Addressing Fraudulent Applications and Enrollment Activity

IN HIGHER EDUCATION

An AACRAO Issue Brief

Executive Summary

Higher education institutions are experiencing a significant rise in fraudulent admissions applications and "ghost student" enrollment schemes. Perpetrators use stolen or fabricated identities—increasingly aided by automation, AI-generated documents, and even human-operated call centers—to access financial aid, exploit .edu email privileges, and harvest institutional data. Some evidence suggests links to organized crime networks.

Institutions face financial liability for Title IV repayments, operational strain across multiple departments, and data integrity issues that affect planning and budgeting. Legitimate learners may experience delayed access to financial aid or encounter additional verification barriers when fraud controls are not carefully calibrated.

Key Points:

- Two primary fraud types require attention: **identity fraud** (impersonation) and **document fraud** (falsified credentials)
- Community colleges and open-access institutions are disproportionately targeted due to their accessibility-focused missions
- Effective response requires **cross-functional teams** spanning faculty**,** financial aid, admissions, registrar, IT, and security
- **Technology solutions help, but cannot replace human verification**—false positives risk blocking legitimate learners
- **Learning and Employment Records (LERs)** represent a systemic solution through verifiable digital credentials

AACRAO's Position: Institutions must balance fraud prevention with maintaining access for legitimate learners. The sector has demonstrated strong self-governance through robust institutional practices, and coordinated action at the institutional, system, and national levels will strengthen these defenses.

Call to Action: AACRAO urges all institutions to review and update their fraud prevention practices regularly, collaborate across departments and with peer institutions, and engage with state and federal partners to strengthen our collective defenses.

The Problem

Higher education institutions are experiencing a significant rise in fraudulent admissions applications and enrollments. These schemes—commonly called "ghost student" activity—involve the use of stolen or fabricated identities to access financial aid and institutional resources. A "ghost student" is a fictitious or stolen identity used to submit fraudulent applications and, in some cases, to enroll and access benefits without the intention of completing coursework or earning credentials.

The problem is pervasive across sectors but disproportionately affects community colleges and open-access institutions, whose missions of accessibility and affordability make them attractive targets. Online learning options and zero-application-fee policies further lower barriers to entry for bad actors. There are also growing reports of fraudulent activity in readmission and non-credit populations at four-year institutions.

This issue brief provides guidance for strengthening fraud prevention practices. Detailed implementation resources—including workflows, checklists, and technology evaluation criteria—appear in the appendices.

Two Forms of Fraud

Identity Fraud involves impersonation using stolen or fabricated identities to gain system access. Fraudsters leverage bots, artificial intelligence, and staffed call centers to impersonate legitimate learners. Indicators include mismatched personal information (name, SSN, DOB) or use of identities belonging to individuals who have stopped out, are deceased, or are incarcerated.

Document Fraud (Academic Credential Fraud) involves falsified records during the application process, including altered transcripts, forged certificates from unaccredited or non-existent institutions, manipulated grades or test scores, and fraudulent GEDs. Technological enhancements have made these forgeries increasingly difficult to detect.

Common Motivations

- **Financial Aid Theft**: Fraudsters exploit federal and state financial aid programs, often enrolling only long enough to trigger disbursement before disappearing.
- **Money Laundering**: Some schemes involve using stolen credit cards to pay tuition, withdrawing before refund deadlines, and redirecting reimbursements to new accounts.
- **Digital Resource Exploitation**: .edu email addresses grant access to discounted software, cloud storage, and can be used for spam/phishing networks.
- **Data Harvesting**: Once inside institutional systems, fraudsters may attempt to access directories or learner data for future exploitation.

Common Red Flags

Category	Key Indicators
Personal Information	Inconsistent or incomplete data; mismatched SSNs or birthdates; commercial or vacant addresses; unusual age patterns; inactive phone numbers
Application Behavior	Multiple applications from a single IP address or geographic area; bulk submissions during holidays or off-hours; identical email patterns or nonsensical usernames
Documents	Forged or altered transcripts; mismatched fonts or formatting; spoofed credentialing services; diplomas from non-existent schools
Behavioral	Urgency about financial aid; refusal to provide ID; unprofessional communication; VPN use to conceal location; contacts from blocked caller ID numbers

See Appendix F for detailed checklists organized by fraud type for staff training.

