Fraudulent Student Account Procedures and Guidelines

These procedures and guidelines govern the prevention, detection, investigation, and resolution of suspected and confirmed fraudulent student accounts and identity theft at Western Michigan University (WMU). They apply to all university staff, administrators, and offices involved in maintaining the integrity of admissions, enrollment, financial aid, student accounts, and student records.

WMU is committed to:

- Screening the application document; enrollment integrity prior to matriculation; reporting red flags.
- Protecting the integrity of all student financial aid programs administered under Title IV of the Higher Education Act (HEA) and applicable federal regulations.
- Safeguarding the personal information of legitimate students, applicants, and the public.
- Complying with requirements established by the U.S. Department of Education (ED), the Federal Student Aid (FSA) office, the Federal Trade Commission (FTC), and applicable state law.
- Cooperating fully with law enforcement and regulatory agencies when fraud is detected or confirmed.

These procedures apply whenever apply whenever any employee has reason to believe that a student account may have been created using a false or stolen identity, whether such indicators are identified at the time of application, at enrollment, or at any point thereafter during the student's enrollment, or when any person reports to the university that their identity has been used without their consent.

Roles and Responsibilities

The following offices share responsibility for fraud prevention, detection, and response. Each office's specific responsibilities during active investigations are detailed in later sections.

Office	Primary Fraud-Related Responsibilities
Student Financial Aid and Scholarships (SFAS)	Review and investigation of suspected fraud affecting eligibility for, receipt of, or administration of Title IV federal student aid, including FAFSA/ISIR information, conflicting information, identity validation, federal reporting, and OIG referrals.
Director of Internal Audit	Receives all Fraud Incident Reports; coordinates cross-departmental investigations; maintains case files; issues Investigation Outcome Reports.
Admissions	Front-end identity screening; application document verification; admission fraud detection; enrollment integrity prior to matriculation; reporting application-stage red flags.
Office of the Registrar	Enrollment monitoring; academic holds; SIS fraud notations; NSC reporting and corrections, supporting NSLDS; records retention.
Information Technology (OIT)	Credential management; system access suspension; IP/device forensics; cybersecurity monitoring; data integrity controls.
Accounts Receivable	Refund holds; fund recovery coordination; bank account records.

Office of General Counsel	Legal and regulatory guidance; FERPA counsel; law enforcement coordination; disclosure decisions.
Campus Public Safety	Criminal referrals, law enforcement liaison, on-campus identity verification (if applicable).
Faculty / Academic Departments	No-show and non-participation reporting; engagement confirmation upon request.
All Staff	Prompt reporting of fraud indicators; confidentiality maintenance.

Proactive Prevention and Departmental Controls

The university shall maintain the following preventative controls across all relevant offices to minimize the risk of fraudulent accounts being established. Each department is responsible for implementing, documenting, and annually reviewing its assigned controls. Department heads must designate a specific staff member as the point of contact for fraud prevention activities within their office.

Admissions

The Office of Admissions* serves as the institution's first line of defense against fraudulent applications. The procedures below outline our current framework for detecting, escalating, and responding to application-stage fraud.

1. **Document Verification Procedures**

   Upon receipt of application materials, admissions staff conduct a baseline review of all submitted documents for internal consistency and authenticity indicators. This includes verifying that formatting, fonts, institutional seals, and signatures on transcripts and supporting documents are consistent with known authentic samples. Documents that appear altered, inconsistent, or implausible are flagged for secondary review before an admissions decision is rendered. All flagged materials are retained in the applicant's file regardless of outcome.

2. **Identity Check Requirements at Application**

   Applicants are required to attest to the accuracy of all submitted information as a condition of application submission. Photo identification may be requested during the enrollment process to confirm that the individual who applied matches the individual enrolling. For populations where identity verification is particularly critical (such as international applicants or those enrolling in fully online programs) additional identity confirmation steps may be initiated prior to or at the point of admission.

3. **Transcript and Diploma Authentication**

   Official transcripts must be submitted directly from the issuing institution or through an approved secure electronic delivery service (e.g., Parchment, National Student Clearinghouse). Paper transcripts submitted in sealed, signed envelopes from the institution are accepted when electronic delivery is unavailable. Faxed or emailed transcripts will not be considered official. Admissions staff are trained to recognize common indicators of transcript manipulation, including irregular GPA progressions, course sequencing anomalies, and formatting inconsistencies. Diplomas submitted as standalone proof of degree completion without accompanying transcripts are not accepted as sufficient documentation.

