How to Detect and Deter Financial Aid Fraud

Presented by the Office of Inspector General

Investigation Services and Technology Crimes Division

INVESTIGATION SERVICES
OFFICE OF INSPECTOR GENERAL
UNITED STATES DEPARTMENT OF EDUCATION

Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION

PROUD SPONSOR of the AMERICAN MIND™

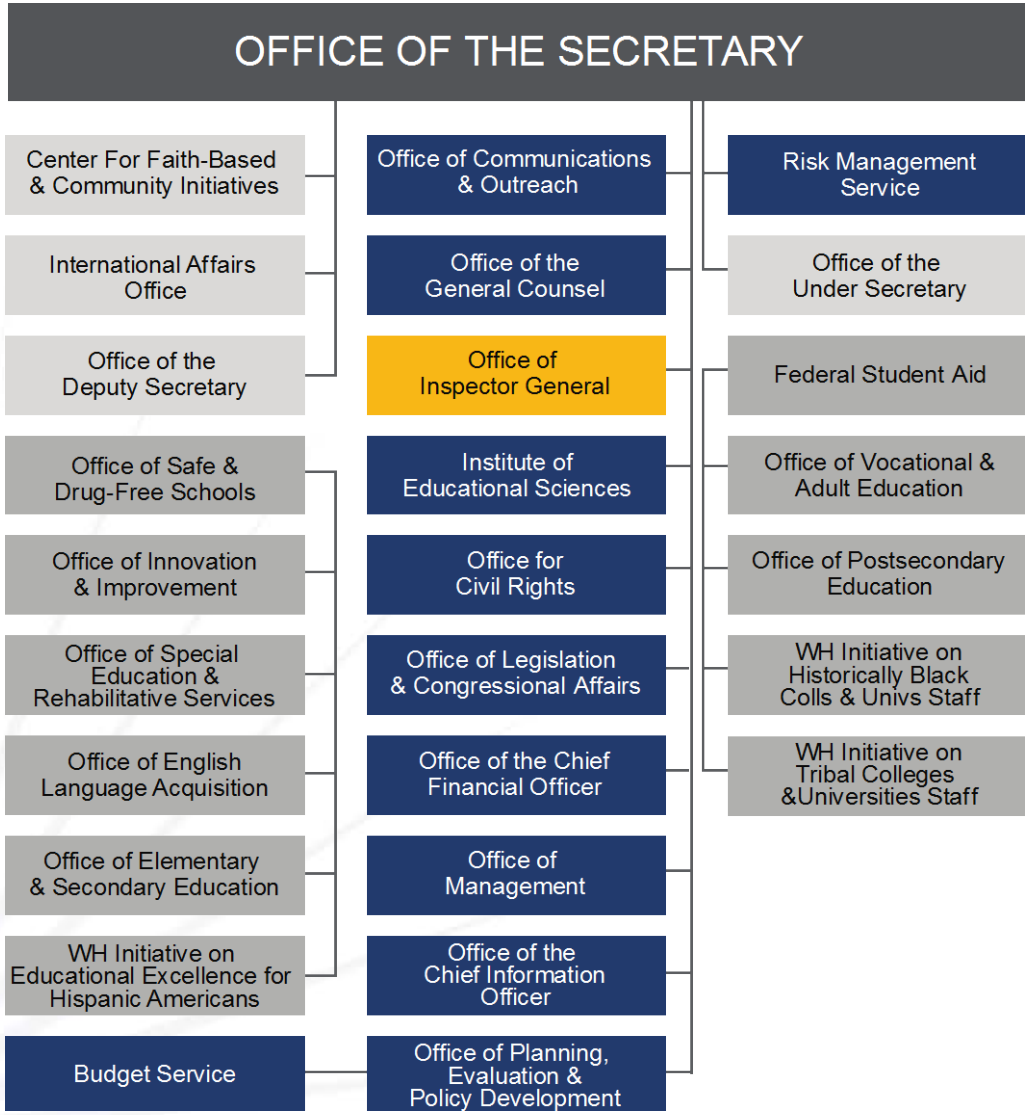
Agenda

- OIG Organization and Mission
- FSA and OIG Coordination
- Sources of Allegations
- Statutory, Regulatory Access to Records
- Standards of Administrative Capability
- Fraud Indicators
- Examples of Title IV Fraud Schemes
- Criminal and Civil Investigations
- Criminal and Civil Remedies
- TCD Structure, Mission, and Investigation
- Ways to Help OIG
- Contact Information

