigation, and fraudulent documents were confirmed by the named high school. The institution now cancels high-risk applications, increases scrutiny for medium-risk cases, and requires visual confirmation of new students.

9. Questionable Admissions Documents and Potential Student Identity Fraud
Manual review of transcripts revealed multiple irregularities, including inconsistent GPAs, signatures, and signs of tampering. Patterns included batches of applications from the same area and mismatched contact information. Immediate actions included withholding financial aid, placing identity confirmation holds, and collaborating with external partners to confirm authenticity. The institution continues to improve technology and policies for fraud detection.

10. Identity Fraud Prevention
Unusual behaviors among students prompted a university-wide investigation, revealing additional fraudulent cases. Common indicators included exclusive enrollment in online courses, inconsistent geographic data, and matching IP addresses for banking accounts. Eight fraudulent students received refund checks before detection. The institution strengthened safeguards, flagged high-risk applications, and launched a reporting tool for suspicious activity. A standing task force reviews policies and training needs regularly.

Best Practice Recommendations

The OACC Fraud Prevention Work Group has developed a list of nine best practices to combat the growing threat of student-level fraud. A detailed description of these best practices is available in Appendix C.

1. **Establish a College-Wide Fraud Team:**
   Form a multidisciplinary fraud awareness team including representatives from admissions, bursar/billing, financial aid, information technology, registrar, faculty governance, internal audit, legal counsel, and campus police/public safety. This team should define its mission, set clear objectives, update policies, create training programs, implement data monitoring, create a campus-wide reporting mechanism for fraud, and coordinate regular meetings for continuous improvement.

2. **Involve Campus Police and Law Enforcement:**
   Campus police should actively participate in fraud investigations, verify identities, document incidents, and collaborate with external law enforcement. Formalize these procedures through written protocols and provide specialized training on digital identity verification and privacy compliance.

3. **Invest in Fraud Prevention and Identity Verification Software:**
   Institutions should leverage advanced software solutions for initial applicant data validation and real-time identity verification. Integrating these tools into CRM platforms or using third-party services can automate risk categorization and enhance accuracy and efficiency in fraud detection.

4. **Implement Financial Aid Disbursement Controls:**
   Adopt best practices for financial aid disbursement, such as verifying attendance, monitoring midterm grades, and ensuring refunds are processed securely. Educate students on aid requirements and encourage proactive communication.

5. **Comprehensive Staff Training:**
   Train front-line staff, financial aid teams, IT personnel, administrators, faculty, and students to recognize fraud indicators, verify identities, and report suspicious activity. Use blended learning, microlearning, annual refreshers, and targeted communications to keep all stakeholders informed.

6. **Internal Reporting and Data Sharing Framework:**
   Maintain a centralized, secure system for reporting and tracking suspected fraud. Ensure confidentiality, regular review of reporting mechanisms, and transparent communication of case outcomes.

7. **Transcript Review Process:**
   Inspect transcripts for red flags such as font inconsistencies, misalignment, missing signatures, and suspicious content. Verify the authenticity of institutions and documents before processing.

8. **Fraud Detection at Point of Application:**
   Monitor application volumes, flag duplicate or suspicious data, automate alerts, cross-reference external databases, and train staff to recognize patterns. Investigate undeliverable acceptance letters and escalate concerns as needed.
9. **Identity Verification for Online Students:**

   Require in-person identity verification for applicants flagged as potential fraud risks, with coordinated processes across participating institutions to ensure accessibility and consistency.

These best practices collectively strengthen institutional defenses, foster a culture of vigilance, and help safeguard the integrity of Ohio's higher education system.

Cost of Fraud to our Institutions

Student-level fraud imposes substantial financial, operational, and reputational costs on Ohio's public colleges and universities. While the full extent of monetary losses is hard to definitively determine, recent incidents across the state highlight the broad and serious impact of fraudulent activity:

- **Direct Financial Losses:** Institutions have reported significant sums lost to fraudulent financial aid disbursements and refund scams. In some cases, fraudulent students have successfully received thousands of dollars in refund checks or financial aid before detection. Similar schemes involving credit card and refund fraud have resulted in attempted or actual losses that can be difficult to recover.
- **Resource Diversion:** Investigating and responding to fraud requires extensive staff time and cross-departmental collaboration. Employees from multiple departments may be engaged in reviewing applications, monitoring account activity, flagging suspicious records, and responding to victims of identity theft. This diversion of resources impacts the institution's ability to serve legitimate students and maintain normal operations.
- **Impact on Enrollment and Aid Distribution:** Fraudulent enrollments can occupy class seats, preventing legitimate students from registering. They also distort enrollment data, which can affect institutional planning and external reporting. In some cases, fraudulent students have received federal financial aid and refunds before being identified, resulting in funds that may be unrecoverable.
- **Reputational Harm and Compliance Risks:** When fraud incidents become public, institutions may face reputational damage that undermines trust among students, families, communities, and regulatory agencies. Additionally, colleges may be required to repay state or federal funds disbursed to fraudulent accounts and may incur investigation and remediation costs.
- **Operational Costs:** The need for enhanced fraud detection, identity verification, and staff training leads to increased operational expenses. Investments in software solutions, manual review processes, and ongoing training are necessary to mitigate future risks.

Estimated Financial Impact

While a comprehensive statewide estimate is challenging due to the evolving nature of fraud and ongoing investigations, individual case studies suggest that the cumulative cost to Ohio's public colleges and universities is substantial. The Fraud Prevention Work Group developed a survey for Chief Financial Officers at Ohio's community colleges and universities to complete. While only five responses were received, the estimated cost from those five institutions (three community colleges and two universities) was more than $300,000. However, based on the input from the Fraud Prevention Work Group, staff resources are extremely high in combating fraud and may be underreported.

Broader Consequences

Beyond financial losses, student-level fraud erodes institutional integrity, disrupts educational access for legitimate students, and necessitates ongoing vigilance and adaptation. The collective experience of Ohio institutions underscores the urgent need for coordinated prevention strategies, robust reporting frameworks, and continuous investment in fraud detection and response

Recommendations to the Chancellor of the Department of Higher Education

As indicated throughout this report, Ohio's public higher education institutions face escalating threats from organized, technology-driven, student-level fraud schemes. Fraudulent applications, stolen identities, and credit card scams have created systemic financial and reputational risks across colleges and universities. To address these challenges, the Ohio Fraud Prevention Work Group has the following recommendations:

Recommendation 1: Ensure Adequate Funding for Fraud Prevention and Identity Verification Software

To address the escalating threat of student-level fraud, it is recommended that Ohio's higher education institutions receive dedicated and adequate funding to implement modern fraud prevention and identity verification software. These solutions are essential for safeguarding institutional resources, protecting student data, and maintaining compliance with state and federal regulations.

- Fraud prevention software can automate the initial validation of applicant data, cross-referencing information such as names, addresses, phone numbers, and IP addresses against authoritative sources to detect inconsistencies and flag high-risk applications.
- Identity verification platforms authenticate government-issued IDs in real time, using advanced features like liveness detection and anti-spoofing checks, which are nearly impossible to replicate manually.
- Investing in these technologies will reduce manual workload, enhance accuracy, and improve efficiency across admissions, financial aid, and IT operations.
- While there is no one-size-fits-all solution for institutions, successful adoption of software aimed at fraud prevention requires careful consideration of each institution's unique structure, existing infrastructure, and compatibility with existing systems.

Estimated Costs:

- The cost of fraud prevention and identity verification software varies depending on institutional size, existing infrastructure, and the chosen solution.
- Based on current market research and feedback from Ohio institutions, initial implementation costs typically range from $25,000 to $100,000 per institution for robust platforms, with annual maintenance and licensing fees between $10,000 and $40,000.
- Additional expenses may include integration with existing systems, staff training, and ongoing support.

Recommendation 2: State-Driven Database for Fraudulent Applications

The creation of a centralized database managed by the ODHE or other designated organization will allow institutions to record and share verified cases of fraudulent applications, student identities, and payment methods. This system will:

- Identify repeat offenders from targeting multiple institutions,

- Enable faster detection of shared fraudulent patterns (e.g., repeated IPs, emails, or addresses),
- Strengthen inter-campus reporting and accountability, and
- Align with federal identity verification standards and Department of Education Title IV compliance requirements.

Recommendation 3: Cross-Sectional Statewide Fraud Prevention Work Group

The establishment of a state-driven fraud prevention and monitoring work group will unite representatives from admissions, registrar, IT, financial aid, law enforcement, bursar, finance, and legal affairs across the state higher education system. This group will assist in keeping current with the ever-evolving student-level fraud.

This statewide work group recommendation mirrors the collaborative approach taken by our own Fraud Prevention Work Group, where representatives from Ohio public community colleges and universities and diverse campus offices came together to address student-level fraud. Throughout the process of writing this report, we learned a tremendous amount from each other—sharing experiences, strategies, and insights that strengthened our collective understanding and shaped the recommendations presented here.