4. **Use of Third-Party Verification Services**

   The Office of Admissions utilizes third-party services to support authentication of credentials that cannot be verified through direct institutional contact. For international credentials, [check with international on specific vendor] evaluations are required for applicants from select countries or when the authenticity of foreign transcripts cannot be confirmed. The National Student Clearinghouse is used to verify prior enrollment history where applicable. Engagement of additional verification services is at the discretion of the Director of Admissions or designee when circumstances warrant.

5. **Internal Reporting**

   The Office of Admissions routinely conducts an internal reporting process, designed to identify potential fraudulent applications/documents. This reporting uses known and common fraud indicators (e.g., multiple students with the same address and/or date of birth, sequencing in email addresses, disproportionate applications to online programs, etc.) to detect possible fraud. As technology advances, so will internal reporting.

6. **Internal Watchlists and Flagging Mechanisms**

   The Office of Admissions maintains an internal record of prior applicants whose files were closed, rescinded, or referred due to confirmed or suspected fraud. This list is reviewed as part of the reapplication screening process. Additionally, staff are trained to cross-reference applicant information, including names, addresses, email domains, and prior institutions against previous flagged files. Coordination with the Registrar's Office occurs when fraud is identified post-enrollment to ensure consistency in institutional recordkeeping.

7. **Escalation of Application-Stage Red Flags**

   When admissions staff identify potential fraud indicators, the following escalation process applies:

   - Level 1 – Staff Review: The reviewing staff member documents the concern and brings it to the Associate Director of Admissions, Operations for a secondary review.
   - Level 2 – Director Involvement: If the concern cannot be resolved through additional documentation, the Director of Admissions is notified, and the application is placed on hold pending review.
   - Level 3 – Cross-Departmental Referral: Cases involving suspected identity fraud, falsified credentials, or patterns suggesting organized fraud are referred to the Internal Audit, General Counsel, and/or Campus Public Safety as appropriate.

   All escalated cases are documented in the applicant's file, and outcomes — including any decision to deny, rescind, or refer — are recorded for institutional reporting purposes.

***Note:** It is recognized that there are multiple offices that oversee and manage admissions processes. For the purpose of this document, the "Office of Admissions" is used as a general descriptor of any office that oversees and admission application/process. Depending on the student population, one of three offices would be involved: the Office of Admissions (domestic, undergraduate) the Haenicke Institute for Global Education (international, undergraduate and graduate), and the Graduate College (domestic, graduate).*

Office of Student Financial Aid and Scholarships

Ellucian Banner and Student Financial Success serve as the university's systems of record for Title IV federal student aid and incorporate automated edits, workflows, exception messages, and other controls designed to identify potential eligibility issues and support accurate and compliant aid administration. The Office of Student Financial Aid and Scholarships reviews and addresses system-generated exceptions in accordance with applicable federal requirements and university procedures.

1. **FAFSA/ISIR Review**

   The Office of Student Financial Aid and Scholarships reviews Institutional Student Information Records (ISIRs) and supporting federal data received through Banner to determine eligibility for Title IV federal student aid. Staff evaluate FAFSA information, federal processing flags, eligibility indicators, and other information received from the U.S. Department of Education for completeness, consistency, and potential indicators of fraud or abuse. ISIRs containing conflicting information, federal warning flags, or unusual eligibility conditions are reviewed and resolved before Title IV aid is awarded or disbursed, as required by federal regulations.

2. **Review of Required Documentation**

   When additional documentation is required to establish Title IV eligibility, the Office of Student Financial Aid and Scholarships reviews submitted records for authenticity, completeness, and consistency with information reported on the FAFSA and other institutional records. Documentation may include, but is

not limited to, identity documentation, citizenship or eligible noncitizen documentation, tax or income information, verification documents, or other records required to establish Title IV eligibility. Documents that appear altered, inconsistent, incomplete, or otherwise suspicious are referred for additional review before eligibility is determined.