Institutional Impact

Fraudulent activity affects institutions across multiple dimensions:

- **Financial Exposure**: Institutions face repayment obligations for stolen federal and state aid and losses from unpaid tuition and fees.
- **Operational Strain**: Admissions, financial aid, and IT teams face increased workloads due to manual identity verification, investigations into suspicious records, and fraud prevention system management.
- **Data Integrity**: Inflated enrollment numbers distort institutional planning and budgeting. "Ghost" students can result in unnecessary class sections or adjunct hires.
- **Cybersecurity Risks**: Fraudulent accounts expand the attack surface for cyber threats and misuse of institutional systems.
- **Barriers for Legitimate Learners**: Overly aggressive fraud controls can inadvertently discourage legitimate applicants—especially first-generation, low-income, housing-insecure, or undocumented learners. Additionally, seats filled by ghost students mean fewer opportunities for real learners.

Current Institutional Practices

Institutions have developed comprehensive approaches to address application fraud, demonstrating the sector's commitment to proactive self-governance.

Procedural Defenses

- **Multi-Stage Verification**: Tiered screening using data reviews and public database cross-checking to identify fraud or validate legitimate applications.
- **Cross-Departmental Coordination**: Fraud response teams, including representatives from admissions, financial aid, records, IT, and campus security.
- **Identity Verification Holds**: Applicants flagged for review will have temporary registration holds until their identities are confirmed.
- **Faculty Engagement**: Instructors take attendance and report non-participating learners early in the term to prevent fraudulent aid disbursement. Note: This is not a fail-safe, as ghost students who understand the participation requirement may log in just enough to trigger aid release before disappearing.

Technology Solutions

Many institutions employ AI-powered fraud detection tools that analyze applicant data in real time and flag inconsistencies based on risk scoring. These systems cross-reference data across public and proprietary databases and detect patterns in location, timing, and applicant behavior. Data sources include:

- **Public and Commercial Databases**: Voter registration, telephone directories, utility and email service providers, global watchlists, and DMV records
- **Financial and Identity Verification Services**: Credit bureaus for cross-referencing Name, SSN, and DOB; some institutions are piloting systems utilizing Lexis-Nexis and ID.me
- **Real Estate and Demographic Information**: Public real estate data to identify addresses listed as commercial properties, vacant lots, or properties for sale

System-Level Responses

Some state systems have developed centralized strategies, including unified application portals, standardized fraud protocols, and cross-institutional data sharing. For example, following publicized financial aid fraud incidents, California implemented a feature that allows learners to connect their CA DMV mobile driver's license via the CA DMV Wallet app for secure identity verification through the Open CCC and CCCApply platforms serving the 116 California Community Colleges. This approach serves as a model other state systems could adapt.

Compliance Considerations for Institutions

Institutions must maintain robust compliance management systems and have capable staff to administer Title IV programs. Financial aid offices manage a broad range of compliance responsibilities related to Title IV funding, but the work of compliance is an institutional effort. The National Association for Student Financial Aid Administrators (NASFAA) offers robust resources to train financial aid administrators in compliance management. Key compliance activities include:

- **Verification**: Schools must verify the identity and eligibility of FAFSA applicants flagged by the Department of Education through specific verification groups (V4 or V5) before disbursing funds. This is handled through the financial aid office. The Department is implementing new identity validation processes to combat fraud rings.
- **Internal Controls and Audits**: Institutions must conduct annual independent compliance audits of their administration of Title IV programs. Ongoing internal monitoring and data reconciliation across admissions, course registration, and financial aid systems help flag anomalies, such as "ghost students" who receive aid but never attend classes.
- **Staff Training**: Faculty, financial aid administrators, admissions, registration, extended and online campus operations, continuing education, and other relevant staff should be trained to identify red flags. Consider contacting the Regional Field Office of the Inspector General to arrange institutional or regional training. Coordination through your State or Regional Association may be helpful: https://oig.ed.gov/contact/regional-offices
- **Policies and Procedures**: Schools should establish clear policies, including disciplinary actions (e.g., expulsion) for learners found to have falsified information with the intent to deceive, and inform learners of the penalties for fraud.
- **Data Security**: Strengthening Identity and Access Management (IAM) systems and requiring multi-factor authentication helps prevent cybercriminals from accessing institutional systems and learner accounts.