Recommendation 4: Collaboration with Law Enforcement

As identity theft and fraud attempts continue to rise across higher education institutions, several colleges and universities in Ohio have observed a troubling trend: many victims are local Ohioans who may have previously attended their institution. In most cases, unless the individual proactively contacts the institution to report the fraud, schools lack the updated contact information, specialized expertise, or resources needed to notify potential victims or investigate further.

To address this gap, we recommend establishing a formal line of communication with local law enforcement agencies to report the names of potential identity theft victims. This partnership would enable institutions to share suspected cases of criminal activity or stolen identities, allowing law enforcement to assist with outreach to affected individuals and investigate broader patterns of suspicious behavior or potential data breaches. By working together, institutions and law enforcement can strengthen fraud response efforts, protect both current and former students from identity-related threats, and uphold public trust in the integrity of higher education.

Conclusion

The collective findings from OACC's Fraud Prevention Work Group demonstrate that fraudulent activity is both widespread and adaptive, exploiting gaps in technology, communication, and policy enforcement for financial gain. Addressing these threats requires a unified, campus-wide approach that includes consistent identity verification, robust data analytics, and close

collaboration with law enforcement and peer institutions. Fraud prevention is no longer the responsibility of a single department; it demands coordinated action across the entire academic community, supported and guided by ODHE. The Department's leadership and resources are essential for establishing statewide frameworks, facilitating collaboration, and ensuring that institutions have access to the tools and funding necessary to combat fraud effectively. By implementing the recommendations outlined in this report—including funding for advanced fraud prevention software, establishing statewide reporting frameworks, and fostering ongoing training and vigilance—Ohio's colleges and universities, with the active support of ODHE, can better safeguard their operations, protect students, and maintain the integrity of higher education in an era of rapidly evolving fraud tactics.

References

EDUCAUSE. (2023, August 15). Colleges battle surge in fake student applications. EDUCAUSE Review. https://www.educause.edu/review/colleges-battle-surge-in-fake-student-applications

Taylor Swaak. (2024, October 1). Colleges See Alarming Rates of Fake Applications. So They're Turning to AI. Chronicle of Higher Education. https://www.chronicle.com/

Appendix A – Survey

Financial Aid Fraud Survey Summary

Survey completed by 27 (18 community colleges and 9 universities) between September 8 and September 24, 2025.

Institutions that submitted the survey:

1. The University of Akron
2. Wright State University
3. University of Cincinnati
4. Miami University
5. Lorain County Community College
6. Cuyahoga Community College
7. Edison State Community College
8. Belmont College
9. The Ohio State University
10. Bowling Green State University
11. Cincinnati State
12. Southern State Community College
13. Youngstown State University
14. Ohio University
15. Columbus State Community College
16. Lakeland Community College
17. Northwest State Community College
18. Owens Community College
19. Rhodes State College
20. Kent State University
21. Washington State College of Ohio
22. Marion Technical College
23. Central Ohio Technical College
24. Terra State Community College
25. North Central State College
26. Clark State
27. Hocking College

Universal Experience of Fraud:

- All participating institutions (100%) reported encountering or identifying cases of application or enrollment fraud.

Types of Application/Enrollment Fraud:

- Identity Theft/Synthetic Identities: Use of stolen or fake identities is prevalent, with increasing synthetic identity cases.
- Fake Applications and Documents: Fake or AI-generated applications, transcripts, diplomas, IDs, and sometimes valid-looking documents from third-party services are common.
- Financial Aid/Refund Scams: Fraudsters often enroll briefly in online courses, submit minimal work, then stop attending to claim refunds or manipulate FAFSA/ISIR data.
- Account Creation/Phishing: Auto-creating accounts to obtain .edu addresses for discounts, phishing campaigns targeting students, and college email abuse occur frequently.
- Fraud Indicators: Multiple applications from the same IP, short completion times, inconsistent residency info, and use of external addresses or non-deliverable contact info are common red flags.
- Enrollment-Stage Fraud: Preference for online courses, specific course selection patterns, and enrollment when fraud is suspected are tendencies observed.
- Detection and Remediation: Manual reviews, ID verification, face-to-face checks, and cross-department collaboration are typical responses.

Financial Aid Fraud:

- Use of stolen identities to submit false FAFSAs, falsified documents, and manipulated income data are reported.
- Many institutions suspect FAFSAs are intercepted or stopped by verification processes, with some aid being diverted or canceled.
- Organized fraud rings submitting coordinated claims and reports from law enforcement are noted.

Credit Card Fraud:

- Incidents involve stolen credit cards used for classes and refunds, with some students dropping classes to trigger refunds to unauthorized accounts.
- Controls include returning refunds to the original card and delaying refunds; some institutions report no incidents.

Fraud Patterns and Prevention Measures:

- Most fraud occurs in online programs, with some cases in in-person settings.
- Common preventive strategies include identity verification before aid disbursement, application screening tools, manual reviews, and cross-departmental collaboration.
- Challenges include limited resources, evolving tactics, and technology gaps.

Policies and Innovation:

- Many institutions have policies allowing enrollment drops or disciplinary actions for fraud, often involving holds, verification, and interdepartmental coordination.
- Innovations include task forces, AI tools, identity verification protocols, and data analytics for ongoing detection.

Supporting Resources & Recommendations:

- Respondents highlight the need for improved upfront verification, enhanced staff training, shared data networks, and statewide cooperation to effectively combat fraud.

Appendix B – Case Studies

Case Study: Application Fraud by Multiple Organized Rings

Dina Galley, Interim Senior Director – Enrollment Services Operations
Columbus State Community College

Background Information

Columbus State has seen a large spike in fraudulent applications being submitted to the college, using personal information of victims of identity theft since late 2024. So far, the college has identified over 700 records submitted by what we believe are multiple organized rings.

Details of Fraudulent Activity

The goal of fraud is to register for courses to get access to financial aid funds. Commonly referred to as "ghost students," they stay engaged in coursework to avoid any consequences from participation reporting, and even earn/complete credit hours, hoping to enroll in subsequent semester and receive financial aid funds again.

Detection and Investigation

Discovery of Fraud

In late May 2025, Enrollment Services staff identified unusual patterns while reviewing a batch of high school transcripts. Several dozen transcripts originated from rural Ohio high schools outside our typical service area, all listing a 2018 graduation year and a uniform 3.2 GPA. Initially, we explored whether these applicants were targeting a specific program. However, further analysis revealed broader inconsistencies, leading to the discovery of over 260 fraudulent documents—many of which had been submitted since February 2025.

These transcripts were linked to applications dating back to November 2024. Unlike earlier attempts that often used fabricated data, this wave of applications appeared more sophisticated, often incorporating real personal information likely obtained through identity theft. The applications included plausible addresses, phone numbers, and educational histories from within Ohio. Once accepted, applicants submitted placement documentation—often fraudulent transcripts—via email. These emails mimicked legitimate document submission portals, but closer inspection revealed telltale signs of fraud, including:

- Minor spelling errors in email addresses
- Overly formal language in email
- Elaborate watermarks and seals on transcripts
- Discrepancies between dates of birth and graduation
- Patterns in naming conventions in student ID numbers

Initial Response

Upon identifying the fraudulent records, we immediately assessed their registration and financial aid status. Nearly 100 were enrolled for Summer 2025, over 100 for Autumn 2025, and more than 70 had completed financial aid processes and were scheduled to receive disbursements. The timely discovery of these documents—just before the start of Summer 2025—allowed us to act

swiftly. We deregistered affected students, blocked aid disbursement, and flagged the records for further review.

Investigation Process

Following the initial response, a cross-departmental team—including Enrollment Services Operations, IT Security, Financial Aid, Cashier's and Student Accounting, Legal Affairs, and Columbus State Police—launched a coordinated investigation. This effort uncovered additional patterns that have since informed our fraud detection protocols. Key indicators include:

- Programs of study were typically AA and AS
- Courses registered were exclusively all online, had little pre-requisites, and were in specific departments (social sciences, humanities, criminal justice, business/marketing)
- Patterns in address, phone number, and school information used (or omitted) during application
- Devices used for multi-factor authentication
- IP addresses and secret questions used for single sign-on log in
- Routing and account numbers used for direct deposit

We also noticed that when one avenue was shut down, they found new avenues to gain placement or re-activate historical records. We've found additional fraudulent activity with virtual placement testing, homeschool transcripts, and historical/inactive record updates. Key takeaways from this specific experience are that we need to be monitoring and training all areas, and that these organized rings have a sophisticated understanding of the innerworkings of institutions and/or they are able to adapt and learn quickly.

These findings have been instrumental in refining our application review process and enhancing our ability to detect and prevent future fraud attempts.

Consequences and Outcomes

Institutional Impact

The fraud incident has placed considerable strain on institutional resources and operations. While the financial loss is still being assessed, its broader impact includes the diversion of staff time—approximately 10 employees across multiple departments remain engaged in reviewing applications, monitoring login activity, flagging suspicious records, maintaining shared documentation, responding to victims of identity theft, and exploring automated solutions to prevent future fraud. Additionally, fraudulent enrollments have kept legitimate students from being able to register in course sections and undermined confidence in the accuracy of enrollment data used for planning and reporting.