3. **Identity Validation**

   The Office of Student Financial Aid and Scholarships reviews identity validation results and related federal indicators received through the FAFSA processing system. When federal identity validation requirements indicate additional review is necessary, students are notified of required documentation and identity concerns are resolved in accordance with U.S. Department of Education guidance before Title IV eligibility is finalized. Cases involving suspected identity theft, identity fraud, or fraudulent use of federal student aid are escalated in accordance with university procedures and applicable federal requirements.

4. **Resolution of Conflicting Information**

   The Office of Student Financial Aid and Scholarships identifies and resolves conflicting information that may affect a student's Title IV eligibility. When discrepancies between FAFSA data, institutional records, or supporting documentation, additional information may be requested from the student or appropriate third parties. Eligibility determinations are not finalized until conflicting information has been resolved and documented in accordance with federal regulations. Title IV processing, awarding, or disbursement may be withheld when suspected fraud, conflicting information, or other unresolved eligibility concerns require further review.

5. **Internal Fraud Monitoring**

   Title IV fraud is subject to specific federal statutory and regulatory requirements, suspected fraud will be evaluated, documented, escalated, and resolved in accordance with applicable federal statutes, regulations, U.S. Department of Education guidance, and university procedures.

   Title IV Federal Authorities:

Authority	Relevance
34 C.F.R. § 668.16(e)	Institutional standards of administrative capability — requires institutions to have procedures to safeguard Title IV funds.
34 C.F.R. § 668.71–.75	Fraud and misrepresentation prohibitions; reporting obligations to the Department of Education.
34 C.F.R. § 668.22	Return of Title IV funds (R2T4) — may apply when a fraudulent student withdraws or is removed.
FSA Handbook, Vol. 1, Ch. 5	Application and Verification Guide — identity verification, fraud referrals, OIG reporting, fraud rings.
FERPA (20 U.S.C. § 1232g)	Governs disclosure of student educational records; limits what may be shared with third parties including identity theft claimants.
FTC Red Flags Rule (16 C.F.R. § 681)	Requires institutions with covered accounts to implement an Identity Theft Prevention Program.
FSA Handbook, Vol. 4, Ch. 3	Treatment of overpayments — required when Title IV funds have been disbursed to a fraudulent account.

   The Office of Student Financial Aid and Scholarships routinely monitors for patterns or indicators that may suggest fraudulent attempts to obtain Title IV federal student aid. Monitoring may include, but is not limited to, federal processing flags, conflicting information trends, repeated use of common

identifying information, unusual documentation patterns, reports generated through institutional systems, or other indicators identified through routine processing.

6. **Escalation of Suspected Title IV Fraud**

When Student Financial Aid and Scholarships staff identify information suggesting possible fraud affecting Title IV federal student aid, the following escalation process applies:

- Level 1 – Staff Review: The reviewing financial aid administrator documents the concern, obtains additional information as appropriate, and refers the file for supervisory review.
- Level 2 – Management Review: The supervisor or designated manager evaluates the documentation, determines whether additional information is required, and decides whether the concern can be resolved through routine Title IV eligibility review.
- Level 3 – Compliance Determination: The Associate Director of Compliance reviews cases that cannot be resolved through routine Title IV eligibility review, evaluates the documentation and applicable federal requirements, determines whether additional compliance review or corrective action is necessary, and recommends escalation to the Senior Associate Director and Director of Student Financial Aid and Scholarships when appropriate.
- Level 4 – Director Review: Cases involving suspected Title IV fraud, identity theft, falsified documentation, or other significant Title IV compliance concerns are referred to the Director of Student Financial Aid and Scholarships (or Sr. Associate Director) for further review and determination.
- Level 5 – Institutional and Federal Referral: When appropriate, Title IV cases may be referred to Internal Audit, General Counsel, Campus Public Safety, the U.S. Department of Education Office of Inspector General (OIG), or other appropriate offices or agencies in accordance with applicable federal regulations and university procedures.

🔒 **CONFIDENTIALITY NOTICE – All Staff**

All fraud investigations are strictly confidential. Suspected fraud must not be disclosed to the subject of the investigation, other students, or unauthorized personnel at any stage. Disclosure may compromise the investigation and expose the university to legal liability.