Reporting Suspected Fraud

Institutions must refer credible information about potential fraud or criminal misconduct related to Title IV programs by an applicant, learner, or third-party servicer to the U.S. Department of Education's Office of Inspector General (OIG). The mechanisms for reporting potential fraud are intended to be used by financial aid administrators, so any such reporting should be led and/or coordinated by your financial aid office. It is also recommended that institutions consult with legal counsel before making an external referral. There are two mechanisms to report fraud:

- **OIG Hotline Portal**: Suspected fraud rings require submitting complaints and supporting documents via the OIG's encrypted web portal at https://oighotlineportal.ed.gov
- **OIG Hotline Phone**: Individual cases can be reported by calling the OIG hotline at 1-800-MISUSED (1-800-647-8733)

Systemic Evolution for Fraud Prevention

AACRAO is deeply engaged in state, national, and global conversations to evolve the records ecosystem toward a digital, learner-sovereign, and verifiable landscape. The transcript is an integral part of that evolution, digitally stored in the Learning and Employment Record (LER). LERs can combat fraud in education by creating verifiable, tamper-evident digital credentials that individuals control. They address identity management issues by providing a standardized, machine-readable format for documenting skills, education, and work history from multiple sources, trusted by employers and other institutions.

In June of 2025, The Department of Education announced **Significant Actions to Prevent Fraud through Identity Verification**, which includes a new Federal Student Aid (FSA) identity confirmation process launched Fall 2025, higher verification rates, changes to identity confirmation requirements, and updated steps to take when fraud is detected. These updates are needed and important, but do not solve for the root of the problem.

Multiple features of LERs directly address the issues of identity management and fraud:

- **Verifiable credentials**: LERs are digitally signed and encrypted by the issuing party, making them verifiable and difficult to alter or forge.
- **Decentralized control**: Individuals, rather than institutions, can control their LERs, which are often stored in personal digital wallets. This gives them agency over their data while ensuring it can be shared with the necessary parties, such as employers.
- **Standardized data**: LERs use open standards, enabling different systems (like HR and credentialing platforms) to share and interpret information accurately and automatically, reducing the risk of manual entry errors and fraud.
- **Comprehensive records**: LERs document a person's entire learning and work history, including formal education, informal training, and on-the-job experience. This provides a more complete and trustworthy picture than traditional paper-based documents or simple degrees alone.
- **Skills-based matching**: LERs can be used to create skills-based profiles that focus on what an individual knows and can do, rather than just degrees. This not only helps match people to jobs more equitably but also provides another way to verify that the person sharing the record is the actual owner.

In the United States, AACRAO is working with institutions and states to develop and deploy LERs. Globally, we were among the founding organizations of the Groningen Declaration Network, which is working to enable the ecosystem. We believe that if educational institutions, employers, and training providers issue verifiable, machine-readable digital credentials, it will not only empower individuals to succeed but also reduce incidents of fraud. To learn more about AACRAO's work advancing the institutional adoption of LERs, visit our website at www.aacrao.org.

Future Outlook

Fraudsters continually evolve, adapting faster than institutional systems. While the concentration of activity has been in the community college sector, there are growing reports of activity in the readmission and non-credit populations at four-year institutions. Balanced strategies are essential to protect both institutional integrity and learner access. Combating these bad actors will require sustained investment, inter-institutional collaboration, and federal guidance. AACRAO will continue to monitor the situation and work with institutions, educational and/or identity technology solutions, and federal authorities to advocate for comprehensive, cost-effective solutions to this growing issue.

Acknowledgments

- Prepared in consultation with:
  - Cassandra Moore, Director, Enrollment Development & Admissions, Anne Arundel Community College
  - Dr. Carrie Jeffers, Vice President, Student Services, Macomb Community College
  - Karen Chico Hurst, Director of Risk Management and Compliance, the State University of New York (SUNY)
  - Melanie Gottlieb, Executive Director, AACRAO
  - Dr. Ryan E. Meador, Registrar, Metropolitan Community College
  - Jaclyn Birks, Director of Admissions, Jefferson College
  - Scott Fiedler, College Registrar, Ozarks Technical Community College
  - Dr. Monty Hickman, Executive Director of Strategic Enrollment Management, NCCC
  - Steven Reeves, AVP, Chief Information Security Officer, NCCC
  - Rachael Achivare Hill, Director, Admission & Prospective Student Services, Tulsa Community College
- Reviewers:
  - Devin Andrews, University of Phoenix
  - Michelle J Smith, CAE, Executive Director, URMIA
  - Tim Amyx, Volunteer State Community College

For More Information

AACRAO American Association of Collegiate Registrars and Admissions Officers One Dupont Circle NW, Suite 520 Washington, DC 20036

Website: www.aacrao.org

Publication Date: January 2026

APPENDICES

Implementation Guidance and Resources

Appendix A: Getting Started — Building Your Fraud Prevention Framework

For institutions formalizing their fraud prevention efforts, the following sequence provides a practical roadmap:

1. **Assess Current State:** Survey existing practices across admissions, financial aid, registrar, and IT. Identify what verification steps are already in place, even if informal. Document recent incidents and how they were handled.