OIG Background

Organizational Chart

The Office of Inspector General (OIG) is part of the Department but…independent. **We examine allegations of waste, fraud, and abuse, and pursue those who seek to enrich themselves at the expense of our nation's students.**



INVESTIGATION SERVICES
OFFICE OF INSPECTOR GENERAL
UNITED STATES DEPARTMENT OF EDUCATION

Inspector General Act of 1978

". . . promote economy, efficiency and effectiveness . . . [and] prevent and detect fraud and abuse . . ." in Department of Education programs and operations

INVESTIGATION SERVICES
OFFICE OF INSPECTOR GENERAL
UNITED STATES DEPARTMENT OF EDUCATION

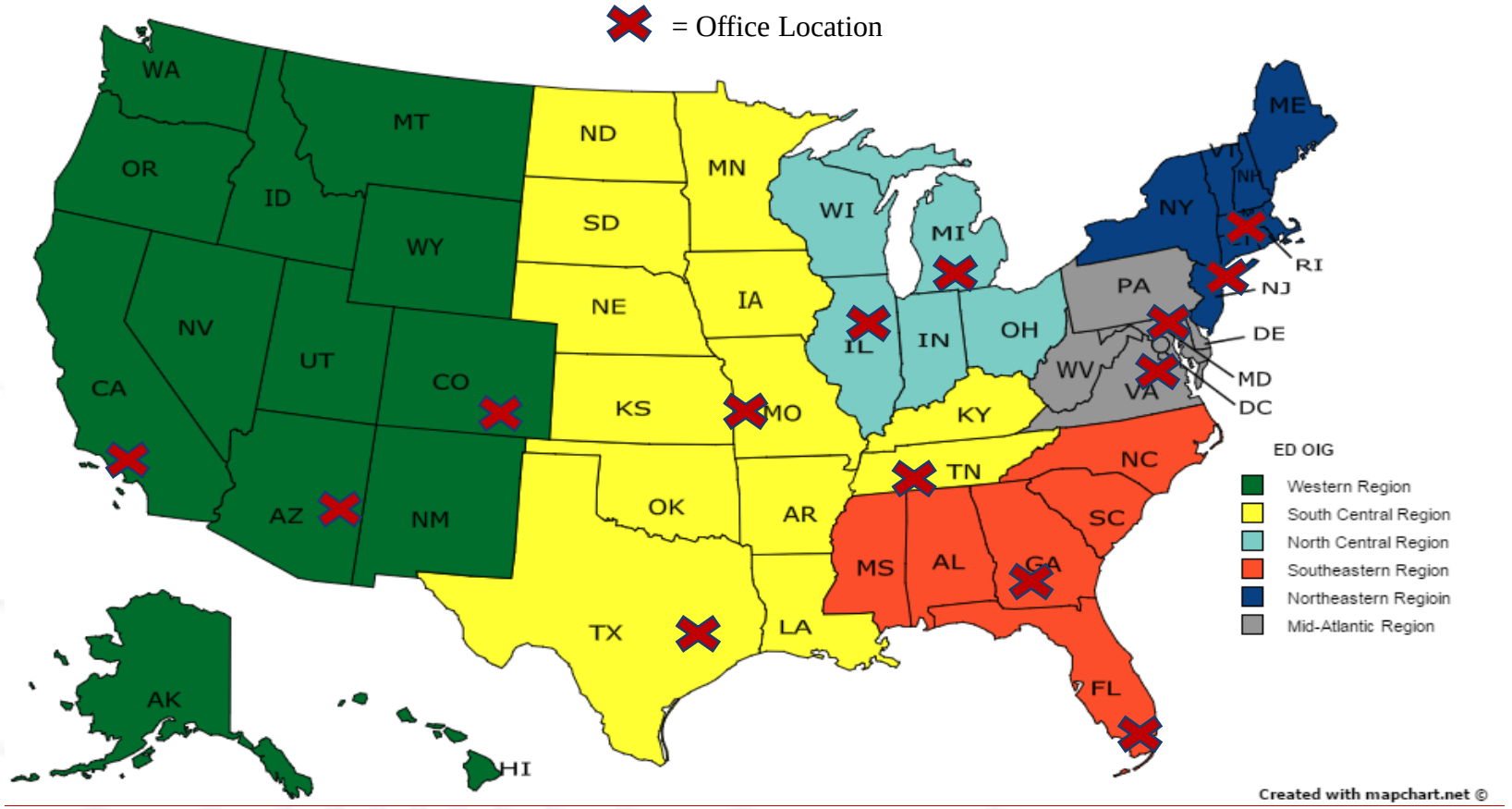
OIG Operational Components

Audit Services

Investigation Services

Information Technology Audits and
Computer Crime Investigations (ITACCI)

Investigation Services Regional Map



INVESTIGATION SERVICES
OFFICE OF INSPECTOR GENERAL
UNITED STATES DEPARTMENT OF EDUCATION

Partnership Between OIG and FSA

FSA and OIG Coordination

OIG assists the Department in promoting the integrity of the Title IV programs.

