Fraud Detection and Prevention: Internal and External Threats Facing Title IV Institutions

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

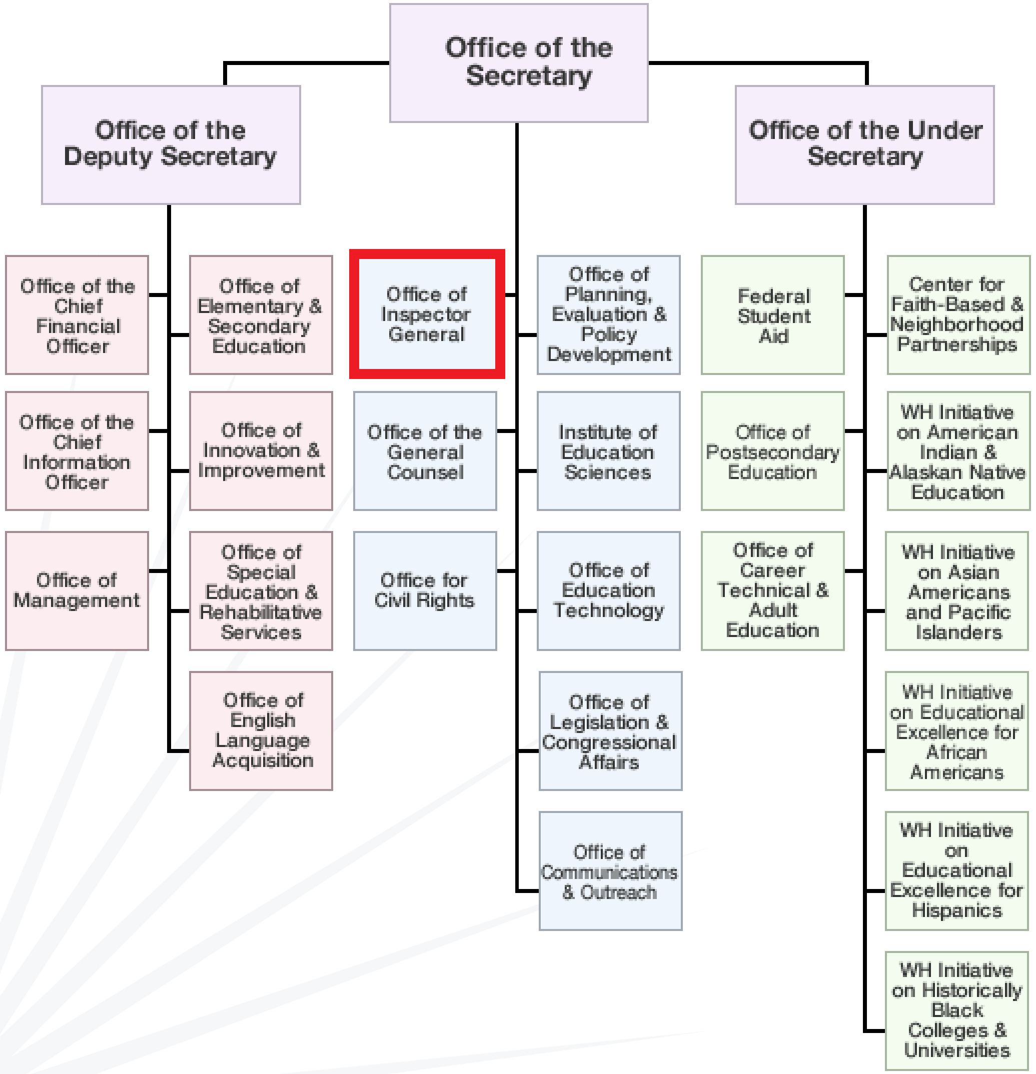
Agenda

- OIG Organization and Mission
- OIG Background
- Why Title IV Institutions are Targets
- External Fraud and Cyber Threats
- Internal Fraud and Cyber Threats
- Prevention and Detection using Fraud Indicators and Analytics
- Ways to Help OIG
- Contact Information

OIG Organization and Mission

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.**



OIG Authority, Access, and Fraud Reporting

Inspector General Act of 1978:

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

- **FERPA** provides that **consent is not required in order to disclose student records to the Office of Inspector General**.
- 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.