Detection, Reporting, and Investigation Procedures

The following steps govern all suspected fraud cases regardless of the type or how they are detected, by staff observation, system alert, or external report.

Step 1: Initial Detection and Employee Reporting

Any employee who observes or suspects that a student account may be fraudulent must take the following actions within one (1) business day:

- Complete the Fraud Incident Report Form (Appendix A) and submit to the Director of Internal Audit. Document the specific indicators observed, including the date, time, system or process involved, and the nature of the concern. Be as specific as possible.
- Preserve all relevant evidence. Do not alter, delete, move, or forward outside secure university systems any records, logs, system screenshots, emails, or communications related to the suspected account.
- Do not contact the suspected fraudulent account holder under any circumstances.
- Do not disclose the concern to anyone outside the authorized investigation team (see Step 2.1 for authorized personnel).

If a claimant contacts WMU to report that their identity was used without their consent to create a student account, apply for financial aid, or receive any institutional benefit the staff member receiving the initial contact must:

1. Remain calm and professional. Do not disclose whether a matching account exists in university systems. Do not confirm or deny specific account details. If pressed by claimant, staff may say: "We are not able to confirm or deny account information, but we take all identity theft reports seriously and will investigate promptly."
2. Collect the following information from the claimant:
    - Full legal name
    - Valid email as the Director of Internal Audit will send the individual a OneDrive link to securely upload required documents to review .
    - Best callback number
    - Description of how the claimant became aware of the potential fraud (e.g., credit report, IRS notice, SSA letter, loan servicer contact, NSLDS inquiry)
3. Advise the claimant that they will need to submit the following documents through a secure OneDrive link that will be sent from the Director of Internal Audit to formally initiate their claim with WMU:
    - Completed the Identity Theft Claimant Intake Form (Appendix B)
    - Copy of a valid, unexpired, government-issued photo ID (driver's license, state ID, or passport)
    - FTC Identity Theft Report (obtained at IdentityTheft.gov)
    - File a police report with local law enforcement; can request WMU Campus Public Safety's assistance in doing so.
    - Additionally, you may provide the claimant with the following protective steps for personal use:
        - Place a fraud alert or credit freeze with all three major credit bureaus (Equifax, Experian, TransUnion).
        - Contact FSA's Federal Student Aid Information Center (1-800-433-3243) to report misuse of their FSA ID, when the individual is a current or prospective Title IV applicant.
        - Contact the Social Security Administration (1-800-772-1213) if their SSN has been compromised.
        - Review their credit report at AnnualCreditReport.com.
4. Explain the university's process. Do not make specific promises about outcomes or confidential account information.
5. Submit the completed Fraud Incident Report Form (Appendix A) to the Director of Internal Audit within one (1) business day.

> ⚠ **FERPA Notice — Required for All Claimant Contacts**
>
> Under FERPA (20 U.S.C. § 1232g), the university may not disclose the records of a student account, even a potentially fraudulent one, to a third party without a lawful basis. When a claimant asserts that an account was created using their identity without authorization, General Counsel must be consulted before any specific account details are disclosed to the claimant. An FTC Identity Theft Report and a police report may support disclosure under applicable FERPA exceptions, but this determination must be made by General Counsel on a case-by-case basis.

Step 2: Notification and Case Initialization

Upon receipt of a Fraud Incident Report, the Director of Internal Audit must, within one (1) business day:

1. When applicable, email the individual a secure OneDrive link to upload the required documentation needed to initiate an identity theft claim.

2. Send an encrypted email to the following office representatives whom are part of the investigation team:
    a. Admissions
    b. Student Financial Aid and Scholarships
    c. Office of the Registrar
    d. Accounts Receivable
    e. OIT Security and Privacy Officer
    f. CC: Controller, General Counsel, Risk Management, Director of Public Safety, Security and Privacy Officer

    The notification email must include at minimum:
    1. Student full name and WMU ID (WIN)
    2. Date of birth
    3. Brief description of the reported indicators and source of detection
    4. Relevant Student Information System (SIS) data and any initial evidence
3. Upon notification, each office will review the reported concern within its respective area of responsibility, determine the impact, and take any appropriate interim or investigative actions in accordance with applicable laws, regulations, and university procedures.
4. Instruct Accounts Receivable to immediately place a refund hold on the account pending investigation.
5. When a reported concern originates from a department other than the Office of Student Financial Aid and Scholarships, the Office of Student Financial Aid and Scholarships will determine whether the reported concern involves, or may involve, Title IV federal student aid.
6. Instruct the Registrar to review whether the student is enrolled in current or upcoming terms and to place an academic hold on the account.
7. Create a case file and maintain all investigation records therein.