- Reviews and comments on all regulations with suggestions on areas for improvement
- Regularly exchanges information with FSA to identify current issues in compliance and abuse, and coordinates oversight and investigatory activities, when appropriate
- Issues Management Information Reports to alert the Department about serious fraud and corruption trends

Differences Between OIG's Investigation Services and FSA's Program Compliance and Enforcement Offices

OIG INVESTIGATION SERVICES

- Investigates any **fraud** impacting ED programs or operations
- Works with federal and state prosecutors to take criminal and civil actions
- Criminal investigators have statutory law enforcement authority to carry firearms and execute search and arrest warrants
- Is independent of ED in exercising its investigative authority

FSA (PC AND EO)

- Conducts compliance reviews, administrative investigations of violations of HEA
- Takes administrative actions authorized by the HEA and program regulations
- Reviewers and Investigators have administrative authority only
- Has program operating responsibilities
- Is required to send allegations of fraud to OIG

Why Are You Important to OIG?

You play a critical role

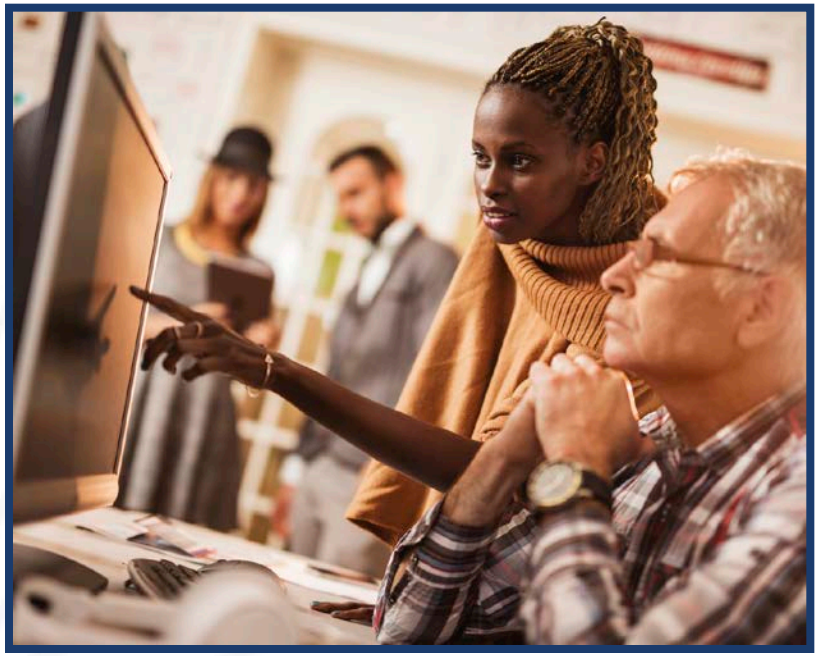
in helping OIG

achieve our mission

You serve as OIG's

"eyes and ears" and help

us detect and prevent fraud



Other Sources of Allegations

- OIG Hotline
- OIG Audits and Inspections
- Department Program Offices
- School Employees and Officials
- Guarantee Agencies
- Contractors and Sub-contractors
- Grantees and Sub-grantees
- Citizens and Students

- Competing Vendors/Schools
- Other Federal Agencies
- U.S. Attorney's Offices
- Other OIG Investigations
- State and Local Law Enforcement Agencies
- Federal Bureau of Investigation
- Qui Tam Actions

Statutory and Regulatory Access to Records

- Under the Inspector General Act of 1978, as amended, OIG can access any records available to the Department of Education to perform audits, investigations and inspections of Department programs and operations.
- The Family Educational Rights and Privacy Act (**FERPA**) requires schools receiving funding from the Department of Education to protect the privacy of student education records. In many cases consent must be received from a parent or student before records can be disclosed.
- **FERPA** also provides that **consent is not required in order to disclose student records to the Office of Inspector General.** The regulations state that representatives of the Secretary, which include OIG, may have access without prior consent in connection with an audit, evaluation, or enforcement of legal requirements related to the Department's programs, or to enforce the terms and conditions of student aid.

