Internal and External Threats Facing Title IV Institutions

Presented by the Office of Inspector General
Investigation Services
U.S. Department of Education

INVESTIGATION SERVICES
OFFICE OF INSPECTOR GENERAL
UNITED STATES DEPARTMENT OF EDUCATION

Agenda

- OIG Background and Mission
- Why Title IV Institutions are Targets
- External Fraud
- Internal Fraud
- Emerging Fraud and Threats
- Pathways to Success
- How to Report Fraud

OIG Background and Mission

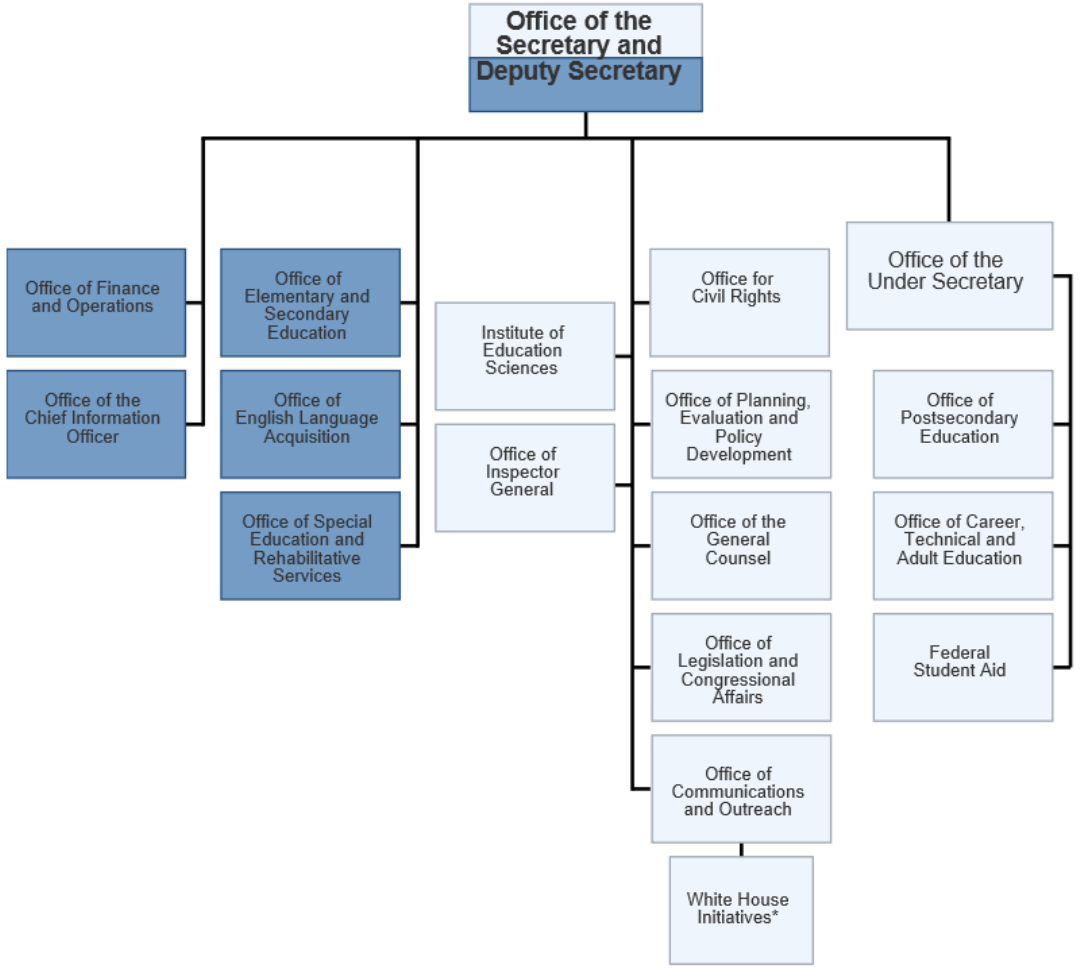
Inspector General Act of 1978

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

Organizational Chart

The Office of Inspector General (OIG) is an independent component of the Department.

We examine allegations of fraud, waste, and abuse, and pursue those who seek to enrich themselves by abusing Department programs at the expense of our nation's taxpayers.