OIG Operational Components

Audit Services

Investigation Services

Information Technology Audits and
Computer Crime Investigations (ITACCI)

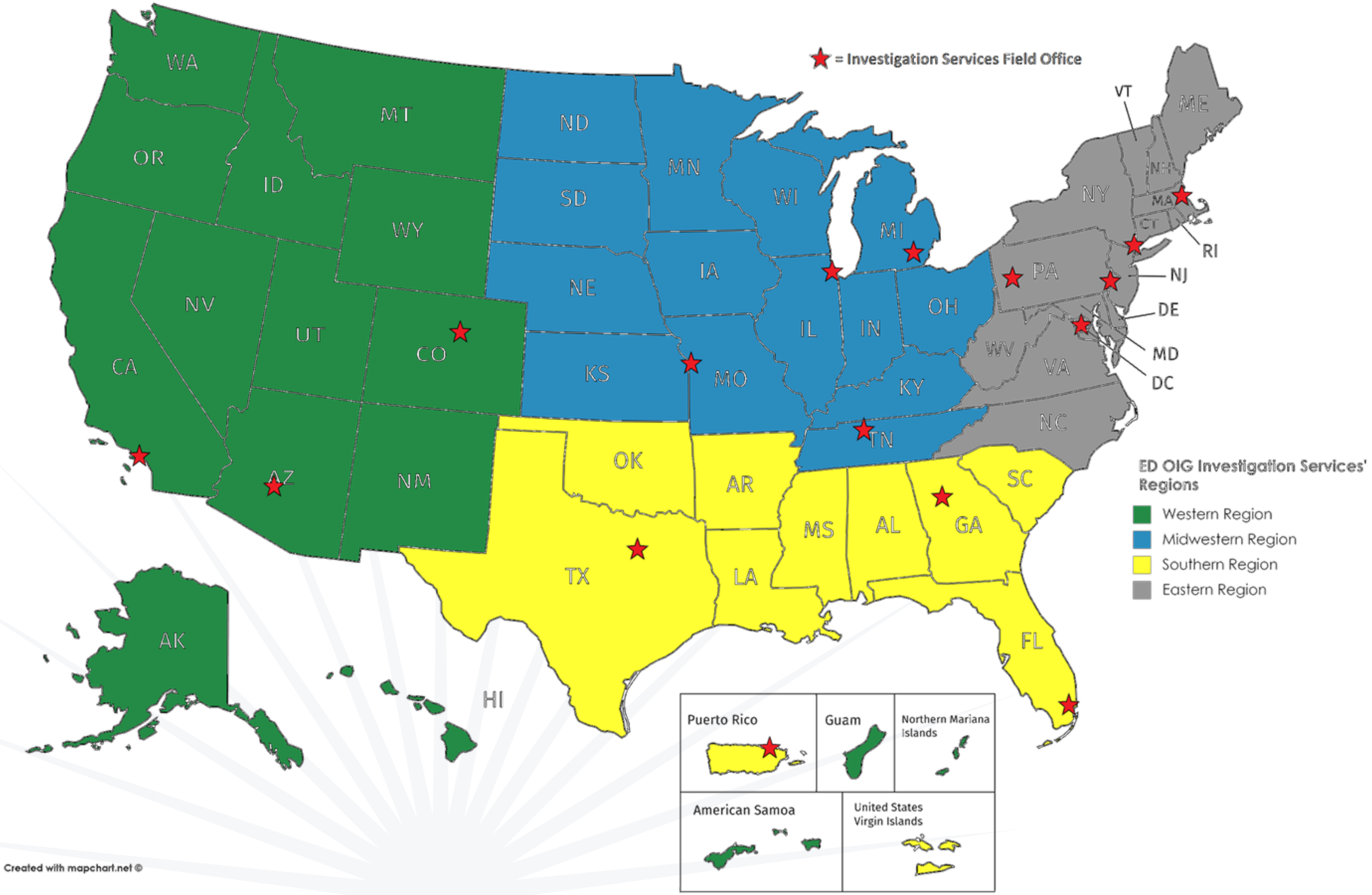
Investigation Services

- Federal law enforcement officers who receive extensive training in criminal and civil law
- Conduct criminal and civil investigations covering a wide range of wrongdoing including Federal student aid fraud, diploma mill schemes, fraud and corruption in after school programs, and fraudulent billing of contracts
- Conduct criminal investigations of suspected fraudulent activities by Department employees, contractors, grant recipients, school officials, teachers, and students
- Coordinates with 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

ITACCI - Technology Crimes Division

- Investigates criminal cyber threats against the Department's IT infrastructure, and criminal activity in cyber space that threatens the Department's administration of federal education assistance funds
- Conducts investigations into the 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

Investigation Services Regional Map



OIG Background

Differences Between OIG and FSA

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

- Conducts compliance reviews, administrative investigations of violations of HEA
- Takes administrative actions authorized by the HEA and program regulations
- Grants reviewers administrative authority
- 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.