Institutional/Preventative/Disciplinary Actions

In response, the college has implemented a series of measures to strengthen fraud detection and prevention:

Application and Identity Review Enhancements

- Daily review of applications using an updated list of red flags, including duplicate addresses and phone numbers.

- Maintenance of a reference file of contact information used in previous applications since January 2025.

IT and Data Monitoring

- Weekly audits of internal data for duplicate or suspicious entries, including IP addresses, devices used for multi-factor authentication, and responses to security questions.

Financial Aid Safeguards

- Pre-disbursement review of banking information, including verification of account holder names with financial institutions.
- Mandatory verification for all first-term students receiving aid, with additional scrutiny for those enrolled exclusively in online courses or requesting to increase loan amounts.

Protocol Development and Staff Training

- Formalized procedures for handling suspicious records, including identity verification requests, system access restrictions, and class deregistration.
- Ongoing training for front-line staff, faculty, and transcript evaluators to recognize and report fraud indicators.
- Developing framework for clearing records of any fraudulently earned grades (newly created records and historical records of genuine students who attended previously).

Legal or Ethical Considerations

The college has identified numerous cases involving Ohio residents whose personal information was used without consent. In many instances, contact information is outdated or unavailable, limiting our ability to notify affected individuals. We recommend establishing a formal channel for reporting suspected identity theft to law enforcement, enabling further investigation and victim outreach.

Support or Counseling Provided

When contacted by victims, Columbus State provides guidance on identity recovery, including access to relevant records and resources available through our IT Security team (Cyber Safety).

Lessons Learned

- Identified Gaps in Policy, Procedure, or Technology
- Reliance on manual review of applications and identity documents is insufficient for detecting organized fraud.
- Prior to this incident, the institution lacked a comprehensive protocol for managing fraudulent records, including registration and grade removal.
- IP address data is a valuable tool for fraud detection but is not consistently accessible across third-party systems. This limitation should be addressed with vendors to explore potential solutions.

Key Insights and Recommendations for Prevention or Improvement

- Invest in technology that enables more robust and automated validation of applicant information and identity.

- Maintain vigilance by monitoring local and national trends in fraud and adapting protocols accordingly.
- Foster ongoing internal dialogue and cross-institutional collaboration to share insights and strengthen defenses.
- Establish and sustain a dedicated fraud prevention committee to oversee policy development, training, and response coordination.

Case Study: Student-level Credit Card Fraud
Cuyahoga Community College

Background Information

- Institution Name: Cuyahoga Community College
- Location: Cleveland, Ohio
- Date of Incident: Spring Term 2024/Fall 2025
- Student(s) Involved (Number and Description) 65 students
- Relevant Policies or Codes of Conduct: Refund Policy and Red Flag Procedures

Introduction

In Spring 2024, Cuyahoga Community College (Tri-C) identified a coordinated fraud scheme involving the creation of multiple fake student accounts. A total of 65 fraudulent students registered for classes using stolen credit card information. After enrollment, the individuals quickly withdrew from all courses to trigger tuition refunds through checks or direct deposits. The fraudulent activity was detected through routine monitoring and internal review processes. Because Tri-C's policy requires all credit card refunds to be returned to the original card used for payment, no funds were ultimately disbursed to the perpetrators. This incident emphasized the effectiveness of existing refund safeguards and highlighted the importance of continuous monitoring, cross-departmental collaboration, and proactive fraud prevention strategies within higher education institutions.

In Fall 2025, Tri-C encountered a similar fraudulent attempt involving approximately 40 fake student accounts. However, this time the perpetrators used stolen checking account information to pay for classes before withdrawing to request refunds. Due to Tri-C's policy of holding refunds from check or e-check payments for 21 days, the fraudulent refunds were successfully prevented. This reinforced the importance of maintaining strong institutional controls and adaptive fraud prevention policies.

Lessons Learned

The incidents from Spring 2024 and Fall 2025 reinforced several important lessons for Cuyahoga Community College. Both cases demonstrated the growing sophistication of fraudulent schemes targeting higher education institutions and the importance of maintaining strong, adaptable internal controls. The College learned that strict refund policies, such as returning funds only to the original credit card or holding check and e-check refunds for 21 days, are essential safeguards that effectively prevent financial loss.

Additionally, enhanced data monitoring and analysis tools proved critical in identifying unusual enrollment and payment patterns early. Collaboration between Financial Services, Enrollment Management, and Information Security played a key role in quickly detecting and addressing fraudulent activity. The College also recognized the need for continued staff training and cross-departmental communication to ensure that all employees remain aware of potential fraud indicators and institutional protocols. Collectively, these lessons have strengthened Tri-C's overall fraud prevention framework, reinforcing its commitment to safeguarding institutional resources and student data integrity.

Best Practices

Based on these incidents, Tri-C has identified several key practices to prevent fraud:

- Strict Refund Policies: Refunds should go only to the original payment method, with holds on checks/e-checks.
- Data Monitoring: Regularly review enrollment and payment activity to detect unusual patterns.
- Cross Department Collaboration: Ensure Financial Services, Enrollment Management, and Information Security communicate effectively.
- Staff Training: Educate employees to recognize and report suspicious activity.
- Identity Verification: Apply strong verification procedures for new student accounts.

Case Study: Suspicious Admission Activity: Over 300 Fraudulent Applications

Kristen Kolenz, Director of Admissions Operations and Processing
Kent State University

Background Information

In February 2025, admissions staff at the Geauga Campus of Kent State University noticed multiple phone calls for purportedly different applicants coming from the same phone number. Staff escalated their concerns, and subsequent investigation uncovered nearly a dozen applications that were sharing phone numbers or had similar email addresses. Each application had suspicious IP address location activity, suggesting that each applicant logged into their admissions portal from points across the country and sometimes the globe. Four of the applications registered for classes with varying outcomes and received federal financial aid. All four were remanded to the Office of Student Conduct for violation of the policy on the Admission of Undergraduate Students and the Student Handbook policy on misrepresentation. The students did not complete their hearings. All were dismissed from the university.
Armed with the knowledge of increased fraudulent activity, Kent State mobilized a team of individuals form across the university to build strategies to improve the identification of potential fraud.

Markers of Fraudulent Activity Observed on Kent State Applications

- Heavy use of first-year freshman applications to online programs that do not require an application fee. Applicants have also applied as graduate students, post-undergraduates, non-degree guests, and reenrolling (former) students.
- Applicants shared phone numbers without a shared physical address.

- Phone calls from applicants to university offices were primarily focused on obtaining financial aid. During the calls, staff observed that the sound of the caller's voice did not match the demographic information on their application (e.g., age, national origin).
- Similar email addresses were used between otherwise unrelated applicants. Some use the suspicious email domain punkproof.com, while most use the hotmail, gmail and icloud domains.
- IP addresses from which the individuals logged into their admission portals did not match the vicinity of applicants' home addresses and often originated from outside the United States. Many IP addresses were repeated across otherwise unrelated applicant logins.
- Email addresses falsified to represent staff at a high school provided high school transcripts that, when compared to the appearance of other transcripts from the same high school, are noticeably fabricated.
- Many fraudulent applications with transcript requirements had official high school and college transcripts to complete their applications.
- During virtual advising appointments, fraudulent applicants refused to appear on video when requested
- Reported high school and college graduation dates do not align with legitimate documents. Or, the reported high school graduation date and an associated fabricated high school transcript place the applicant at an advanced age at the time of high school graduation.

Consequences and Outcomes
The Admissions Office remains on high alert for fraudulent documents and suspicious application data. Applicants to online degree programs are reviewed with increased scrutiny. Over 300 applicants have been marked Fraudulent since February 2025.

Four students who applied fraudulently have been dismissed from the university, preventing further enrollment and use of university resources.

The offices of admissions and the university registrar are working together to address system records created by fraudulent applications. Institutional Research is involved to ensure that fraudulent applications are not reported in official reports to external entities and agencies.

Remediation Efforts
Fraudulent applications are identified using technical and manual means. The University CRM enables staff to find suspicious IP address locations, known problematic email domains, and shared contact information.

To stop the submission of falsified applications with the intent to defraud, the following offices have created a Suspected Fraud team in Microsoft Teams where suspected fraud can be reported and discussed:

- Admissions
- University Registrar

- Financial Aid and Scholarships
- Bursar
- Internal Audit
- Information Technology
- Kent State University Police
- Student Conduct

When fraudulently enrolled students are discovered, they are addressed in the Team as quickly as possible to prevent the disbursement of financial aid. Guidelines on establishing a "confidence indicator" in an accusation of fraud are being designed, as well as steps to be taken when fraud is identified at different moments in the admissions funnel.

The Suspected Fraud team meets monthly to discuss the evolving nature of fraudulent applications. A subcommittee has formed to review technology that can assist in verifying the identity of applicants before an applicant is admitted and enrolled.

Case Study: Application Fraud for Financial Aid Refunds

Hocking College

Introduction

At Hocking College, the majority of the Fraudulent applications are working on obtaining refund overage money from the Financial Aid. These groups/individuals will apply for admission and send in full ISIRs for the student and then enroll in classes. The Fraudsters will then either sign into the courses long enough to receive the refund or complete the classes.