INVESTIGATION SERVICES
OFFICE OF INSPECTOR GENERAL
UNITED STATES DEPARTMENT OF EDUCATION

OIG Operational Components

Audit Services

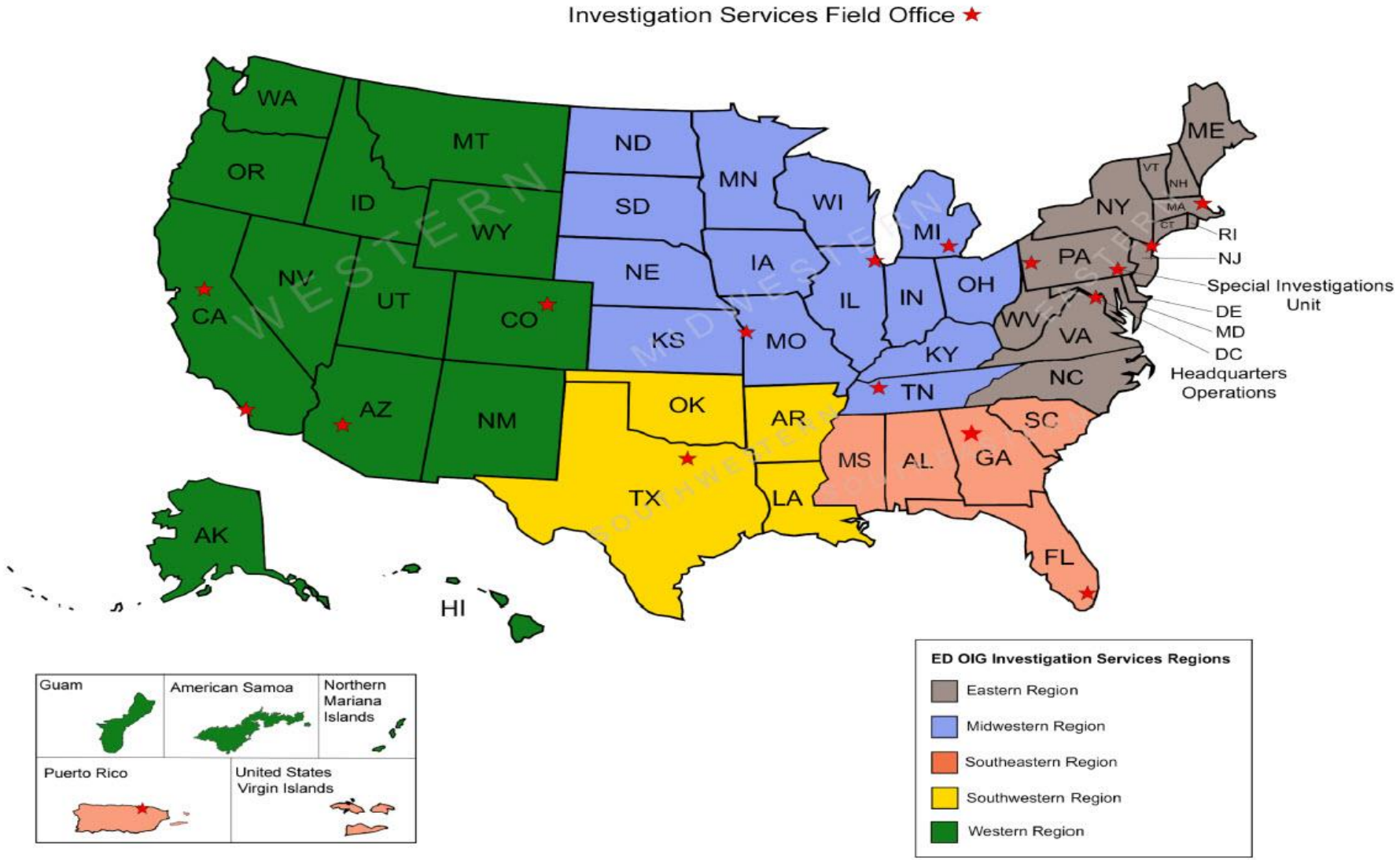
Information Technology Audits and
Computer Crime Investigations (ITACCI)