Sources of Allegations

- School Employees and Officials
- OIG Hotline
- OIG Audits
- Department Program Offices
- Private Citizens and Students
- Federal, State, Local, and Tribal Agencies
- U.S. Attorney's Offices/State Attorney General's Offices
- Qui Tam or Other Civil Actions
- LEAs and SEAs
- Controllers/Auditors

Types of Cases

- Criminal
- Civil
- Administrative

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

Administrative Remedies

In some circumstances, it may be to the agency's advantage to pursue a case administratively, rather than criminally or civilly

- The $100 case
- The judgment-proof defendant
- Financial offset
- Suspension and Debarment

Why Title IV Institutions are Targets

Why Are You a Target for Fraud?

- You are a financial institution that handles millions of dollars every year.
- Your "customers" do not typically consider the fraud threat.
- Your infrastructure may not be configured for fraud detection, prevention, and deterrence.

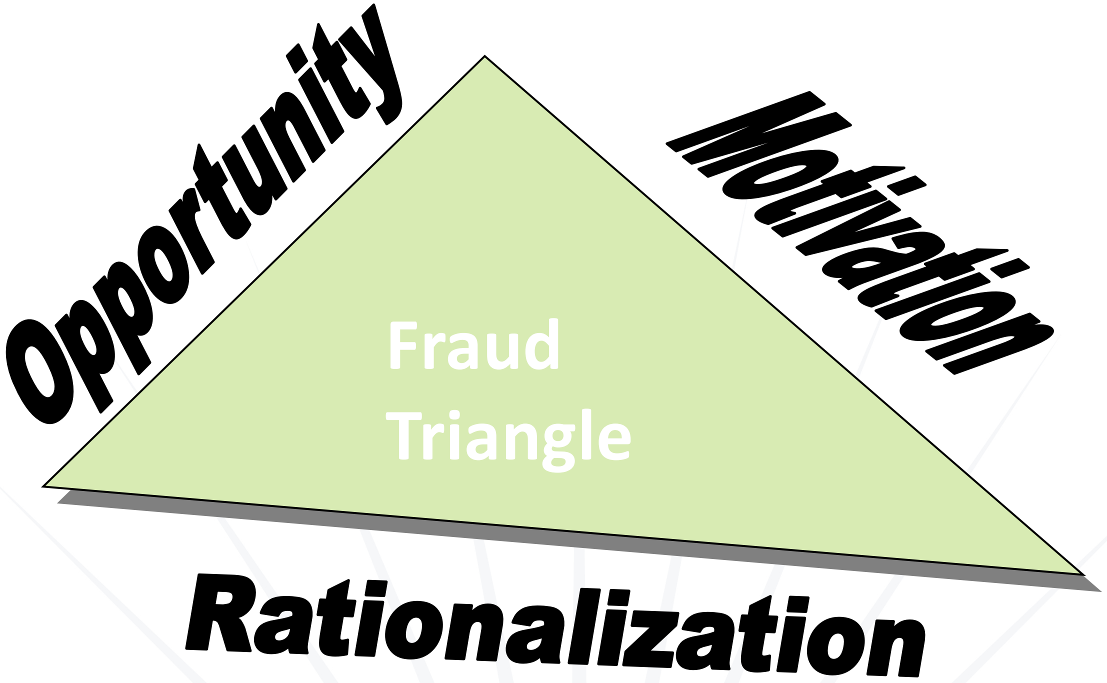
What is Fraud?

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

-or-

Lying and cheating.

- Weak controls
- Little or no oversight
- Lax rules



- Debt
- Addictions
- Status
- Greed

- Everyone does it.
- I was only borrowing the money.
- I was underpaid and deserve it.

Types of Potential Fraudulent Activity

- FAFSA Fraud
- Falsification of Documents
- Identity Theft
- Distance Education Schemes
- Fraud/Theft by School Employee
- Ghost Students
- Financial Statement Falsification
- Obstruction of a Federal Audit or Program Review
- 90/10 Rule Manipulation

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

Cyber Threat

- Criminals access data and systems through:
  - Exploiting vulnerabilities, compromises, social engineering, phishing, and backdoors
  - A weak IT security posture (i.e., shared passwords, lack of priority to or emphasis on network security)
  - Single factor authentication
- What criminals do on your network:
  - Scan for vulnerable systems (reconnaissance)
  - Take low-hanging fruit if possible
  - Abuse trusted computing relationships
  - Exfiltrate data
  - Manipulate accounts
  - Use your computers and network assets

Why Are You a Target for Cyber Attacks?