2. **Convene a Cross-Functional Team**: Establish an identity-verification working group (see Appendix B for composition). Even a small initial group can begin standardizing response protocols.

3. **Develop Written Procedures**: Document your fraud identification and response workflow (see Appendix E). Ensure staff know who to contact and what steps to follow when they suspect fraud.

4. **Train Frontline Staff**: Use the checklists in Appendix F to train admissions counselors, financial aid staff, and registration personnel on red flags. Schedule refresher training at least annually.

5. **Implement Quick Wins**: Many improvements require no new technology—cross-referencing addresses against public databases, verifying phone numbers are active, and checking email domains can be done manually.

6. **Evaluate Technology Needs**: Once manual processes are established, assess whether volume or complexity warrants technology investment. Use the evaluation criteria in Appendix D to guide vendor conversations.

7. **Establish Review Cycles**: Schedule quarterly reviews of fraud incidents and near-misses. Adjust procedures based on emerging patterns. Fraudsters adapt quickly; your practices must evolve accordingly.

Appendix B: Structuring Your Fraud Response Team

Effective fraud prevention requires collaboration across administrative silos. Institutions that have successfully addressed application fraud typically establish a standing cross-functional team with the following characteristics:

Recommended Team Composition

- **Financial Aid** (often serves as team lead given Title IV compliance responsibilities)

- **Admissions/Enrollment Services** (first point of contact for applications)
- **Registrar/Records** (credential evaluation and enrollment management)
- **Information Technology/Security** (system access, data security, technical detection)
- **Campus Security/Police** (when criminal referral may be warranted)
- **Legal Counsel** (consulted as needed for external referrals and policy review) **Online/**
- **Extended Campus** (if applicable—online programs often face higher volumes)
- **Faculty Governance Representation**

Operational Structure

- **Meeting Cadence**: Monthly during normal periods; weekly or as-needed during peak application cycles or active fraud incidents
- **Reporting Line**: Typically reports to VP of Enrollment Management, VP of Student Affairs, or Chief Financial Officer depending on institutional structure
- **Decision Authority**: The team should have clear authority to place verification holds and make enrollment decisions on flagged applications without requiring escalation for each case
- **Documentation**: Maintain case logs with sufficient detail to support OIG referrals if needed, but protect from public disclosure (see "Protecting Investigative Data" in Appendix D)

Appendix C: Resource Considerations

Fraud prevention investments vary significantly based on institutional size, application volume, and current infrastructure. The following framework can help structure budget conversations:

Low-Cost/No-Cost Approaches

- Cross-departmental coordination (reorganization of existing staff time)
- Manual verification using free public databases and search tools
- Staff training using resources from AACRAO, NASFAA, and OIG
- Written procedures and workflow documentation
- Peer institution information sharing through professional networks

Moderate Investment

- Dedicated staff time for fraud review (partial FTE or reassigned duties)
- Subscription to commercial identity verification databases
- Enhanced document imaging and review tools
- Consultant engagement for initial assessment and procedure development

Significant Investment

- AI-powered fraud detection software (typically priced per application or as annual subscription)
- Integration with third-party identity verification services
- Dedicated fraud prevention position(s)
- Custom SIS modifications for automated flagging and holds

Cost-Benefit Note: When building a business case, weigh technology costs against financial risk (potential liability for Title IV repayment), operational risk (staff time spent on manual review), and reputational risk. Institutions that have experienced significant fraud often find that prevention investments are substantially less than remediation costs.

Appendix D: Recommendations When Evaluating Technology Solutions

While technical solutions can improve efficiency, they are prone to false positives and still require human oversight. Manual review remains critical, especially for applicants with limited data footprints.

Evaluation Criteria

1. **Define Operational Goals**: Technical solutions should enhance efficiency without replacing human verification. Human verification enables institutions to respond to the realities of diverse learner populations without compromising access.