Investigation Services

Investigation Services

- 75 Federal law enforcement officers who receive extensive training in criminal and civil law
- Conduct criminal, civil and administrative investigations covering a wide range of wrongdoing including Federal student aid fraud, diploma mill schemes, fraud and corruption in after school programs, and grand and contract fraud
- Coordinates with other federal, state, and local law enforcement agencies and also federal prosecutors at the U.S. Department of Justice
- Operates the OIG Hotline
- Works with the Department to develop appropriate enforcement actions and recommend fixes to Department programs vulnerable to fraud
- Conduct outreach and provide fraud briefings on how to identify fraud

Investigation Services Regional Map



INVESTIGATION SERVICES
OFFICE OF INSPECTOR GENERAL
UNITED STATES DEPARTMENT OF EDUCATION

Differences Between OIG and FSA PROGRAM COMPLIANCE

OIG INVESTIGATION SERVICES

- Investigates any **fraud** impacting Department 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
- Operates independently of the Department in exercising its investigative authority

FSA PROGRAM COMPLIANCE

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

OIG and FSA Coordination

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

- Issues Management Information Reports to alert the Department about serious fraud and corruption trends
  - Distance Education Fraud Ring Report
    - Dear Colleague Letter – Fraud in Postsecondary Distance Education Programs
    - OIG Audit – Additional Safeguards Are Needed to Help Mitigate the Risks That Are Unique to the Distance Education Environment
  - PIN Security Vulnerabilities Report
- 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

Why Title IV Institutions are Targets

What is Fraud?

A deliberate distortion of the truth in an attempt to obtain something of value.

-or-

Lying and cheating.

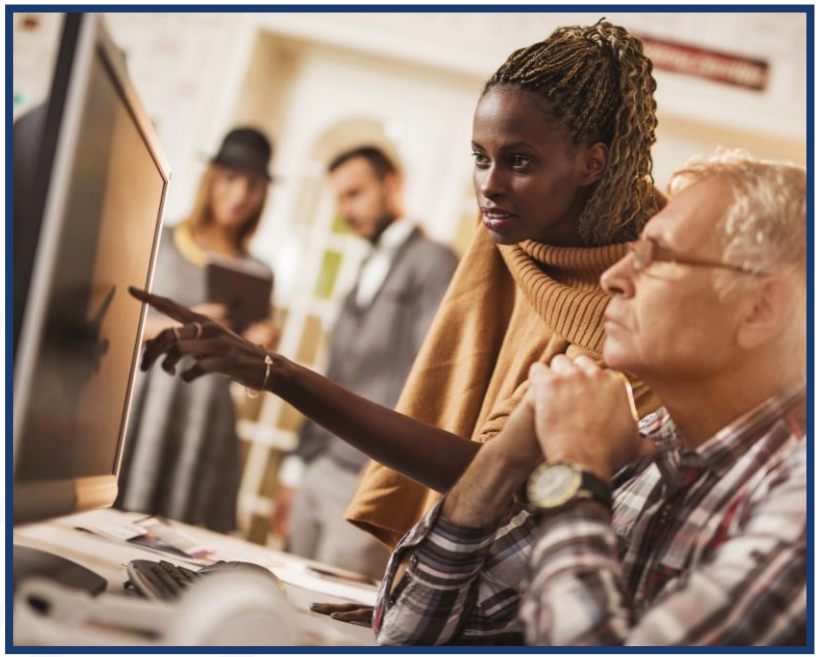
Why Are You a Target for Fraud?

BECAUSE YOU HAVE WHAT CRIMINALS WANT!

- **$$$ MONEY $$$** - You are a financial institution that handles millions of dollars every year.
- Your "customers" do not typically consider the fraud threat.
- You have network resources and sensitive student and financial data that are of interest to commercial entities, insiders, hackers, terrorists, etc.
- Your infrastructure may not be configured for fraud detection, prevention, and deterrence. ID Theft Resource Center reports that in 2019, there were **1,473 breaches** of over **164 million records**! Of these breaches, 118 were in the education sector.