Fraud Obligations

Schools must develop and apply "an adequate system to identify and resolve discrepancies in the information that the institution receives from different sources with respect to a student's application for financial aid under Title IV." 34 C.F.R. § 668.16(f).

Schools and their third party servicers must refer to the OIG "**any credible information**" indicating that a student, school employee, third party servicer, or other agent of the school "**may have engaged"** in fraud, criminal or other illegal conduct, misrepresentation, conversion, or breach of fiduciary duty involving Title IV. 34 C.F.R. § § 668.16(g) and 668.25(c)(2).

Fraud Risk Indicators

- One person in control
- No separation of duties
- Lack of internal controls/ignoring controls
- No prior audits
- High turnover of personnel
- Unexplained entries in records
- Unusually large amounts of payments for cash
- Inadequate or missing documentation
- Altered records
- Financial records not reconciled
- Unauthorized transactions
- Related Party transactions
- Repeat audit findings

Examples of Title IV Fraud Schemes Related to Students

- FAFSA Fraud
  - Social Security Number
  - Alien Registration Status
  - Dependency Status
  - Income and Assets
  - Number of Family Members in College
- Falsification of GEDs/HS Diplomas
- Identity Theft
- Distance Fraud Schemes

Examples of Title IV Fraud Schemes Related to Schools

- Ghost students
- Leasing of eligibility
- Default rate fraud
- 90/10 Rule manipulation
- Financial statement falsification
- Falsified last date of attendance
- Obstruction of a federal audit or program review
- Fraud/theft by school employee
- FAFSA fraud - enrollment
- Falsification of GEDs/HS diplomas
- Falsification of attendance and Satisfactory Academic Progress
- Falsification of grades
- Failure to make refunds
- Loan theft/forgeries

Examples of Criminal and Civil Investigations

School Referral to OIG

EMBEZZLEMENT SCHEME

- **Referral:** Referred by Prism Career Institute to the OIG
- **Allegation:** Diane Bowler former Vice President abused her position of trust, diverted over $500,000 by submitting fraudulent reimbursement requests for personal expenses.
- **Investigation:** Special Agents of the FBI Resident Agency and Department of Education OIG led the investigation.
- **Outcome:** Bowler was sentenced to serve 24 months in federal prison

School Referral to OIG

FRAUD RING SCHEME

- **Referral:** Detected by the Rio Salado College and referred to the OIG.
- **Allegation/Investigation:** From 2007 to 2011, Cheryl Jean Jones used identities of 52 individuals to prepare, submit applications for FSA funds, many of whom were ineligible for the funds. This resulted in disbursements of about $513,000.
- **Outcome:** Jones was arrested in February 2013. She pleaded guilty to 10 counts of wire fraud and was sentenced to 24 months in prison, and ordered to repay $166,000 to the Department of Education.

OIG Criminal Investigation

- **Allegation:** Michael Gagliano, President of Galiano Career Academy, used a "diploma mill" owned by his wife to make students eligible for student assistance programs.
- **Investigation:** FSA conducted a program review at Galiano Career Academy in 2009, and when it saw suspicious activity it referred the matter to OIG which launched a criminal investigation. OIG Special Agents later learned Gagliano installed cameras and microphones prior to the Department's visit so he could hear their conversations.
- **Outcome:** Gagliano pleaded guilty in August 2013. In February 2014, in Orlando, FL, U.S. District Judge Roy B. Dalton sentenced Gagliano to four years in federal prison for theft of government property, obstruction of a federal audit, and aggravated identity theft. The court also ordered restitution, entered a judgment of $2,105,761.00, the proceeds of the charged criminal conduct.

Criminal Investigation

- **Allegation:** Guled Ali Omar, Abdurahman Yasin Daud, Mohamed Abdihamid Farah and their co-conspirators made multiple attempts to join ISIL in Syria between May 2014 and April 2015.
- **Investigation:** The FBI-led Joint Terrorism Task Force, with support from the Department of Education OIG, conducted the investigation. It was the first multi-defendant ISIL-related trial.
- **Outcome:** They were convicted in June 2016 of conspiring to commit murder in Syria on behalf of ISIL and to provide material support to the organization. Omar was also convicted of attempted financial aid fraud, and Farah was convicted of perjury and providing a false statement.