BECAUSE YOU HAVE WHAT CRIMINALS WANT!

- $$$ MONEY $$$
- 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 2018, there have been **864 breaches** of over **34.1 million records**!

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:
  - Insiders
    - Requesting access to systems to which they do not require access
    - Using removable media in systems where data should not be removed
    - Accessing systems outside normal work hours
    - Bragging about having access to sensitive data
  - Outsiders
    - Excessive complaints about identity theft
    - Unexplained mail delivery rules in mailboxes

Work with your IT Department!

External Threats

Prison Fraud Ring Using Inmate Information

- Referral from Pikes Peak Community College (CO)
- Approximately 183 applications containing names of inmates were submitted for federal student aid at several community colleges in Colorado and Arizona
- Scheme involved Trammel Thomas and co-conspirators submitting false claims for federal student aid using stolen identities of prison inmates
- The loss was approximately $500,000
- 3 guilty pleas and one trial conviction

Terrorism-Related Investigations

"Three Minnesota men convicted of conspiring to join Islamic State" *U.S. Department of Justice, June 2016*

"Two Orange County Men Convicted of Conspiring to Join ISIL; They also Engaged in Fraud to Finance One's Trip to Syria" *U.S. Department of Justice, June 2016*

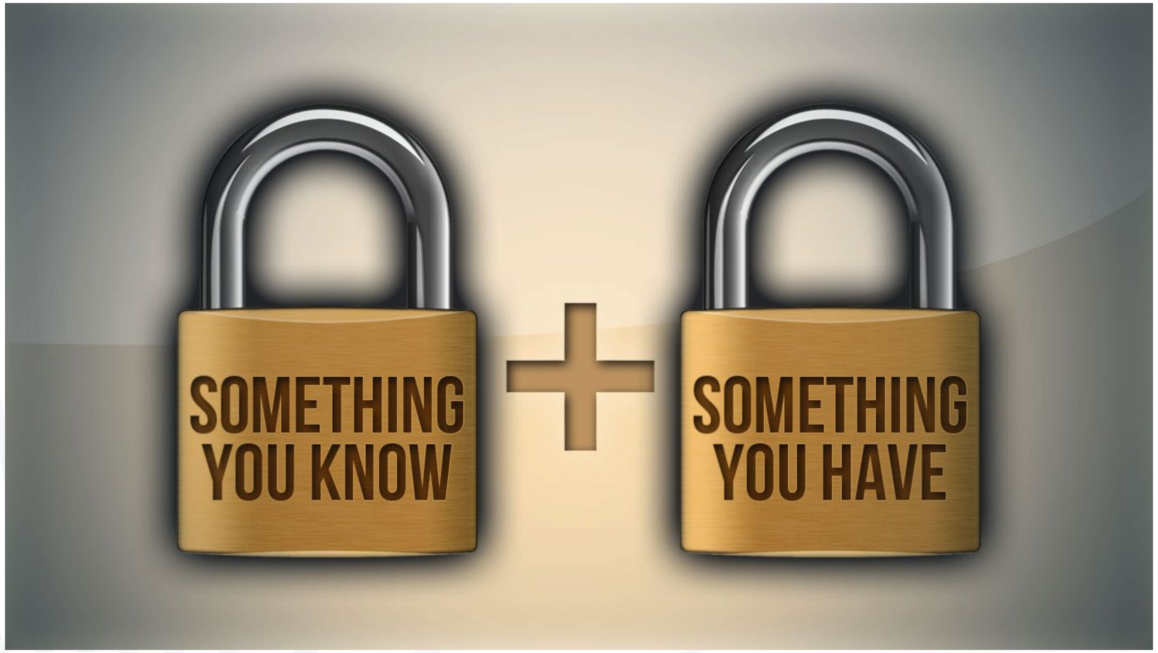
The defendants (Muhanad Badawi, pictured) and were convicted of terrorism and fraud charges for using their federal student aid to purchase plane tickets so that they could travel to the Middle East and join ISIL. These cases are the result of an investigation conducted by the FBI-led Joint Terrorism Task Force with support from the OIG.