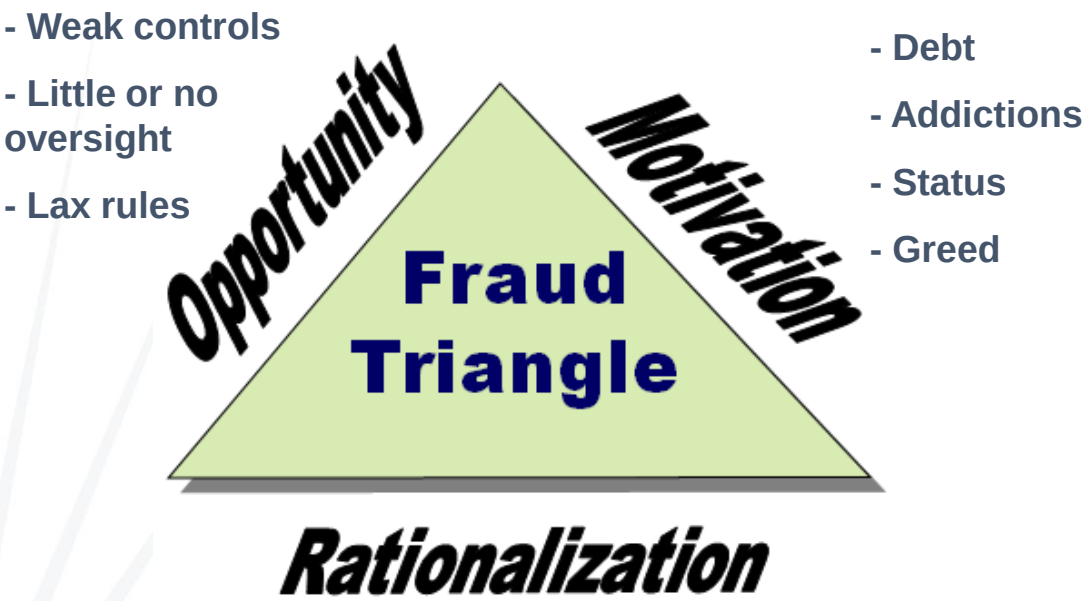
Why Are You Important to OIG?

You play a critical role in helping us achieve our mission by serving as the OIG's "eyes and ears" to help us detect and prevent fraud.



Fraud Risk Indicators

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



Types of Fraudulent Activity

Fraud Committed by Students

- FAFSA Fraud
  - Social Security Number
  - Alien Registration Status
  - Dependency Status
  - Income and Assets
  - Number of Family Members in College
- Identity Theft
- Falsification of Documents
- Distance Education Schemes

Fraud Committed by School Officials, Contractors, Grant Recipients, etc.

- Ghost Students
- Theft/Embezzlement
- Obstruction of a Federal Audit or Program Review
- 90/10 Rule Manipulation
- Compromise of system privileges or compromise of protected information
- Unauthorized or exceeding authorized access of IT systems or protected data

Statutory and Regulatory Access to Records

- Under the Department's regulations at 34 CFR 668.24(f), an institution that participates in any Title IV, HEA program and the institution's third-party servicer, if any, must cooperate with the Department of Education's IG, in the conduct of audits, investigations, program reviews, or other reviews authorized by law. Cooperation include access to records and personnel for interview.
- 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 OIG**. 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.

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 anyone who attempts to perform the above actions
- 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

External Fraud

Distance Education Fraud Ring

- OIG received a referral from a guaranty agency who received three complaints from individuals who claimed they never attended college in Arizona but had loans disbursed in their names.
- OIG worked with Maricopa County Community College to identify 289 students accounts accessed by the same IP address associated with the three individuals.
- The investigation determined that a father and son used over 300 mostly stolen identities to cause $1.4M in Federal student aid to be disbursed.
- The subjects were each charged with over 10 counts of fraud and pled guilty to conspiracy to commit financial aid fraud.
- The subjects were sentenced to 12 months and 1 day and 15 months imprisonment and ordered to pay restitution of $936.014.

Debt Relief Fraud

- A company called Student Loan Relief Department (SLRD) allegedly lured borrowers through advertisements on Facebook to reduce their debt.
- SLRD allegedly obtained and used PII from student borrowers responding to the ads to gain access to FSA's student loan portal.
- SLRD allegedly advised borrowers that they qualified for a debt relief program and enticed them to take out high-interest loans to pay the company a fee up to $1,300 for their services.
- The services SLRD offered, including loan deferment and income-driven repayment programs, are already available to the students through ED free of charge.
- In March 2020, five SLRD officials, including the chief executive officer, chief financial officer, and general manager were arrested in a 20-count indictment for allegedly preying on student loan borrowers.