Details of the Fraudulent Activity

Describe the fraudulent activity with specific attention to the category, method, and scope.

- Type of Fraud: Fraudulent student applied for admission in Spring 2025 in General Studies. Enrolled in 10 credits for Spring 2025 Semester. Completed all classes with grades 2- A's and 1- F for the semester. Received an overage/Refund check of $5,280.00.

Detection and Investigation

- Enrolled in the summer semester and Autumn semester. We identified as Fraud during the summer semester before disbursal and froze all financial aid. We requested a Valid State ID for the verification process and have had no response. Students did not complete the summer classes and did not attend the Autumn semester since there was not a possibility of overage.

Consequences and Outcomes

- The real Individual that had their Identity Stolen called the school since they were notified, they have loans for Financial aid for Hocking College. We are working with the real person to identify all the fraud and resolve all issues.

Lessons Learned
This was one of many fraudulent applications received by Hocking College. The Applications are now processed through Bank Mobile application review and are flagged as fraud. There is still the need for the manual eyes-on approach to the applications as well. The applications that are received are being critically reviewed by the Registrar's Department. Hocking College has implemented a uniform approach for Fraud that includes all departments from the Registrar through academics involvement.

Case Study: Stolen Credit Card Refunds

Hocking College

Introduction
At Hocking College received fraudulent payments for outstanding charges on multiple student accounts.

Details of the Fraudulent Activity
Type of Fraud: The group in this fraud scenario applied for admission and registered for classes at Hocking College. After they registered, the students used a stolen credit card to pay their bill in full. After paying the charges the group dropped all classes except 1 to stay as a student within the system. This created a refund on their account. The true owner of the credit card identified these were fraudulent charges and the back notified Hocking College. This activity of enrolling, paying the charges and dropping classes occurred within a 5 minute time frame.

Detection and Investigation
When the bank notified Hocking College of the Fraudulent charges it immediately froze all accounts. This stopped any refund and Hocking reviewed all accounts to see if there were any other situations where a single credit card was used to pay on multiple accounts.

Consequences and Outcomes
The outcome is that the Fiscal office is now reviewing the payment methods from students to see if this continues to happen and stay ahead of this type of Fraud.

Lessons Learned
The lesson learned was that we need to be more aggressive in our monitoring of payments to see if there are multiple accounts being paid by a single credit card. Secondly make sure that any of these types of activities that create a refund are returned to the original credit card instead of disbursing a check.

Case Study: New Student Application, Identify, and Financial Aid Fraud

Lakeland Community College

Introduction/Background Information

Around summer of 2024, suspicions started to arise about the validity of recent applicants to Lakeland Community College in Kirtland OH. The following are the most blatant suspicious activities:

- SAT scores submitted directly from applicants were altered (different fonts, date of test was over 10 years after applicant graduated)
- When applicants contacted the Student Service Center to schedule Counseling and Advising appointments, it appeared to be the same person due to their similar way of speaking
- Applications were submitted back-to-back in the early hours of the day with most fields completed using all caps
- Multiple applications were submitted with the same mailing address; many of these addresses were for homes that were currently for sale and from several hours/states away
- Applications were being submitted from uncommon and disposable email addresses, such as punkproof.com, dcpa.net and ptct.net.
- High school transcripts were submitted from fraudulent high school email addresses
- A larger than normal number of applications with bachelor's and master's degrees earned were submitted

To date, nearly 700 new applicants have been identified as suspected fraud.

Details of the Fraudulent Activity

The intent of these suspected fraudulent applicants varies. It appears that some apply with the intent to commit identity fraud so that they can enroll in classes and receive federal financial assistance. For others, it appears they apply with the intent to commit phishing schemes to gather student information.

- We were able to identify less than a dozen applicants who were able to complete the admission process, register for classes and be awarded federal aid; unfortunately, they also did receive refunds for these classes. However, once identified, they were removed from their classes, and their federal aid was suspended until in-person verification at the Financial Aid Office was completed.
- For those students who were admitted but were identified prior to registration, in-person identity is required.
- Finally, for the phishing schemes, these applicants used their myLakeland student portal to access other student emails to request personal data and login information.

Detection and Investigation

All detection of fraudulent applications has been manual as our current CRM application system is currently lacking fraud detection. Thanks to the awareness of front-facing staff members, we were able to review applications and determine similar patterns (as indicated above). Once identified, the Admissions Office would use various methods to research applicant information.

The most common research methods we currently use are:

- Free Reverse Phone Number Lookup (https://www.usphonebook.com/)
- Google Maps
- Voter Records
- Lakeland's Police Department
- Lakeland's Administrative Technologies Department

Consequences and Outcomes

The most substantial consequences of suspected fraudulent applicants to the college are:

- Occupying class seats, thereby preventing legitimate students from registering
- Extensive staff resources are allocated to research within areas ranging from Admissions to Administrative Technologies
- The impact on financial aid has yet to be determined; however, any refunded aid funds represent an unfortunate outcome

Lessons Learned

These are some of the steps that have been taken by the college:

- New applications where information cannot be verified are sent an email that they must come in person to verify their identity and that their application is closed
- Admission and Transfer Center staff have been trained on the identification of fraudulent transcripts
- An in-person identity hold is placed on the student's record preventing the student from registration; the only way to remove the hold is to come in person to the college to verify their identity
- A financial aid hold is placed on the student's record preventing the distribution of federal aid; the only way to remove the hold is to come in person to the college to verify their identity
- New Student Orientation was changed to in-person; if an exception needs to be made, the student must fill out a Microsoft form providing the reason for the exception. If approved, the student must attend the meeting via WebEx and must show their ID to the counselor/advisor
- Admissions Office and Administrative Technologies work closely together to verify the validity of email and IP addresses and, if necessary, will block entire domains to prevent future applications
- Administrative Technologies identified the shortcomings of some of our existing products and is working with current and new vendors to upgrade our fraud detection capabilities
- Existing reports were modified to capture students with the same mailing address
- Re-introduction of the weekly review of an existing report to ensure that high school or college transcripts received are valid

Case Study: Returning Student Phishing Fraud

Lakeland Community College

Introduction/Background Information
Around early spring of 2025, suspicions started to arise regarding the validity of applications being submitted for returning students to Lakeland Community College in Kirtland OH. Since the returning student application does not require an application account to be created, it was much easier for these suspected fraud students to gain access to their myLakeland login information. The following are just some of the suspicious activities:

- Applications were submitted back-to-back in the early hours
- Applications were being submitted providing uncommon and disposable email addresses, such as punkproof.com, dcpa.net and ptct.net.
- Applications were being submitted with updated phone numbers and/or email addresses

To date, nearly 140 returning student applicants have been identified as suspected fraud.

Details of the Fraudulent Activity
Returning student applications were being submitted on a larger than normal scale. At first, these applications went unnoticed, and the student's account was reactivated, and they were sent their student portal login information. Using this information, it allowed them to phish current students for their personal data and login information. Additionally, some of the returning students did enroll in classes with the intent to receive federal aid funds.

Detection and Investigation
Eventually, it was discovered that many of these returning student applicants were providing new phone numbers and/or email addresses from uncommon and disposable email addresses. For the email addresses, we worked with the Administrative Technologies Department to block the entire domain to prevent further applications.

During this time, each application had to be manually reviewed by the Admissions Office to ensure the validity of the applicant.

The most common research methods we are currently using are:

- Free Reverse Phone Number Lookup (https://www.usphonebook.com/)
- Google Maps
- Voter Records
- Lakeland's Police Department
- Lakeland's Administrative Technologies Department
- Phone calls to applicants

Consequences and Outcomes
The most substantial consequences of suspected fraudulent applicants to the college are:

- Occupying class seats, thereby preventing legitimate students from registering
- Extensive staff resources are allocated to research within areas ranging from Admissions to Administrative Technologies

- The impact on financial aid has yet to be determined; however, any refunded aid funds represent an unfortunate outcome

Lessons Learned
These are some of the steps that have been taken by the college:

- Office of the Registrar has been trained on the identification of fraudulent applications
- An in-person identity hold is placed on the student's record preventing the student from registration; the only way to remove the hold is to come in person to the college to verify their identity
- A financial aid hold is placed on the student's record preventing the distribution of federal aid; the only way to remove the hold is to come in person to the college to verify their identity
- The returning student application was modified to include IP addresses and their location
- Admissions Office and Administrative Technologies work closely together to verify the validity of email and IP addresses and, if necessary, will block entire domains to prevent future applications
- Administrative Technologies identified the shortcomings of some of our existing products and is working with current and new vendors to upgrade our fraud detection capabilities

Case Study: Application Fraud: Returned Mail Leads to Falsified Transcript

Tony Box, Director of Admissions & Recruitment
Marion Technical College

Background Information
This incident began on August 15th when an application for general admission was submitted to Marion Technical College, Marion, Ohio. The application was made under the name of *John Doe* with a mailing address of Mentor, Ohio. The applicant did get enrolled into Fall 2025 term online classes but was removed from classes due to the submission of a fraudulent transcript. This is a violation of college policy AP420, Student Code of Conduct and Disciplinary Action.