Civil Investigation

- **Allegation:** EDMC was accused of violations of the Higher Education Act's Incentive Compensation Ban and of deceptive and misleading recruitment practices. It was accused of running a high pressure boiler room, where administration personnel were paid based purely on the number of students they enrolled.
- **Outcome:** In 2015 U.S. Attorney General Loretta Lynch announced that a global civil settlement had been reached with EDMC for $95.5 million.

Criminal and Civil Remedies Used by OIG

CRIMINAL

Education Fraud
20 U.S.C. § 1097 (a)

- Any person who knowingly and willfully embezzles, misapplies, steals, obtains by fraud, false statement, or forgery, or fails to refund any funds, assets, or property provided or insured under Title IV of the HEA, or attempts to embezzle…
- Persons convicted of a **felony** shall be fined not more than $20,000 or imprisoned for not more than 5 years, or both.
- Attempt is defined as, “an undertaking to do an act that entails more than mere preparation but does not result in the successful completion of the act.”

CIVIL

Civil False Claims Act
31 U.S.C. § 3729

- Knowingly presents, or causes to be presented, to the United States Government a false or fraudulent claim for payment or approval (no proof of specific intent to defraud is required.)
- …or makes, uses, or causes to be made or used, a false record or statement to get a false or fraudulent claim paid or to conceal, avoid, or decrease an obligation to the Government.
- Burden of Proof – “Preponderance of the Evidence” (More likely than not).
- Specific Intent to Defraud the Government not required
- Liable for Civil Penalties of between $10K and $20K per count **plus** 3 times the amount of actual damages.

Technology Crimes Division (TCD)

TCD Structure

- TCD centralizes OIG digital investigations and our support missions for traditional OIG services:
  - Comprised of three separate units, each with a distinct mission, that support each other and other OIG components
- Staffing:
  - Special Agents
  - IT Computer Specialists
  - Investigative Analysts
  - Financial Analysts

ELECTRONIC CRIMES TEAM

DATA ANALYSIS AND REFERRAL TEAM

DIGITAL FORENSIC LABORATORY

TCD Investigative Mission

- Investigates criminal cyber threats against the Department's IT infrastructure, or criminal activity in cyber space that threatens the Department's administration of Federal education assistance funds
- Conducts investigations unauthorized access of any information technology system used in the administration, processing, disbursement, or management of Federal funds originating from the Department
- Identifies and provides referrals of vulnerabilities in Department's systems and programs

Why Are You a Target?

BECAUSE YOU HAVE WHAT THREAT ACTORS WANT!

- The Department, FSA and entities receiving Title IV funding have network resources and sensitive student and financial data that could be of interest to several groups:
  - Commercial entities, Insiders, Hackers, Terrorists, Foreign Intel Services
- Data and resources of interest:
  - Hardware and bandwidth
  - Personally Identifiable Information (PII) on ~100 million US citizens (FAFSA applications, PAS, CPS, NSLDS)
- ID Theft Resource Center reports that in 2016, there have been **783 breaches** of over **29 million records!**

The Threat

- Criminals access data as a result of:
  - Identifying vulnerabilities, compromises, social engineering, phishing and backdoors
  - A weak IT security posture (i.e., shared passwords, lack of priority and emphasis on network security)
- What criminals do on your network:
  - Scan for vulnerable systems (reconnaissance)
  - Take low-hanging fruit if possible
  - Abuse trusted computing relationships
  - Exfiltrate data

TCD Investigation

- **Allegation:** A University of Nebraska student gained unauthorized access to the PeopleSoft CampusVue program used in the administration of Title IV funds and stole the academic profiles of 650k students. The student was allegedly attempting to change his recorded grades.
- **Investigation:** TCD, the FBI and the University of Nebraska Police Department jointly conducted the investigation. The student's personal computers were seized via search warrant and forensically examined by TCD. The exam revealed that the student had performed several weeks' worth of reconnaissance from outside and inside the University of Nebraska networks, using Virtual Private Network login credentials. After combining the information from the student's computers with logs from the university, investigators were able to compile a comprehensive timeline of the student's actions to prove the student committed the crime.
- **Outcome:** The student was convicted of violating 18 U.S.C. 1030, fined $107,000 and confined for one year.