Step 3: Cross-Departmental Interim Actions During Investigation

While the reporting and impacted department conducts its investigation, all departments must take the following actions and maintain them for the duration of the investigation:

Office of Student Financial Aid and Scholarships

1. If the reported concern does not currently involve Title IV:
    - Place an appropriate Banner alert or processing indicator to ensure the student's Title IV eligibility is reviewed before any possible future awarding or disbursement while the investigation remains active.
2. If the reported concern involves, or may involve, Title IV federal student aid:
    - Suspend the processing, awarding, or disbursement of Title IV federal student aid, as appropriate, until eligibility has been established in accordance with applicable federal regulations and university procedures.
    - Follow all applicable federal requirements while conducting a Title IV compliance review and implementing any required administrative actions.
    - Proceed to Step 4

Accounts Receivable

- Maintain the refund hold on the student account for the duration of the investigation.
- Freeze and/or stop all refunds associated with the account.
- Preserve and make available to the investigation team all bank account records, payment history, and transaction logs associated with the account.

Office of the Registrar

- Maintain the academic hold on the student account for the duration of the investigation.
- Do not process any enrollment changes, grade postings, or transcript requests for the account during the investigation without authorization from Internal Audit.
- Preserve all enrollment records and historical SIS data associated with the account.
- Notify faculty in affected courses (without disclosing the nature of the investigation) that the student's enrollment status is under administrative review, if necessary to confirm attendance/engagement.

Information Technology (OIT)

- Preserve relevant system access logs, login records, IP address history, device fingerprint data, and other records associated with the account, as determined necessary based on the circumstances of the investigation. Avoid purging or archiving records that may be relevant to the investigation.
- Monitor the suspected account for any new login attempts or activity, and report findings as soon as reasonably practical or when circumstances warrant.
- Use discretion when determining whether to suspend or restrict account access. While premature suspension may alert the subject and compromise the investigation, circumstances may warrant immediate action to secure the account.

Faculty and Academic Departments

- If contacted by Internal Audit or the Registrar, provide attendance and academic engagement records for the enrolled student.
- Report any contact or communication received from the student to Internal Audit immediately.
- Do not share information about the investigation with other students or faculty.

All Other Departments

- Refer any contact from or about the student account under investigation to Internal Audit.
- Do not take independent action on the account without authorization from Internal Audit.
- Maintain strict confidentiality.

Step 4: Title IV Investigation (Student Financial Aid and Scholarships)

Student Financial Aid is the institutional lead for all Title IV-related fraud investigations.-Upon receiving the Step 2 notification identifying a potential Title IV impact, the Office of Student Financial Aid and Scholarships will adhere to the following procedures:

4a - Student Identity Verification Attempt

1. Contact the student via all contact information on file in the SIS (phone, email, and postal mail) and request that the student verify their identity.
2. Identity verification must be conducted via one of the following methods:
    a. In-person presentation of an unexpired, government-issued photo ID at a designated university office.
    b. Live video call with a trained staff member, during which the student presents their unexpired, government-issued photo ID to the camera.
3. Document the date, time, method, and outcome of all contact attempts in the Case File.
4. Allow the student a reasonable opportunity to respond (minimum 5 business days for initial contact, unless exigent circumstances require faster action).
5. If the student fails to respond or cannot verify identity within the allotted timeframe, escalate to the Director of Student Financial Aid for authorization to proceed with investigation without verification.

4b - Title IV Financial Aid Record Review

6. Review the student's Title IV financial aid file for inconsistencies, verification flags, or discrepancies.
7. Review the disbursement history including dates and amounts received.

4c - Coordination and Escalation

8. Maintain ongoing communication with the Director of Internal Audit throughout the investigation.
9. Consult with General Counsel on any legal questions arising during the investigation.
10. Complete and submit an Investigation Status Update to Internal Audit every 10 business days until the investigation is closed.
11. Target investigation completion within 30 business days. Extensions require written authorization from the Director of Student Financial Aid and must be documented in the Case File.