Details of Fraudulent Activity
The college employs AI-based fraud detection on all submitted applications through its CRM, Element451. This particular application was scored as a medium risk. It showed signs of potential fraud but not enough to warrant immediate cancelation. The student's application was admitted on August 20, 2025 and a letter of acceptance mailed on August 21, 2025.

The student registered for classes on August 25, 2025. This was the first day of the fall term. The academic advisor reported that the student was aggressively rushing the enrollment process. The student was registered by the academic advisor during a phone appointment. No visual contact was made. The academic advisor reported that the student had a thick Asian or African accent.

Financial aid was being processed for this applicant. The applicant was set to receive $2,065 in Pell Grant, $3,500 of subsidized loan and $6,000 of unsubsidized loan.

Detection and Investigation
The applicant's acceptance letter was returned to the college by the USPS. It was received on September 17, 2025. The label, dated September 7, 2025, said refused. Further investigation into the applicant's record ensued. It was discovered that the address was an apartment complex that may not have been occupied by the applicant. It was also discovered that the high school transcript submitted was fraudulent. This was confirmed by the named high school. The submission of fraudulent documents is in violation of college policy AP420, Student Code of Conduct and Disciplinary Action. Although the IP addresses used during this time were Ohio-based, a recent check revealed that the applicant continued to open emails from an IP address in Nairobi, Kenya.

Once the transcript was determined to be fraudulent the academic advisor, director of financial aid, and IT staff were notified. The applicant's access to college resources was removed and financial aid processing stopped. I instructed the academic advisor to have the applicant contact me if the applicant questioned the denied access. The applicant did call me and, once informed of the fraudulent document, hung up.

Consequences and Outcomes
While the applicant suffers no consequences, the college was able to prevent this applicant from further use of college resources and the receipt of federal grants and loans.

Lessons Learned
The following are steps now taken by the college.

- New student applications that are scored as high risk are cancelled.
- New student applications that are scored as medium risk undergo more scrutiny.
- Further training on the identification of fraudulent transcripts has taken place.
- Returned acceptance letters trigger immediate scrutiny of the applicant's record. This includes review of the IP addresses used when interacting with admissions communications.
- An alert has been established in the college's CRM to notify admissions staff of applications submitted from IP addresses in Kenya.
    - Ideally, this notification would include applicant records for which IP addresses used are from outside the United States. Programming toward this is in process.
- Academic advisors are now aware that new students must be visually confirmed when scheduling classes. Zoom appointments must be conducted with the camera on and the applicant must present an ID to the academic advisor.
- Academic advisors also know to report suspicious applicants to the admissions office for further review of their record and online activity.
- Financial aid staff are notified early when an applicant is under further review.

Case Study: Questionable Admissions Documents and Potential Student Identity Fraud

Sherri Jiannuzzi, Director of Student Financial Aid Operations
University of Toledo

Background

During routine manual review of high school transcripts submitted in the Admissions process, staff identified multiple irregularities suggesting the possible submission of falsified or altered academic documents. The initial discovery prompted a broader investigation into admissions data and related student records.

Initial Findings

The review revealed numerous inconsistencies and anomalies within a subset of applications, primarily within the Online Admissions Applications. The irregularities included:

- Inaccurate or inconsistent GPA calculations
- Missing or mismatched signatures
- Poor grammar or spelling on official transcripts
- Obvious signs of digital overlay or tampering
- Identical signatures appearing on documents from multiple schools

These findings indicated a potential pattern of document fabrication or identity misuse.

Pattern Identified

Several recurring patterns and inconsistencies were noted among the suspect applications:

- Document and Origin Similarities
    - Batches of applications submitted from the same geographic area and/or using similarly formatted documents.
    - Clusters of submissions occurring within short time frames.
- Location and Contact Mismatches
    - Network pings or IP addresses originating outside the U.S. or in locations inconsistent with listed student addresses.
    - Student address on the high school transcript matching the current address for older applicants (unusual for legitimate records).
    - Area codes not aligning with listed physical addresses or schools.
- Email and Communication Irregularities
    - Unusual email formats (e.g., full name + full date of birth, or nonsensical combinations of letters/numbers).
    - Nearly identical email inquiries from different “students” regarding application status.
- Parchment Transcript Issues
    - Submitted Parchment ID numbers not found in the Parchment system.
    - ID numbers linked to different student names in Parchment.
    - Parchment notifications received regarding potential fraudulent submissions.

Scope of Identified Cases

- The initial review identified approximately 60 prospective students with questionable documentation.

- Most were intercepted prior to admission.
- Seven applicants successfully matriculated and registered for fall classes before detection.
- Immediate mitigation included placing Identity Confirmation Requirements on these student accounts.

Expanded Review of Current Students

To identify other potentially compromised or fraudulent student records:

- Data sources: Slate (Admissions system), Touchnet (payment processing), and other university reports.
- The Office of Special Accounts reviewed over 200 student accounts exhibiting red flag indicators.
- Approximately 100 students were identified for financial aid intervention:
    - Aid was withheld from packaging or removed entirely.
    - Students who could not be reached were placed on Identity Confirmation Holds to prevent further aid disbursement or enrollment activity.

Immediate Actions Taken

- Flagged accounts were reviewed jointly by Admissions, Financial Aid, Registrar, and Special Accounts.
- Identity verification processes were strengthened for all affected and at-risk students.
- Once there was confirmation that the "student" did not initiate admission and/or file for financial aid,
    - Courses were removed
    - Financial aid was cancelled, and any disbursed amounts were reversed
    - Holds were placed on student accounts
    - Access to portal and email were suspended
- Collaboration was initiated with Parchment to confirm transcript authenticity and monitor fraud alerts.
- In Process:
    - Report to the Department of Education's Office of Inspector General
    - Researching options to enhance technology to automate fraud detection flags
    - Reviewing institutional policies and procedures to address the increase in "red flag" activity across campus through training and awareness

Conclusion

The investigation revealed coordinated patterns of potentially fraudulent application activity involving falsified documents and mismatched identity data. Through swift cross-departmental collaboration, most affected cases were identified and mitigated before enrollment or financial aid disbursement. Continued vigilance, system improvements, and policy enhancements are essential to protect the integrity of the University of Toledo's admissions and financial aid processes.

Case Study: Identity Fraud Prevention

Kim Everhart, Director of Financial
Wright State University

Background

In July 2025, academic advisors at Wright State University's Lake Campus observed unusual behavior among four students enrolled in summer courses. These students exhibited signs suggesting they may not be who they claimed to be. Suspicious behaviors included:

- Unusual urgency in completing enrollment steps
- Inability to recall basic personal or academic information
- Inconsistent or multi-voiced responses during meetings
- Refusal to turn on cameras during virtual advising sessions
- Insistence on enrolling in fully online courses

These observations led advisors to suspect identity fraud, prompting a formal investigation.

Detection and Investigation

A university-wide task force was immediately established, consisting of representatives from:

- Lake Campus Enrollment Services
- Admissions
- Financial Aid
- Bursar's Office
- Internal Audit
- General Counsel
- Information Technology (CATs)
- Vice President of Enrollment Management
- Campus Police

Immediate Actions

1. Reviewed student data to identify additional fraudulent cases.
2. Selected suspicious students for aggregate verification through Financial Aid.
3. Flagged records within the ERP system.
4. Locked all covered accounts where fraud was confirmed.

Findings

- 4 additional fraudulent students identified at the Dayton Campus.
- 50 more applicants for the fall semester were flagged as high risk.

Common Indicators of Fraudulent Cases

- Enrolled exclusively or primarily in online courses
- Listed as *independent* on the FAFSA
- No prior financial aid history
- Geographic location is not consistent with historical trends
- IP addresses originating from outside Ohio or the U.S.
- Matching or similar IP addresses used to create banking accounts

- Refunds funneled into two common bank accounts
- Similar high schools: Wilmington High School and Oak Hills High School
- Submitted authentic transcripts
- Used Outlook email addresses

Consequences and Outcomes

- Eight fraudulent students successfully received $18,000 in refund checks for the summer semester.
- All cases were reported to the Office of Inspector General (OIG) for further investigation.
- Institutional safeguards were strengthened immediately following detection.

Policy and Process Enhancements

- Applications with high-risk indicators are now flagged before being admitted. If admitted with a suspicion of fraud, they are selected for aggregate verification and flagged in our ERP system**.**
- If fraud is confirmed, all covered accounts are locked.
- Financial Aid and Bursar teams actively monitor for fraud indicators among currently enrolled students.
- A reporting tool was launched to allow staff and faculty to report suspicious student activity.
- A standing Fraud Prevention Task Force meets regularly to review:
    - Policy updates
    - Procedural improvements
    - Training needs across departments

Appendix C

Best Practice Recommendations

Based on the case studies, Ohio public community colleges and institutions have developed a variety of actions to combat fraud. These best practices are detailed below

I. Establish a College-Wide Fraud Team: Key Offices and Top Priorities

Establishing a dedicated college-wide fraud awareness team is essential for protecting the institution's reputation, resources, and academic integrity. With rising threats such as fraudulent applications and financial aid misuse, a unified response allows campuses to proactively address vulnerabilities, foster transparency, and support students and staff in recognizing and reporting suspicious activity.