The Rhodes Scholar

- Referral from USA Funds
- Individual legally received a second SSN based on personal safety issues
- Individual used her new SSN to defraud lenders out of more than $600,000 in student loan money that she used to play the stock market, buy a condo and launch a startup business
- Received approximately $240,000 in Stafford subsidized and unsubsidized loans in addition to almost $700,000 in private loans through Sallie Mae and USA Funds
- Sentenced to 57 months

2 Factor Authentication - refund redirection

Allegation: Multiple institutions reported student accounts compromised by phishing email, then direct deposit information was changed so that student refunds were sent to different bank accounts not controlled by the students. Also, compromised accounts were used to phish other institutions.
Investigation: still ongoing.
Outcome: undetermined.
Takeaway: 2 Factor Authentication is absolutely necessary in today's e-banking environment.



Internal Threats

Fraud by Student Adviser

- Valdez was employed by a for-profit automotive college in Arizona as a student benefits advisor
- Valdez forged the signatures of more than 150 students at the school on deferment and forbearance forms, then submitted them to the US Department of Education and its loan servicing partners
- Indicted on 5 counts in the Superior Court of the State of Arizona for fraudulent schemes and artifices, theft, and forgery

Fraud by School Executives

CROWN COLLEGE

TACOMA, WA

- Vice-President, Financial Aid Director, Business Manager, and Admissions Director
- School executives obtained $65,750 in Pell Grant and FFEL loan funds for family, friends, and themselves
- Claimed to be students when they were not students
- Planned to have loans discharged after the school officially closed
- Two trial convictions and two guilty pleas

Galiano Career Academy

- Galiano President Michael Gagliano used a "diploma mill" owned by his wife to make students eligible for financial aid.
- FSA conducted a program review at Galiano Career Academy in 2009
- FSA uncovered suspicious activity and a criminal investigation was launched.
- OIG later learned Michael Gagliano installed cameras and microphones prior to FSA's visit so he could hear their conversations.
- Sentenced for Theft of Federal Funds, Obstruction of a Federal Audit, and Aggravated Identity Theft
- Sentenced to four years in federal prison and restitution in the amount of $2,105,761.00

Fraud by IT Contractor

Allegation: PII for 63 student borrowers was found by local police at a residence during a search warrant.

Investigation: An individual residing at the search warrant location was employed by a large IT contractor that provided support to state student financial aid and medicare programs. Examination of the victim list revealed disbursed financial aid for which the students had not applied. Additionally, victims had false tax returns filed in their name.

Outcome: The individual was sentenced to 24 months of incarceration, 36 months of probation, and restitution of $434,988.00

INVESTIGATION SERVICES
OFFICE OF INSPECTOR GENERAL
UNITED STATES DEPARTMENT OF EDUCATION

Prevention and Detection using Fraud Indicators and Analytics

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 in cash

- Inadequate or missing documentation
- Altered records
- Financial records not reconciled
- Unauthorized transactions
- Related Party transactions
- Repeat audit findings

Fraud Prevention & Detection Using Analytics

Detecting fraud before disbursing funds is the best way to combat this crime

Monitor the Admissions Process

- Students submit applications from the same IP Address
- Students call in from the same phone number or use the same fax number
- Students use the same email address, use disposable email addresses, or aliases (use of "+" or "." with Gmail)
- Students list the same references on Master Promissory Note
- Students appear to reside in a geographic location that is anomalous to the locations of other students
- Students submit forged High School Diplomas or GEDs

Fraud Prevention & Detection Using Analytics

Monitor Class Activity

- Same IP addresses associated with multiple students (logins and/or course work)
- Same email address used to participate in program
- Same/Similar password, challenge question & answers for school login
- Enrolled in same classes/programs

Fraud Prevention & Detection Using Analytics

Monitor Disbursements

- Funds for different students disbursed to the same bank account
- Debit cards and/or refund checks mailed to the same address/geographic area
- Student's debit card address is different than the application or FAFSA address
- Student's debit card address changed just prior to disbursement

Pathways to Success

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
- Don't "tip off" subjects of actual or pending investigation
- Continue normal course of business unless otherwise directed
- Don't feel compelled to prove a case
- **Contact the OIG if you suspect fraud**
- **Cooperate with the OIG in connection with an audit or investigation**