Network Intrusion

- A University of Nebraska student gained unauthorized access to the University's computer system and stole the academic profiles of 650k students. The student was allegedly attempting to change his recorded grades.
- TCD, FBI and the University Police investigated and seized the student's personal computers via search warrant.
- TCD forensic exam revealed the student had performed reconnaissance from outside and inside the University's networks.
- By comparing this data 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.
- The student, who was convicted of violating 18 U.S.C. 1030 (fraud and related activity in connection with computers), was sentenced to one year confinement and fined $107,000.

Internal Fraud

Civil Investigation (Qui Tam)

- A qui tam was filed in the District of South Carolina alleging that North Greenville University (NGU), Oral Roberts University (ORU), and San Diego Christian College (SDCC) each violated Department's ban on incentive compensation.
- The OIG and USDOJ investigation determined the schools used Federal funds to pay vendor commissions, bonuses, and/or incentive payments for recruiting students for enrollment.
- As a result of the investigation, the USDOJ reached civil settlements with the schools.
- The settlement required the following payments:
  - NGU agreed to pay $2.5M to FSA
  - ORU agreed to pay $303,502 to FSA

School President

- ED received an allegation that the president of Galiano Career Academy (GCA) was using a "diploma mill" owned by his wife to make students eligible for student assistance programs.
- FSA conducted a program review at the school, and when it saw suspicious activity it referred the matter to OIG, which launched a criminal investigation.
- During the execution of a search warrant, OIG discovered the school had installed cameras and microphones prior to the FSA program review in order to record the reviewers' conversations.
- The OIG investigation revealed GCA used the diploma mill to falsely certify ineligible students as high school graduates to circumvent Title IV requirements.
- The GCA president pleaded guilty to theft of government property, obstruction of a federal audit, and aggravated identity theft.
- He was subsequently sentenced to four years in prison and ordered to pay $2,105,761 in restitution.

Director of Financial Aid

- The former Director of Financial Aid (DFA) for Teachers College, Columbia University unilaterally inflated students' cost of attendance increasing the amount of financial aid they were eligible to receive. Over $1.4 million in unauthorized stipends were approved for students.
- DFA is alleged to have received $350K in kickbacks from the students.
- The former DFA and four graduate students were arrested and charged with bribery, federal student aid fraud, and conspiracy to commit wire fraud and bribery.
- All defendants plead guilty.
- DFA sentenced to 40 months in jail and over $2M in restitution.
- Students received a range of sentences from supervised release to 1 year and a day incarceration.

Emerging Fraud and Threats

CARES Act – Education Stabilization Fund

$30.75 billion to the U.S. Department of Education to prevent, prepare for, and respond to coronavirus. The funds include $16.8 billion for state and local education agencies, and $13.9 billion for students, institutions of higher education (IHE) and education related entities.

- Distance education fraud rings due to increased online education;
- Incentive compensation violations due to more aggressive marketing to enroll students;
- Procurement fraud – lack of internal controls creates opportunities for fraud;
- Theft and embezzlement - increased purchasing of equipment for distance learning) without proper internal controls;
- Public corruption - public officials taking advantage of the COVID- 19 crisis to engage in fraudulent or otherwise illegal schemes.

Third Party Debt Relief Companies

INVESTIGATION SERVICES
OFFICE OF INSPECTOR GENERAL
UNITED STATES DEPARTMENT OF EDUCATION

Pathways to Success

Best Practices

- Conduct a fraud risk assessment and assess potential threats
- Create a plan to mitigate risks and to evaluate potential fraud
- Coordinate with IT departments to identify
  - Common addresses (including IP and email)
  - Common bank accounts
  - Common passwords and challenge questions,
  - Anomalous geographic locations
- Participate in information sharing with other schools
- Require two-factor authentication to improve security of student accounts
- Formalize a process for reporting potential fraud, waste, and abuse to OIG