Colleges such as Columbus State Community College, Cuyahoga Community College (Tri-C), Lorain Community College, and Kent State University have already established fraud prevention teams, demonstrating the effectiveness of collaboration across departments. These institutions serve as models for others by illustrating how coordinated efforts improve risk detection, reporting, and the overall security of institutional operations.

Recommendations for Representation

It is recommended that a core fraud prevention team include the following offices (or similar functions):

- Admissions: Screens applications to detect and prevent credential fraud and misrepresentation.
- Bursar/Billing: Oversees payments and student accounts, identifying financial anomalies.
- Financial Aid: Monitors aid distribution for irregularities and investigates suspicious claims.
- Information Technology: Protects data systems and implements digital security measures.
- Registrar: Maintains academic records and ensures transcript integrity.

Related areas that would add value to a fraud prevention team include:

- Faculty Governance: Supports academic integrity and policy alignment.
- Internal Audit: Reviews processes and recommends controls to reduce fraud risk.
- Legal Counsel: Ensure the college operates within the boundaries of the law and to mitigate legal risks associated with its operations.
- Campus (Community) Police/Public Safety (if applicable): Investigate criminal aspects of fraud and protect campus/community assets.

Top Priorities for the Fraud Awareness Team

Following the creation of a campus fraud awareness team, it will be important for the team to:

1. Establish a Charter: Define the team's mission, scope, and values to guide activities and decision making.
2. Define Objectives: Set clear goals such as reducing fraud risks, promoting integrity, and ensuring regulatory compliance.

3. Update Policies and Procedures: Responsibility for reviewing current vulnerabilities and make recommendations to strengthen and change existing processes.
4. Create a Training Program: Develop educational initiatives for students, faculty, and staff to recognize fraud and understand reporting procedures.
5. Implement Data Monitoring: Set up systems to track and analyze fraudulent application patterns, financial irregularities, and other suspicious activities. Use metrics to inform prevention strategies and measure effectiveness.
6. Fraud Reporting: Create a process for institutions to track fraudulent activity and provide necessary reporting to state level authorities.
7. Regular Coordination & Continuous Improvement: Hold standing meetings to review case trends, share updates, and refine policies and training based on changing threats and lessons learned.

By prioritizing the creation of a multidisciplinary team, colleges can proactively defend against application and financial aid fraud, improve transparency, and cultivate a culture of integrity across campus operations. The involvement of the key offices listed above, and a focused set of priorities ensures that the institution remains vigilant, adaptive, and supportive in safeguarding its students, staff, and resources. The experience of Columbus State Community College, Cuyahoga Community College, Lorain Community College, and Kent State University underscores the value and practicality of establishing such teams within the college environment.

II. Involve Campus Police/Security and Outside Law Enforcement in Fraud Investigations

To ensure the integrity of our academic and administrative processes, it is recommended that Campus Police/Security continue to play an active role in investigating suspected fraudulent student activity. Their involvement is essential in verifying student identities, determining physical locations of suspected individuals, and supporting cases of potential identity theft or other fraud.

Campus Police, who assist in fraud investigations:

- Verify the identity and location of individuals suspected of fraud;
- Investigate and document incidents related to identity theft;
- Coordinate with external law enforcement agencies when cases extend beyond campus jurisdiction.

Recommendation:

- Maintain and formalize these collaborative procedures through written protocols or Memoranda of Understanding (MOUs) between Campus Police and local law enforcement agencies
- Provide specialized training for Campus Police on digital identity verification, online fraud detection, and privacy compliance
- Continue to foster cross-departmental communication between Campus Police/Security, Student Affairs, IT, Business Office and Enrollment Services to ensure timely and coordinated responses to potential fraud cases

III. Invest in Fraud Prevention and Identity Verification Software

Higher education institutions are facing an increasingly complex landscape of fraud, driven by rapidly evolving tactics and technologies. Many institutions remain reactive, struggling to keep pace with the shifting threat environment. Through conversations with various stakeholders and research into current practices, two critical areas have emerged where software solutions could significantly enhance efficiency and accuracy: the initial validation of applicant data and real time identity verification.

Initial validation of applicant data usually involves cross-referencing applicant data (e.g., name, address, phone, email, IP address) against authoritative sources to detect inconsistencies and strengthen downstream identity verification. Although many institutions are tackling this process manually, it can be embedded directly into customer relationship management (CRM) platforms like Slate and Element 451, or integrated via APIs and third-party services such as LexisNexis, Trestle, Bankmobile, and SAFE. By leveraging robust databases and intuitive AI, these tools enable institutions to automatically categorize applicants into customizable risk tiers, significantly reducing the manual workload for admissions and operations staff and enhancing both accuracy and efficiency.

Identity verification software is another critical tool frequently cited by institutions seeking to reduce fraud. These solutions can authenticate government-issued IDs by analyzing hundreds of micro-details that are nearly impossible for staff to be familiar with and verify manually in real time. Platforms like Intellicheck and IDScan offer intuitive, self-service interfaces that empower applicants to complete the verification process independently. In addition to scanning a wide range of ID types within seconds, these tools often include advanced features such as liveness detection and anti-spoofing checks, further strengthening the integrity of identity validation without burdening staff.

While there is no one-size-fits-all solution for institutions, investing in a software solution or combination of solutions may reduce the risk of financial loss, reputational damage, and resource strain currently being caused by fraudulent activity and help safeguard their operations and student communities. Successful adoption of software aimed at fraud prevention requires careful consideration of each institution's unique structure, existing infrastructure, and budget. Evaluating software options based on their features, accuracy, cost, and ease of implementation and integration will help ensure that the chosen solution delivers meaningful impact. Although it is difficult to know the best path forward in an increasingly complex and ever-changing fraud landscape, institutions can take meaningful steps toward prevention by embracing a layered, customizable, and technology-driven strategy. In a time when fraud is growing more sophisticated, adopting smart, scalable safeguards is essential.

IV. Implement Financial Aid Disbursement Best Practices (Pell Grants and Two Disbursements of Student Loans

Overview

Lorain County Community College (LCCC) disburses financial aid—including Pell Grants and Federal Direct Student Loans—based on student enrollment, attendance, and academic progress.

This guide outlines best practices for supporting students through the disbursement process, with a focus on the two-part loan disbursement policy.

General Financial Aid Disbursement Principles

- Tuition and fees are paid first from financial aid funds.
- Remaining aid is applied to other educational expenses (e.g., books, housing).
- Students are responsible for monitoring their account balance in MyCampus.
- Non-payment results in a Bursar's hold, preventing future registration.

Pell Grant Disbursement

- Pell Grants are disbursed **starting in the fifth week of the term**, but only for courses where the student has **commenced attendance**.
- Late-start courses are not eligible for disbursement until attendance begins.
- Pell eligibility is based on **enrollment intensity** as of the **census date** (14th calendar day of the semester).
- Only courses that count toward the student's program of study and are registered by the census date are eligible.

Student Loan Disbursement: Two-Disbursement Policy

To promote student success and reduce loan default rates, Federal Direct Student Loans are disbursed in two installments during fall and spring semesters:

First Disbursement (Week 5)

- Student must have commenced attendance.
- Must be enrolled in at least six credit hours.
- Disbursement includes half of the eligible loan amount.

Second Disbursement (Week 10)

- Student must still be enrolled in at least six credit hours.
- Must have successful midterm grades in those courses.
    - Grades of W (Withdrawn), U (Unsatisfactory), or FAW (Failure due to non-attendance) do not count toward the six-credit minimum.
- Remaining half of the loan is disbursed.

Summer Term

- Only one disbursement occurs, around July 1.
- Student must be enrolled in six credit hours and have commenced attendance.

Refunds

- Refunds are processed by the Student Accounts Office, not Financial Aid.
- Refunds are mailed to the student's official address listed in MyCampus.
- Students should be advised to keep their address updated and monitor MyCampus for billing and refund status.

Key Advising Tips

- Encourage students to attend all classes from the start of the term to avoid delays or loss of aid.
- Monitor midterm grades and proactively support students at risk of losing eligibility for second loan disbursement.
- Remind students that dropping below six credit hours before loan disbursement will result in cancellation of loan funds.
- Advise students to check with instructors before withdrawing from a course.
- Ensure students understand that aid may be adjusted if they do not begin attendance or withdraw from all classes

Communication Best Practices

1. Reinforce that **not receiving a bill is not an excuse** for non-payment—balances are always visible in MyCampus.
2. Use multiple channels (email, advising sessions, workshops) to educate students on disbursement timelines and requirements.
3. Encourage students to ask questions before using any aid funds if they're unsure about eligibility.