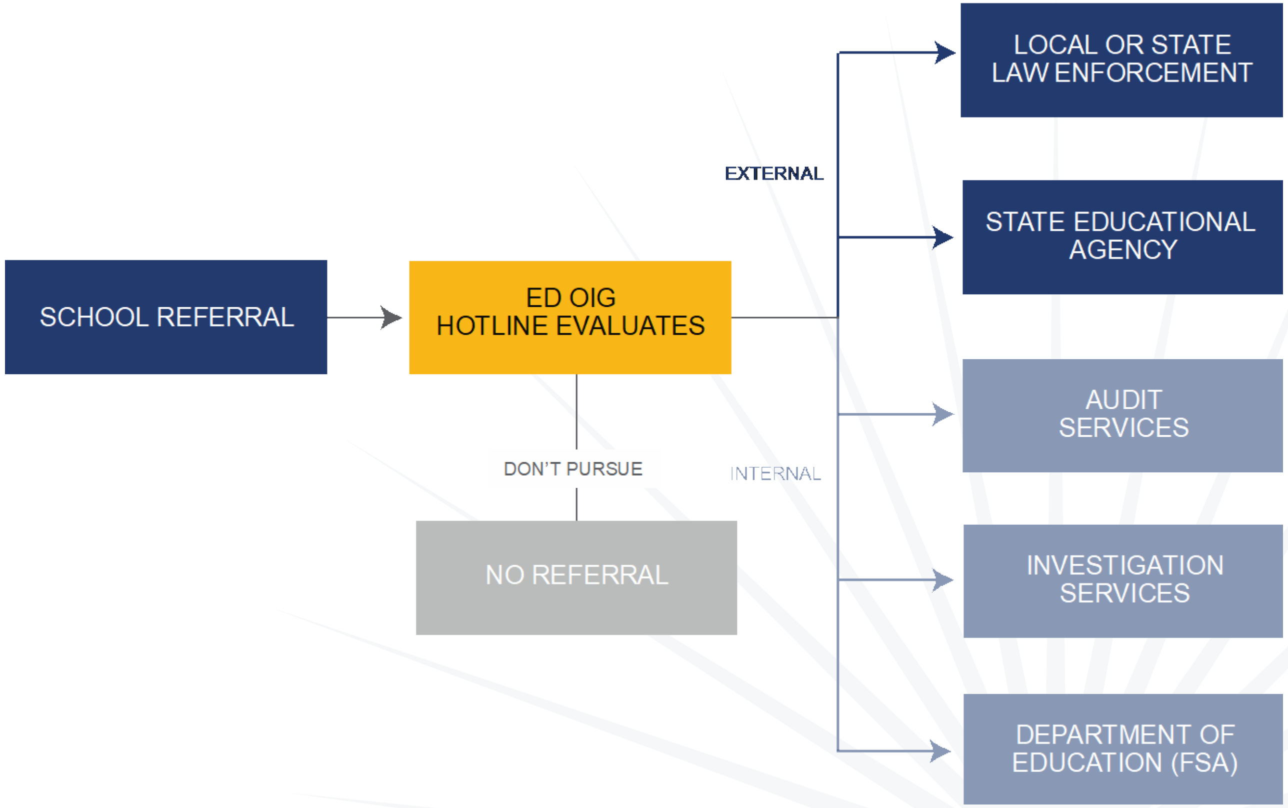
Why Report Fraud to OIG?

- 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

34 CFR § 668.16 Standards of Administrative Capability

- The Secretary considers an institution to have administrative capability if the institution:
- (f) Develops and applies 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.
- (g) Refers to the Office of Inspector General…any credible information indicating that an applicant for Title IV, HEA program assistance may have engaged in fraud or other criminal misconduct in connection with his or her application.
- Schools must also refer to the OIG any third-party servicer who may have engaged in fraud, breach of fiduciary responsibility, or other illegal conduct involving the FSA Programs and must include a requirement for the 3rd party service to report fraud to the OIG in their contract with that 3rd party servicer (34 C.F.R. § 668.25(c)(2)).

OIG Hotline Referrals and Resolution



Not all complaints filed with the OIG will generate an investigation or audit 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.

Report Fraud!

Inspector General's Hotline

You can reach the Hotline on the web at:

OIGhotline.ed.gov

For questions, call

1-800-MIS-USED

Adam Shanedling, Special Agent in Charge

Adam.Shanedling@ed.gov

(562) 980-4136

Chris Hodge, Assistant Special Agent in Charge

Christopher.Hodge@ed.gov

(562) 980-4132

One World Trade Center, Suite 2300, Long Beach, CA 90831

Questions?