2. **Minimum Functional Capabilities**: Solutions should, at a minimum, cross-check data, detect document alterations, and identify behavioral anomalies. Solutions that verify identity at the point of application offer the best (though not foolproof) protection against fraud.

3. **Holistic Implementation**: No single administrative unit should implement a technical solution. A successful implementation requires significant collaboration across departments. Some institutions have developed interdepartmental identity verification and document verification teams to plan implementation, monitor progress and performance, and maintain evidence integrity.

4. **Data Handling and Encryption**: Institutions should ask how the vendor handles customer data during identity verification and which encryption methods are used.

5. **Data Hosting and Residency**: Policies on data hosting, data residency, and storage must be clearly understood to ensure the institution complies with state, national, and international privacy regulations.

6. **Information Security Vetting**: Institutions should request an information security policy or a Higher Education Cloud Vendor Assessment Tool (HECVAT) report from the technology vendor.

7. **Access Control**: The software must manage access control and user roles to ensure sensitive information is accessible only to authorized personnel.

8. **Verify Regulatory Compliance**: Ensure compliance with applicable regulations, including the Family Educational Rights and Privacy Act (FERPA) and relevant state privacy laws. Vendors can request (for a fee) a FERPA compliance review from AACRAO for an added layer of confidence.

Security Concerns with Identity Verification

A recurring security concern is verifying sensitive identifiers such as Social Security Numbers (SSNs). Some institutions have disabled SSN verification through their identity verification software due to serious data security issues. While SSN verification allows the software to cross-reference identity components (Name, DOB) against external databases (like credit bureaus), some colleges have opted not to use it due to these concerns.

Protecting Legitimate Learners and Institutional Data

- **Protecting Investigative Data**: Institutions are strongly encouraged to exercise caution when sharing online or in any discoverable manner information about document fraud detection or identity management tactics, as perpetrators quickly adapt their strategies. Identity data gathered during mitigation efforts must be protected from public disclosure to the fullest extent permitted by law, given ongoing investigations and the potential for further harm to systems.

- **Using "Identity Verification" Terminology**: When contacting learners about a flagged application, institutions should avoid using the word "fraudulent." Instead, use the term "identity verification" to avoid falsely accusing legitimate learners.

Avoiding False Positives: Human checks remain critical to ensure technology does not inadvertently block legitimate learners, especially since real applicants can be flagged if their information (such as living in temporary housing or being a minor) complicates data verification.

Appendix E: Fraud Response Workflow

When fraud is suspected or detected, institutions need clear procedures for response. The following workflow provides a framework that institutions can adapt to their specific context and governance structures.

Step 1: Initial Detection and Documentation

- Staff member identifies potential fraud indicators (see Appendix F checklists)
- Document all observations with screenshots, timestamps, and specific data points
- Do not contact the applicant/learner at this stage
- Notify the designated fraud response team contact immediately

Step 2: Verification and Investigation

- Fraud response team reviews documentation and conducts additional verification
- Cross-reference data across institutional systems (SIS, LMS, financial aid)
- Check external databases and public records as appropriate
- Determine if this appears to be an isolated case or part of a pattern/ring
- Document findings in a secure case file

Step 3: Immediate Protective Actions

- **Place an administrative hold** on the account to prevent registration, transcript release, and financial aid disbursement
- **If already enrolled**: Coordinate with financial aid to halt any pending disbursements
- If aid has already been disbursed: Document the amount and date; consult with financial aid on recovery procedures and reporting requirements
- **Secure digital access**: IT disables institutional email, LMS access, and any other system credentials

Step 4: Identity Verification Outreach (If Warranted)

In some cases, the individual may be a legitimate learner whose identity was compromised or whose information triggered a false positive. Before taking final action:

- Contact the individual using "identity verification" language (not "fraud")
- Request documentation to verify identity (government-issued ID, in-person verification, etc.)
- Set a reasonable deadline for response (typically 5-10 business days)
- Document all outreach attempts and responses

Step 5: Final Determination and Action

If fraud is confirmed:

- Withdraw/cancel enrollment per institutional policy
- Apply a permanent "Fraudulent Account" service indicator to prevent future enrollment
- Reverse any grades or credits awarded
- Process financial aid return/repayment as required

If identity is verified as legitimate:

- Remove holds and restore access
- Document verification in the file
- Consider whether the learner's identity may have been stolen elsewhere and offer resources if appropriate

Step 6: External Reporting

- Financial aid fraud: Financial aid office coordinates referral to OIG (see Reporting Suspected Fraud section in main brief)
- Credential Fraud: Notify issuing institutions if forged credentials were submitted
- Identity Fraud: Notify the National Student Loan Data System (NSLDS) and/or National Student Clearinghouse (NSC)
- Criminal activity: Consult with campus security and legal counsel regarding law enforcement referral
- Pattern/ring activity: Consider notifying peer institutions and state/regional associations (protect specific case details)
- Vendor notification: Alert application platforms, credentialing services, or transcript vendors if their systems were exploited

Note: A case might fall under multiple of the above categories, necessitating multiple external reports

Step 7: Case Closure and Review

- Complete all case documentation
- Store records securely with appropriate retention
- Include the case in aggregate reporting for fraud response team review
- Identify any process improvements or training needs revealed by this case

Appendix F: Quick-Reference Checklists for Staff Training

The following checklists can be used for staff training and as reference tools. Consider printing these for frontline staff or incorporating them into training materials.

Checklist 1: Spotting Fraudulent Applications

- [ ] Submission patterns: Multiple applications with slightly different names or details from the same IP address or similar email patterns
- [ ] Geographic/technical anomalies: Bulk applications from high-risk geographic locations or using VPNs
- [ ] Age band targeting: Bulk applications within specific age ranges (e.g., 30-40 or 40-50 years old)
- [ ] Data uniformity: Minimal information provided; single unknown parent listed; identical self-reported GPAs; no test scores
- [ ] Address anomalies: Commercial properties, vacant lots, one-bedroom apartments (for family claims), stadiums, or movie theaters listed as home addresses
- [ ] Timing: Applications submitted during holidays, weekends, or unusual hours in high volume

Checklist 2: Spotting Identity Fraud

- [ ] Mismatched personal information: Inconsistent data points (name, SSN, DOB) or repeated requests to change these identifiers
- [ ] Stolen identity indicators: Use of identities belonging to deceased individuals, persons with justice system involvement, or formerly enrolled learners
- [ ] Legitimate transcript, fraudulent applicant: Real transcripts received through verified sources, but the applicant is not the person named on the transcript
- [ ] Human contact does not remove suspicion: Fraudsters increasingly use actual people in call centers to submit applications and complete initial assignments
- [ ] Document forgery: AI-generated or altered documents (fake transcripts, diplomas, passports, driver's licenses)
- [ ] Virtual meeting anomalies: Blur effects, video distortion, and color breaks during video verification may indicate AI filters
- [ ] Verification resistance: Unusual urgency about financial aid, resistance to providing documentation, and unprofessional communication

Checklist 3: Spotting Academic Credential Fraud

- [ ] Fabricated records: Fake transcripts or certificates from unaccredited or non-existent institutions; manipulated grades/test scores; fraudulent GEDs; degrees from diploma mills
- [ ] Document irregularities: Mismatched fonts, inconsistent formatting, unusual paper quality, missing security features
- [ ] Credential request patterns: Repeated requests for credentials (especially transcripts) for different individuals sent to the same third-party address
- [ ] Digital address red flags: Requests for digital credentials to be sent to free email domains (e.g., admissions@institution.gmail) instead of institutional domains
- [ ] Source verification: Always verify that transcript sources are legitimate before adding to approved third-party source lists
- [ ] Legitimate Vendor, Fraudulent documents: Use of a legitimate mailing house to send fraudulent documents

Checklist 4: Spotting Financial Aid and Payment Fraud

- [ ] Aid misrepresentation: False claims about dependency status, household income, or family structure to inflate financial aid eligibility
- [ ] Residency manipulation: False claims of state residency to qualify for in-state tuition; local addresses listed solely to qualify for fee waivers
- [ ] Disbursement schemes: Enrollment and minimal participation only until aid is disbursed, then disappearance; cashing disbursement checks without completing coursework
- [ ] Payment anomalies: Multiple failed credit card payment attempts followed by additional card attempts; payments

- [ ] Refund manipulation: Enrollment with a stolen payment method, withdrawal before the drop deadline, request for a refund to a personal bank account

Remember: If you observe any of these indicators, document your observations and notify your designated fraud response contact immediately. Do not confront the applicant or learner directly.