V. Train Staff on Fraudulent Applications and Ghost Students

Fraudulent applications and "ghost students" are a growing threat. Given the sophistication and scale of these fraudulent activities, comprehensive training across every level of the institution is essential. Bad actors who submit fraudulent applications constantly adapt their methods, targeting vulnerabilities in admissions, financial aid, and IT systems. Without coordinated awareness and preparedness, institutions risk significant financial losses, data breaches, and reputational damage. By training front-line staff, administrators, and faculty, colleges ensure that everyone, from those verifying documents to those overseeing policy and compliance, can recognize suspicious patterns, respond quickly to emerging threats, and collaborate to fortify defenses.

Institution-wide training not only equips each department with specialized skills tailored to their responsibilities but also fosters a culture of vigilance and accountability. Admissions teams learn to detect anomalies in applications, IT professionals stay current with the latest security tools, and faculty become alert to irregular attendance or participation that might signal a ghost student. When all staff members understand the stakes and share best practices, the institution becomes more resilient, able to respond proactively to fraud rather than reactively after damage is done. This unified approach is crucial for safeguarding financial resources, protecting student data, and maintaining the integrity of the institution.

Front-Line Staff: Admissions/Enrollment Staff, Financial Aid, IT Helpdesk

Focus: Recognizing fraud at point of entry

Front-line staff such as admissions and enrollment personnel, financial aid teams, and IT helpdesk workers play a crucial role in detecting and preventing fraudulent applications and ghost students at the initial point of contact.

Frontline staff should be trained to identify and intercept fraudulent applications and ghost students from the outset before it can affect institutional resources. They should learn comprehensive identity verification using multi-factor checks and be able to spot red flags, such as repeated contact information across multiple applications or unusual IP addresses that may indicate coordinated fraud. Staff should receive a guide on application red flags that is routinely updated based upon changing trends and issues. Staff should also develop expertise in authenticating documents, including detecting fake transcripts or forged paperwork, fake government issued IDs, and should be encouraged to utilize automated verification tools when available. Furthermore, frontline personnel should be familiar with the latest fraud detection software and link analysis technologies, ensuring they are equipped to recognize evolving patterns of fraudulent activity and networks of connected accounts.

Financial Aid Staff Training: Financial aid staff should receive specialized training to recognize irregularities in FAFSA filings and verification paperwork, such as discrepancies in reported income, suspicious patterns in dependent status, or inconsistencies between student-provided documentation and official records. Training should include guidance on detecting unusual or altered financial documents, verifying the authenticity of tax transcripts, and identifying signs of identity theft or manipulation in aid applications. In addition, financial aid teams should be well-versed in federal and state regulations related to student aid fraud, such as requirements for identity validation, reporting suspected fraud, and maintaining compliance with Department of Education standards. Staff should also learn best practices for secure document handling, proper use of verification software, and collaborating with other departments to share information about emerging fraud trends. Regular workshops or webinars on regulatory updates, fraud prevention strategies, and case studies of recent incidents can further strengthen the financial aid team's ability to protect institutional and federal financial aid resources.

In addition, IT staff should receive training on leveraging institutional resources to proactively identify and prevent fraud. This includes effective use of multi-factor authentication systems, such as Duo, to safeguard access and verify user identities.

Administration

Focus: Policy, oversight, and resource allocation.

This section emphasizes the importance of comprehensive training for administrators, focusing on policy, oversight, and resource allocation to combat fraudulent applications and ghost students. Administrators are equipped with the knowledge to meet compliance requirements, including identity-validation standards set by the Department of Education. Through risk assessment workshops, they learn to identify vulnerabilities in online enrollment and financial aid systems, enabling proactive prevention strategies. Crisis response drills are recommended to ensure administrators are prepared to manage large-scale fraud incidents, complete with well-defined escalation procedures and clear communication protocols. Additionally, data analytics training helps administrators leverage dashboards to monitor unusual patterns in enrollment and aid distribution, allowing for early detection and response to potential threats. This targeted approach ensures that leadership is actively involved in safeguarding institutional and financial resources.

Faculty

Focus: Classroom-level awareness and reporting.

Faculty should receive targeted training to help maintain classroom integrity and identify fraudulent activities at the instructional level. This training should focus on increasing awareness of ghost students and the risks associated with classroom-level fraud. Instructors should be trained to routinely verify class rosters and promptly report any instances where seats remain empty despite being officially full, as this may signal fraudulent enrollment. Additionally, faculty should receive basic cybersecurity instructions to recognize the misuse of institutionally assigned email accounts by ghost students—such as for phishing attempts or unauthorized access to institutional resources. The training must also include clear, accessible procedures for reporting suspicions of fraud to compliance teams to ensure swift investigation. With these protocols and knowledge, faculty will be equipped to actively contribute to a collaborative, vigilant campus environment that helps protect the institution from evolving threats.

Students

Focus: Awareness and self-protection.

Students should receive training designed to increase their awareness and ability to protect themselves against fraud. This includes participating in brief online modules during orientation that emphasize the risks of identity theft and explain how scams can interfere with financial aid processes. The training should teach students to recognize phishing scams by identifying fraudulent emails, text messages, or websites that attempt to obtain personal or financial information. Key topics should include typical phishing strategies, such as urgent requests for login details, deceptive links, and suspicious attachments, as well as the ways these scams can jeopardize student accounts or redirect financial aid funds. Instruction should also cover essential digital hygiene practices, providing students with practical tools to safeguard their personal data and spot phishing attempts.

Recommended Delivery Methods

- Blended Learning: Combine online modules for scalability with in-person workshops for interactive problem-solving for faculty and staff.
- Microlearning: Short, role-specific videos for quick refreshers.
- Annual Refreshers: Update training to reflect evolving fraud tactics (e.g., AI-driven scams).
- Routine Stakeholder Communication: Implement scheduled emails and newsletters to all stakeholders—administrators, faculty, and students—with timely updates on new fraud trends, reminders about detection protocols, and policy changes.
- Targeted Publications: Distribute regular bulletins and guides tailored for each stakeholder group, containing relevant case studies, step-by-step reporting instructions, and best practices for fraud prevention and response.

VI. Create an Internal Reporting and Data Sharing Framework

Purpose

This best practice establishes a recommended framework for institutional transparency and responsible data collection, data sharing, and internal reporting in support of fraud prevention.

The goal is to ensure that all members of the institution understand their roles in the detection, reporting and case support of suspected fraud.

Scope and Assumptions
This best practice:

- Applies to all faculty, staff, and affiliated personnel of the institution.
- Complements existing institutional policies on ethics, compliance, and data governance, while outlining operational expectations for transparency, fraud detection, research and reporting.
- Assumes the institution has adopted a model in which a *Campus-Wide Fraud Awareness Team* has been established to coordinate and oversee fraud prevention efforts.

The institution is committed to protecting students, prospective students, and the broader community from individuals or entities engaging in fraudulent or deceptive activities. Unchecked fraud can cause significant harm to individuals and to the institution's reputation.
Members of the institution are expected to support internal fraud investigations and promptly report suspected fraudulent activity. The institution will ensure that all reports are handled with confidentiality, fairness, and due process.

Data Collection, Sharing, and Transparency
The *Campus-Wide Fraud Awareness Team* is responsible for maintaining a centralized and secure reporting system or database for receiving, tracking, and managing suspected fraud information.
The system shall:

- Be accessible to faculty, staff, and other affiliated personnel;
- Contain clear guidance on how to report information through secure web forms, designated email addresses, or other approved communication methods;
- Protect the confidentiality of reporters and the information provided; and
- Provide access to case outcomes or summary updates where appropriate, in compliance with privacy and legal requirements.

The team shall regularly review the effectiveness of the reporting mechanism and recommend improvements as needed. Information collected will also support ongoing efforts to identify trends, strengthen internal controls and enhance prevention strategies.

Confidentiality
Individual cases and identifying information shall not be disclosed outside authorized personnel, except as required by law or institutional policy.

VII. Establish a Transcript Review Process

Prior to entering transcript data into software system, always inspect the transcript for any red flags.

Transcript Appearance:

1. Font/Size Inconsistency: Transcript grades, courses, student name, dates have inconsistent fonts or font sizes.

2. Mis-alignment: Terms or other data tables seem misaligned with the rest of the transcript.

3. Missing signature and/or seal: notice if they appear extremely pixilated/blurry.

4. Extra or inconsistent blank/empty spaces

5. Page numbering that does not match the total number of pages received

6. Missing grading scale/legend

Transcript Content:

1. Course subjects:
    a. If a transcript is missing general education/traditional coursework.
    b. If course subjects don't align with the timeline the student attended (i.e. "Typewriting", but the student graduated in 2020
    c. For college transcripts: does the course subject matter generally align with their declared major?
    d. Generic course titles: like "Business" or "Computers"

2. Grade vs. GPA:
    a. If the cumulative GPA is notably higher than the course grades would typically allow.
    b. Honors are awarded consistently or despite low grades.

3. Graduation/attendance dates: If the date(s) of graduation/attendance do not generally align with the student's age

4. Print date: Was this transcript printed within the last year?

5. Inconsistent course codes: Do the course subject and numbers follow a standard format throughout?

6. Credit completion rate:
    a. Does the transcript list an over-abundance of completed coursework in one term or year?
    b. Was there a reasonable time to degree completion/graduation?