4d - Investigation Documentation Requirements

The following must be documented and retained in the Case File:

- All contact attempts and responses (or non-responses) from the student.
- Copies of all identity documents reviewed.
- FAFSA data reviewed.
- All disbursement records associated with the account.
- All communications among the investigation team.
- Timeline of all actions taken.
- Any referrals made to OIG.

Step 5: Outcome Determination

Upon completion of any type of investigation, the Director of Internal Audit and the director(s) responsible for a particular case, must jointly make one of the following determinations.

Outcome	Immediate Action	See Section
Fraud Confirmed	Proceed to Step 5a: Handling Confirmed Fraud	Step 5a
No Fraud Found — Account Legitimate	Lift all holds, restore account, document, notify student. See Step 5b.	Step 5b

Step 5a: Fraud Confirmed

When an investigation concludes that fraud is confirmed, the following actions must be taken in the order listed. All actions must be documented in the Case File.

5a.1 - Immediate Administrative Actions

Complete within two (2) business days of the fraud determination, the Director of Internal Audit will provide formal written notification to the investigation team listed in Step 2.1 and instruct the following to be executed:

- Notify Accounts Receivable to convert or maintain any financial hold as a permanent Fraud Hold and restrict all account access.
- When Title IV federal student aid is involved, notify Student Financial Aid and Scholarships to implement all required Title IV administrative and corrective actions in accordance with Section 5a.2.
- Authorize OIT to suspend or disable all institutional credentials (email, portal login, LMS access) associated with the fraudulent account, in a timely and practical based on the specifics of the case.
- Notify the Registrar and Admissions to revoke admission and enrollment.

5a.2 - Title IV Corrective Actions (Student Financial Aid and Scholarships)

In accordance with Title IV requirements:

- Do not make any further disbursements of Title IV, HEA funds to the student or on the applicant's behalf (per FSA Handbook, Vol. 1, Ch. 5).
- Determine and implement all required Title IV administrative actions based on the findings of the investigation and applicable federal regulations.
- Update the student's Title IV eligibility, awards, and financial aid record to reflect the final determination of the investigation and any required corrective actions.
- Submit required corrections to federal systems as required.
- Determine whether a Title IV overpayment exists, treat any Title IV funds already disbursed as an overpayment, and initiate the overpayment recovery process in accordance with 34 C.F.R. § 668.22 and FSA Handbook, Vol. 4, Ch. 3 (Treatment of Overpayments).
- Perform an R2T4 (Return of Title IV Funds) calculation, where applicable.
- Coordinate with Accounts Receivable, as appropriate, regarding Title IV financial aid adjustments resulting from required Title IV administrative actions.
- Update the student's Banner Title IV financial aid record with the appropriate fraud indicator or administrative alert in accordance with university procedures to ensure future Title IV eligibility is reviewed before any financial aid is awarded or disbursed.
- Participate in any required referral to the U.S. Department of Education Office of Inspector General (OIG), in coordination with Internal Audit and General Counsel, when appropriate.

5a.3 - OIG Referral and Law Enforcement Coordination (General Council)

- If it's suspected that any student, employee, or other individual has misreported information or altered documentation to fraudulently obtain federal funds, report your suspicions and provide all evidence to the ED Office of Inspector General (OIG). Referral contact information is available in the FSA Handbook, Application and Verification Guide, Ch. 5 (Referral of Fraud Cases).
- Coordinate submission of distance education fraud ring complaints through the ED's OIG encrypted complaint portal at oighotlineportal.ed.gov.
- Coordinate with Campus Public Safety regarding any criminal referral to local or federal law enforcement.
- No public statements or media coordination regarding the case may occur without prior consultation with and approval from General Counsel.

5a.4 - Record Management (Admissions, Registrar and Internal Audit)

- Flag the fraudulent student record permanently in the CRM and SIS with a "Fraud Confirmed" notation and the assigned Case Number. This record must never be purged.
- Do not expunge academic records; retain all records in accordance with the university's records retention schedule and applicable law.
- Report enrollment data corrections to NSLDS within 30 days of account closure, as required by 34 C.F.R. § 685.309.
- Retain the complete Case File permanently. Case files must include: the Fraud Incident Report, all investigation records, the Investigation Outcome Report, all communications, fund recovery documentation, OIG referral documentation (if applicable), and all law enforcement coordination records.