Types of Potential Cyber Crime Activity

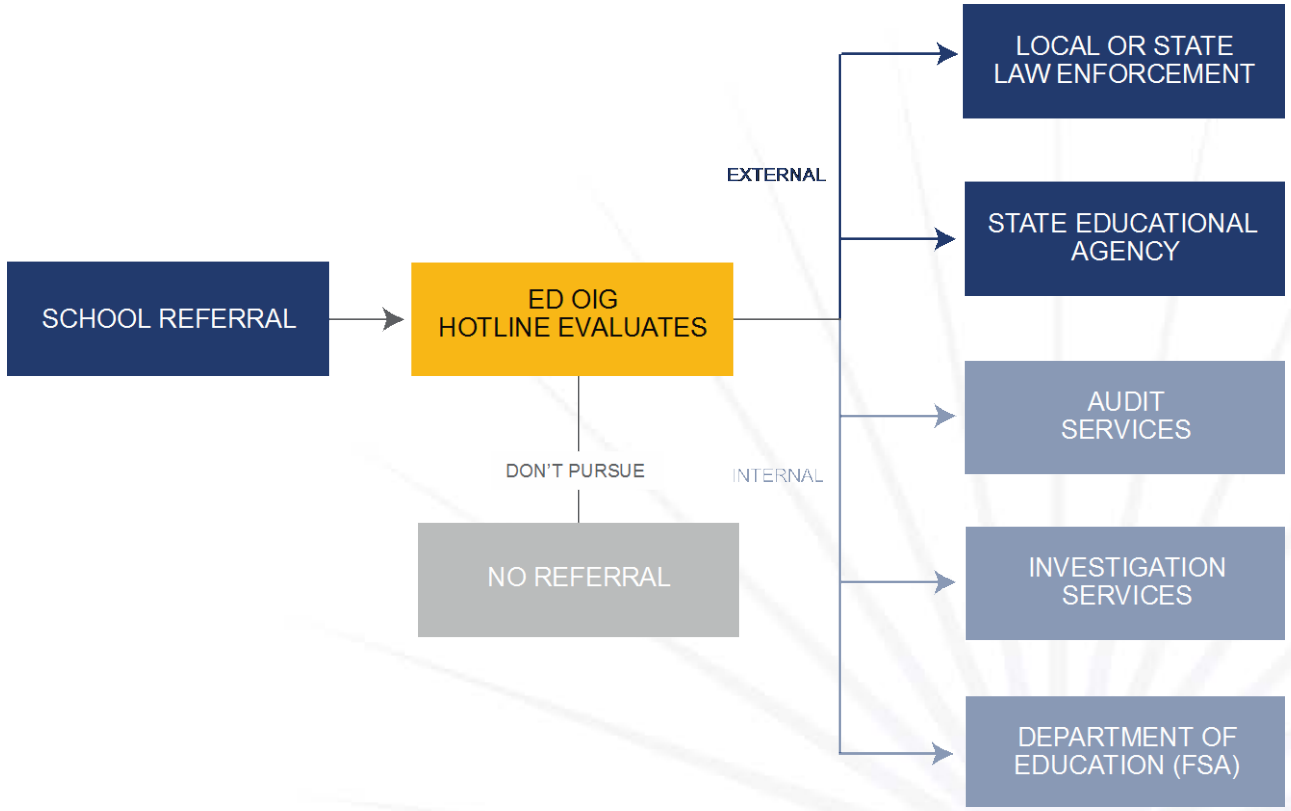
- Compromise of system privileges
- Compromise of information protected by law (FERPA, GLBA, etc..)
- Unauthorized or exceeding authorized access of IT systems or protected data
- Indicators of possible criminal activity:
  - Requesting access to systems they do not require access to
  - Using removable media in systems where data should not be removed
  - Accessing systems outside normal work hours
  - Bragging about having access to sensitive data
  - Excessive complaints about identity theft

Pathways to Success

Why Report Fraud to OIG?

- Meet statutory and regulatory requirements
- Comply with ethical responsibility
- Deter others from committing fraud and abuse
- Protect the integrity of the Title IV Programs
- Avoid being part of a fraud scheme
- Prevent administrative action
- Avoid civil penalties
- Prevent criminal prosecution

OIG Hotline Referrals and Resolution



Not all complaints filed with the OIG will generate an investigation, audit or inspection by the OIG. We may refer matters to another office within the Department or to an external entity as appropriate. The OIG Hotline does not provide updates regarding the status of complaints.

How You Can Help

- Ensure that staff receive necessary Title IV training
- Review documents thoroughly
- Question documents/verify authenticity
- Request additional information from students or their parents
- Compare information on different documents
- **Contact the OIG if you suspect fraud**
- **Cooperate with the OIG in connection with an audit or investigation**

Report Fraud!

Inspector General's Hotline

You can reach the Hotline on the web at:

OIGhotline.ed.gov

Or call

1-800-MIS-USED

Questions?