7. Spelling, punctuation, and grammar: Are there consistent or egregious spelling, punctuation, or grammar errors?

Parchment-specific Transcripts:

1. Home school transcripts sent via Parchment are not verified by the servicer. Be sure the student submits a District Verification Letter prior to processing.
2. Verify the Parchment banner at the top of the document is spelled correctly and not blurry. It should always contain a DID and Parchment ID.
3. Parchment never alters the appearance of a transcript, so the same items above should be considered.

Initial steps when a document is in question:

1. Verify the institution and its general information.
    a. Does this all match perfectly with what is on the transcript?
    b. Is the school still in operation?
    c. Was it in operation when the student attended?
    d. Is it accredited?
2. Confirm how it was received:
    a. If via Parchment or National Student Clearinghouse: verify through their portal libraries.
    b. If a physical copy was mailed, verify in OnBase who uploaded the transcript.
        i. Reach out to that individual and inquire if they noticed anything suspicious.
    c. Always check SPACMNT for any relevant comments.
3. Have we received previous copies of this student's academic record from the institution? If yes, confirm the information matches previous versions.
4. If any questions persist, add an RV hold immediately, and clarify the situation in a SPACMNT comment.
    a. Use "See SPACMNT" in the SOAHOLD comment.
    b. Use "INF" for the comment code in SPACMNT.
5. Notify the Assistant Registrar and Registrar immediately

VIII. Implement Processes and Create Reports for Fraud Detection at Point of Application

- Monitor Application Volume
    - Run volume reports daily or weekly to identify spikes in application submissions.
    - Set thresholds (e.g., more than X applications in an hour/day) to trigger alerts for further review.
    - Flag batches of applications submitted within short timeframes, especially from the same IP address or device.
- Identify Duplicate or Suspicious Data
    - Duplicate Data Report: Find repeated email addresses, phone numbers, or SSNs.
    - Geolocation Report: Flag applications from high-risk or mismatched regions.
    - Document Verification: Check for altered or suspicious documents.
- Automate Alerts and Reviews
    - Configure system alerts for unusual submission patterns (e.g., many applications at once).

    - Schedule regular audits of flagged applications and maintain investigation logs.
- Cross-Reference External Databases
    - Use identity verification services to validate applicant details.
- Monitor Returned Admissions Acceptance Letters
    - Track and report on admissions acceptance letters that are returned as undeliverable.
    - Investigate patterns of returned letters, as these may indicate fraudulent or inaccurate applicant addresses.
- Staff Training
    - Train admissions staff to read reports and recognize and escalate suspicious patterns.

IX. Allow Identify Verification for On-Line Students at Participating Colleges

To maintain the integrity of the admissions process and protect against fraudulent activity, the colleges require identity verification for applicants whose records raise concerns of potential fraud. In such cases, students are asked to present a valid, government-issued photo ID in person. Applicants located within one hour of campus are required to complete this verification at the College's Admissions Office. For students residing beyond this distance, participating institutions across the State of Ohio may facilitate the verification, allowing students to visit the school closest to them. Each institution designates a single admissions contact responsible for confirming the student's identity and communicating verification approval to the requesting institution. This coordinated approach ensures both accessibility for applicants and consistency in upholding secure admissions standards statewide.

The coordinated identity verification process prompted significant discussion regarding its potential application within Financial Aid offices, particularly for the federally mandated V4 verification process. Currently, Financial Aid offices permit students to complete identity verification either in person or through a certified notary. However, some expressed concerns about extending this responsibility to participating institutions, citing differences in institutional procedures. Others noted declining confidence in the notary option due to the increasing sophistication of fraudulent identification documents and the limited training most notaries receive in detecting them. Several stakeholders suggested that trained Financial Aid professionals at other Ohio institutions may, in fact, be better equipped to perform this verification accurately and securely. FERPA compliance could easily be built into the process. Given these differing perspectives, further discussion and alignment among participating institutions will be necessary before expanding the coordinated verification model to include Financial Aid functions.

Appendix D

Fraud Prevention and Identity Verification Software Reviewed by Fraud Prevention Workgroup

LexisNexis

- **Software Type:** Tailored risk models based on institution's risk tolerance
- **Key Features:** "Emailage" and Flex ID options for parsing application information into risk categories for further follow-up
- **Notable Strengths:** Massive identity consortium, predictive analytics
- **Limitations:** No real-time ID verification; possible to get around with enough identity info?
- **Pricing Model:** Custom enterprise pricing
- **Compatibility / Ease of Implementation:** Not specified

Trestle

- **Software Type:** Robust identity data APIs that enhance contactability and verification
- **Key Features:** Cross-references applicant data (e.g., name, address, phone, email) against authoritative sources to flag inconsistencies and improve downstream identity checks
- **Notable Strengths:** Not specified
- **Limitations:** Not specified
- **Pricing Model:** Options ranging from $0.04–$0.15 per verification
- **Compatibility / Ease of Implementation:** Not specified

Telesign

- **Software Type:** Phone number verification
- **Key Features:** Validates number type, tenure, and subscriber status; can provide an "Intelligence Risk Score"
- **Notable Strengths:** Strengthens and validates end-user mobile identity
- **Limitations:** Only validates phone number information, not email, not real ID
- **Pricing Model:** "Intelligence Risk Score" is an added cost (exact pricing not specified)
- **Compatibility / Ease of Implementation:** Not specified

IDScan.net

- **Software Type:** Real-time ID Verification (document and selfie)
- **Key Features:** ID verification (state IDs and passports), DMV API integration
- **Notable Strengths:** Real-time ID validation, hardware integration for in-person, SOC 2 certified
- **Limitations:** Not verifying phone or address info or providing risk categories for application review with that info; DMV integration an added cost
- **Pricing Model:** Tiered plans, $800/mo for 2,000 verifications; DMV integration additional $1.25 per scan completed
- **Compatibility / Ease of Implementation:** Can use ad hoc or integrate into application

Intellicheck

- **Software Type:** Real-time ID Verification (document and selfie)
- **Key Features:** Real-time ID barcode verification, state IDs and passports, REST API, omnichannel support, white-label capture
- **Notable Strengths:** 99.975% verification accuracy, DMV system integration, seamless integration, mobile SDK, SOC 2 Type II Audit
- **Limitations:** Not verifying phone or address info or providing risk categories for application review with that info
- **Pricing Model:** One-time integration fee ($500 for portal; API fee not specified); $5,000 annual minimum; $1.68 per verification completed
- **Compatibility / Ease of Implementation:** Can use ad hoc or integrate into application

Element451

- **Software Type:** CRM with built-in AI-powered fraud detection
- **Key Features:** Verifies address and phone number, assigns risk level to applications for further follow-up
- **Notable Strengths:** More automated initial application review, no added cost to fraud detection if using CRM software
- **Limitations:** Must use Element451 as your CRM; still need manual follow up on risk categories
- **Pricing Model:** Not specified
- **Compatibility / Ease of Implementation:** Not specified

LightLeap AI

- **Software Type:** Generative AI and Intelligent Automation platform
- **Key Features:** Real-time detection of anomalies and suspicious behaviors in admissions, registration, and financial aid; verifies ID (photo ID and selfie), address, phone number, IP address, and assigns fraud risk
- **Notable Strengths:** System learns and adapts as it collects more data from across all users to improve fraud detection
- **Limitations:** Higher cost for full suite of options may be expensive for smaller institutions
- **Pricing Model:** Tiered subscription plan
- **Compatibility / Ease of Implementation:** Designed for plug-and-play integration with SIS, LMS, CRMs, etc. Leverages N2N core middleware for integration

S.A.F.E. (Student Application Fraudulent Examination)

- **Software Type:** Fraud detection and prevention software suite
- **Key Features:** ID verification, checks public record data, flags potential fraud indicators, assigns risk level
- **Notable Strengths:** Cross references data across multiple databases
- **Limitations:** Address verification is a link to Zillow, cost per ID check
- **Pricing Model:** Custom pricing based on number of applications, implementation fee, and yearly subscription fee
- **Compatibility / Ease of Implementation:** Integrates with CRM and SIS using API connector

BankMobile

- **Software Type:** Direct feed from CRM to evaluate all applications as they are submitted
- **Key Features:** Verify address and IP Address, phone numbers
- **Notable Strengths:** System builds and learns from all colleges input
- **Limitations:** Not specified
- **Pricing Model:** About $12,000 setup cost; designed for spreadsheet uploads or direct feed from SMS
- **Compatibility / Ease of Implementation:** Not specified

SLATE

- **Software Type:** CRM with built-in AI-powered fraud detection
- **Key Features:** Stripe-powered identity verification process
- **Notable Strengths:** Small additional cost ($2 per verification)
- **Limitations:** Must use SLATE as your CRM; still need manual follow up on risk categories
- **Pricing Model:** Not specified
- **Compatibility / Ease of Implementation:** Schedule a demo here: https://slate-partners.technolutions.net/portal/admissions

Free resources to use on an ad hoc basis:

- IDScan app for validating state IDs (not checking against DMV information) - limited free trial
- Individual phone # verification: USPhoneBook or NumLookUp
- Batch phone # verification: Trestle (limited free trial) or Twillio