Your Role in Preventing and Detecting Fraud

- Review documents thoroughly, question/verify authenticity, and request additional information
- Ensure that staff receive necessary Title IV training
- Stay current on alerts and communication from Federal Student Aid
- Stay current on types of fraud affecting Title IV schools by signing up for the OIG's free **Notification Service**, and follow us on **Facebook** and **Twitter**
- **Cooperate with the OIG in connection with an audit or investigation.** Don't "tip off" subjects of actual or pending investigation, continue normal course of business unless otherwise directed
- **Contact the OIG if you suspect fraud**

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
- Avoid administrative, civil and criminal penalties

To participate in any Title IV program:

- *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, school, 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).*

How to Report Fraud

ED OIG HOTLINE

You can reach the Hotline on the web at:

OIGhotline.ed.gov

Or

Contact one of the OIG's regional offices at www.ed.gov

Secure Electronic Reporting

OIGHOTLINE.ED.GOV

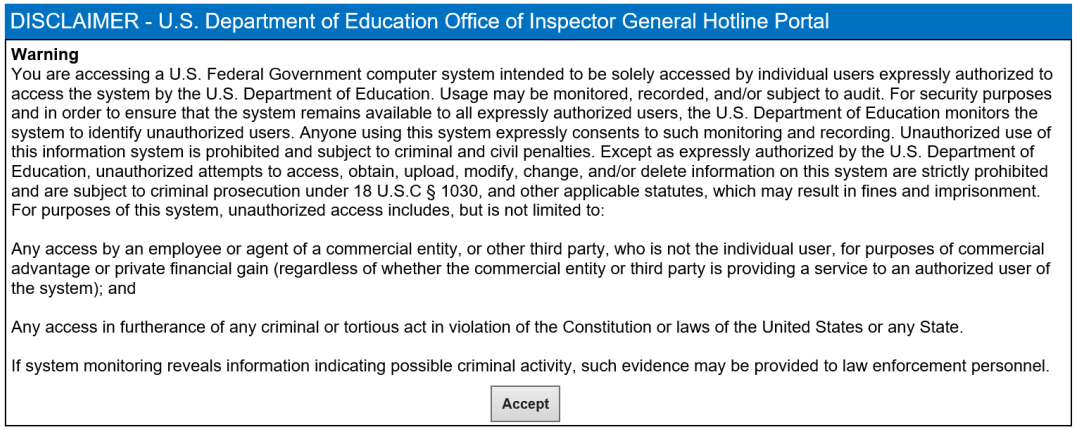
OIG Hotline

Report Fraud Now!

The OIG Hotline is available for anyone who knows of or suspects fraud, waste, abuse, mismanagement, or violations of laws and regulations involving ED funds or programs. This includes allegations of suspected wrongdoing by ED employees, contractors, grantees, schools and school officials, persons in positions of trust involving ED funds or programs, collection agencies, recipients of student financial assistance, or lending institutions. If you have knowledge of any wrongdoing involving ED funds or operations, let us know! **Click the button below to get started.**

REPORT HERE

- What to Report to the OIG Hotline
- What Not to Report to the OIG Hotline



DISCLAIMER - U.S. Department of Education Office of Inspector General Hotline Portal

Warning

You are accessing a U.S. Federal Government computer system intended to be solely accessed by individual users expressly authorized to access the system by the U.S. Department of Education. Usage may be monitored, recorded, and/or subject to audit. For security purposes and in order to ensure that the system remains available to all expressly authorized users, the U.S. Department of Education monitors the system to identify unauthorized users. Anyone using this system expressly consents to such monitoring and recording. Unauthorized use of this information system is prohibited and subject to criminal and civil penalties. Except as expressly authorized by the U.S. Department of Education, unauthorized attempts to access, obtain, upload, modify, change, and/or delete information on this system are strictly prohibited and are subject to criminal prosecution under 18 U.S.C § 1030, and other applicable statutes, which may result in fines and imprisonment. For purposes of this system, unauthorized access includes, but is not limited to:

Any access by an employee or agent of a commercial entity, or other third party, who is not the individual user, for purposes of commercial advantage or private financial gain (regardless of whether the commercial entity or third party is providing a service to an authorized user of the system); and

Any access in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State.

If system monitoring reveals information indicating possible criminal activity, such evidence may be provided to law enforcement personnel.

Accept

Questions?

Chris Hessberger
Special Agent
Chris.Hessberger@ed.gov