5a.5 - Linked Accounts

If the investigation reveals accounts linked to the confirmed fraudulent account through shared SSNs, bank accounts, IP addresses, application data, or other identifiers, each linked account must be individually investigated. Individual SAFs must be placed on each linked account pending those investigations. Findings must be reported to OIG if a fraud ring is suspected.

Step 5b: No Fraud Found — Account Legitimate

When an investigation concludes that the account is legitimate and no fraud has occurred, the following actions must be completed promptly to restore the student's standing:

1. Accounts Receivable must remove all financial/refund holds placed during the investigation.
2. Registrar must remove all academic holds placed during the investigation.
3. Office of Student Financial Aid and Scholarships must resume any suspended Title IV financial aid disbursements and processing after verifying current eligibility.
4. Office of Student Financial Aid and Scholarships must remove any temporary Title IV Banner alerts, holds, or administrative indicators that were placed solely because of the investigation, when appropriate.
5. Office of Student Financial Aid and Scholarships must close the Title IV compliance review.
6. Notify the student that the review has been completed and their account has been restored, if applicable. Consult with General Counsel regarding the appropriate scope and wording of any communication to the student.
7. If a third-party claimant initiated the investigation, notify the claimant of the outcome (consult General Counsel to determine permissible scope of disclosure under FERPA).
8. Document the resolution in the Case File, including the basis for the determination and the date all holds were removed.
9. Retain all Case File documentation in accordance with the university's records retention schedule. Do not purge investigation records even when no fraud is confirmed.

Appendix A — Fraud Incident Report Form

INSTRUCTIONS

Complete this form immediately upon observing fraud indicators. Submit to the Director of Internal Audit within one (1) business day. Do NOT contact the suspected student account holder. Do NOT disclose the concern to unauthorized personnel. Retain a copy for your records.

Reporting Employee Name:	
Title / Department:	
Date of Report:	
Date Indicators First Observed:	
Student Account Name (if known):	
Student WMU ID (WIN):	
SSN (last 4 digits only):	

Detailed Description of Observed Indicators:
Records / Evidence Preserved (list all):

Reporting Employee Signature:

X _____ Date: _____

FOR CLAIMANT USE

This form is used to initiate an identity theft claim with Western Michigan University. Complete all sections and submit along with the supporting documents listed in Section 3 of these procedures. Your information will be kept strictly confidential and used only for the purpose of investigating your claim. Submission of this form does not guarantee a particular outcome.

Section 1 — Claimant Information

Full Legal Name:	
Date of Birth:	
SSN (last 4 digits only):	
Current Mailing Address:	
City / State / ZIP:	
Daytime Phone Number:	
Email Address (secure):	
Preferred Contact Method:	☐ Phone ☐ Email ☐ Mail

Section 2 — Description of Identity Theft

How did you learn that your identity was used? (describe):

Section 3 — Supporting Documents (check all attached)

- ☐ Government-issued photo ID (driver's license, state ID, or passport) (**Required**)
- ☐ FTC Identity Theft Report (IdentityTheft.gov) (**Required**)
- ☐ Law enforcement / police report (**Required**)
- ☐ Credit report showing fraudulent account
- ☐ IRS notice / SSA letter / loan servicer letter
- ☐ Other: _____

Section 4 — Affirmation

By signing below, I affirm under penalty of perjury that I did not authorize any person to use my identity, Social Security Number, or personal information to apply for admission, enroll at, or receive financial aid from Western Michigan University, and that all information I have provided on this form is true and correct to the best of my knowledge.

Claimant Signature: X _____

Date: _____

Printed Name: _____

Return completed form and provide supporting documents via the secure OneDrive link send by the Director of Internal Audit:

Western Michigan University — Director of Internal Audit

Mailing Address: 1903 W. Michigan Ave. Kalamazoo, MI 49008-5222

Secure Email: joan.beffel@wmich.edu

Phone: (269)387-3862