Fraud Alert
Avoiding Scholarship Scams, Phishing, and Identity Theft

María A. Domínguez
First Assistant United States Attorney
District of Puerto Rico
Fraud Defined

- An **intentional** distortion of the truth in an attempt to obtain something of value. Does not have to result in monetary loss.

- **Layman’s terms:**
  Lying, cheating, and/or stealing.
“There is no kind of dishonesty into which otherwise good people more easily and frequently fall than that of defrauding the government.”

Benjamin Franklin
Who Commits Fraud Involving Education Funds?

- School employees, officials, owners, financial managers, and instructors
- Lenders and lender servicers
- Guarantee Agencies
- Award recipients
- Grantees and contractors
- Department of Education employees
- Others
Examples of Title IV Fraud Schemes

- Fraudulent enrollment
- Falsification of entrance exams
- Falsification of GEDs/HS Diplomas
- Falsification of attendance
- Falsification of grades
- Failure to make refunds
- Ghost students
- Leasing of eligibility

- Student Loan Fraud
- Loan theft/forgeries
- Fraud/theft by school employees
- Default rate fraud
- Financial statement falsification
- Falsified last date of attendance
- Obstruction of a federal audit or program review
Scholarship Scams

1. **Cash up front:** If you see a scholarship offer that requires you to send in an application or processing fee, this so-called "scholarship" is almost always a scam. Even if the offer adds a disclosure statement that guarantees a refund, money you send up front is almost never returned.

2. **Free seminar:** You may get an invitation or E-mail inviting you to attend a free seminar offering advice on financial aid and providing other helpful knowledge. While this may sound appealing, it's often a trap.

3. **Rewards without entries:** You may have seen pop-up ads that scream, "Congratulations! You have just won a $10,000 scholarship to college! To obtain your reward, please send in a $100 processing fee." If you did not apply for a scholarship or enter in a specific contest for this money, this is probably a scam.
4. **Time-sensitive scholarships**: Time-sensitive scholarships do not mean scholarship with deadlines. Nearly all scholarships have a certain date by which an applicant must complete and submit their application. In contrast, time-sensitive scams are on a first-come-first-served basis.

5. **Sweeping claims**: Lastly, be aware of scholarship offers that make sweeping claims. If you see an offer that declares any of the following, stay away.
Phishing

The use of social media engineering and technical subterfuge to steal consumer’s personal identity data and financial account credentials.

- Typically social engineering schemes use “spoofed” emails to direct users to counterfeited websites,

- Use of spyware, key loggers to capture personal data.
What can be done?

- Be suspicious of any email with urgent requests for personal financial information.
- Unless email is digitally signed, you can’t be sure it wasn’t forged or “spoofed”
- Phishers typically include upsetting or exciting, but false, statement in emails to get people to react immediately.
What can be done?

- Phishers typically ask for information such as:
  - Usernames,
  - Passwords,
  - Credit card numbers,
  - Social Security numbers, etc.

- Phisher emails are typically NOT PERSONALIZED while valid messages from your bank or e-commerce company generally are.
Prevention

- Don’t use links in an email to get to any web page if you suspect the message might not be authentic.

- Call the company on the telephone, or
- Log onto its website directly by typing in the web address to your internet browser.

- Avoid filling out forms in email messages that ask for personal financial information.

- You should only communicate information such as Credit card numbers using a secure web site or the telephone.
Prevention (Continuation)

- Always ensure you’re using a secure web site when submitting credit card and other sensitive information via your web browser.

- To verify if you are using a secure web server, check the beginning of the web address in your browser address bar:
  - It should always be “https://”

- Consider installing a web browser tool bar to help protect you from known phishing fraud web sites.
Prevention (Continuation)

- Regularly log into your online accounts
- Don’t leave it for a long time, before you check each account..
- Check your bank, credit and debit card statements to ensure that all transactions are legitimate:
  - If anything is suspicious contact your bank and credit card issuers
- Ensure that your browser is up-to-date and security patches are applied.
Reporting Phishing

- Always reports phishing or “spoofed” emails to the following groups:
  - Forward your emails to:
    - reportphishing@antiphishing.com
    - Federal Trade Commission
      - spam@uce.gov
    - FBI Internet Fraud Complaint Center
      - www.ifccfbi.gov
Reporting Phishing

- Always forward the “spoofed” of “abuse” email including the entire original email with its original header information intact.

- Forward the email to the “abuse” email address at the company that is being spoofed: e.g. “FSA help desk”
Identity Theft Prevention

- Properly handle documents
- Shred sensitive information
- Use key identifiers instead of the SSN
- Password protect sensitive information
- Audit access
- Review access privileges
- Verify who you are talking to
Statutes

Aiding and Abetting – 18 USC §2

False Statement – 18 USC §1001

Mail Fraud – 18 USC §1341

Wire Fraud – 18 USC §1343

Aggravated Identity Theft – 18 USC §1028A(a)(1)

Education Fraud – 20 USC §1097(a)

Conspiracy – 18 USC §371
Aiding and Abetting
18, United States Code, Section 2

(a) Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal. (b) Whoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal.
False Statement
18, United States Code, Section 1001

Whomever knowingly and willfully falsifies, conceals, or covers up by any trick, scheme, or device a material fact; makes any materially false, fictitious, or fraudulent statement or representation; or makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry;

shall be fined under this title, imprisoned not more than 5 years or, if the offense involves international or domestic terrorism (as defined in section 2331, imprisoned not more than 8 years, or both. If the matter relates to an offense under chapter 109A, 109B, 110, or 117, or section 1591, then the term of imprisonment imposed under this section shall be not more than 8 years.
Aggravated Identity Theft
18, United States Code, Section 1028A(a)(1)

Whoever, during and in relation to any [enumerated] felony violation ... knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.
Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses . . . for the purpose of executing such scheme . . . places in any post office or authorized depository for mail matter . . . to be sent or delivered by the Postal Service . . . or delivered by any private or commercial interstate carrier . . . or knowingly causes to be delivered by mail or such carrier . . . shall be fined under this title or imprisoned not more than 20 years, or both.
Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.
Educational Fraud
20, United States Code, Section 1097(a)

(a) In general 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 . . . (b) Assignment of loans: Any person who knowingly and willfully makes any false statement, furnishes any false information, or conceals any material information in connection with the assignment of a loan . . . (c) Inducements to lend or assign: Any person who knowingly and willfully makes an unlawful payment to an eligible lender . . . (d) Obstruction of justice: Any person who knowingly and willfully destroys or conceals any record . . . or attempts to so destroy or conceal with intent to defraud the United States or to prevent the United States from enforcing any right obtained by subrogation under this part, shall upon conviction thereof, be fined not more than $20,000 or imprisoned not more than 5 years, or both.
Conspiracy
Title 18, United States Code, Section 371

If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both.

Applies to all crimes, including drugs, white collar, etc.

5-year statutory maximum penalty.
Ghost Student Scam

A Chicago Public School principal and her programmer created 94 “ghost students” for the 2010-11 school year to push school attendance figures past 500 students, in order for the school to qualify for a Board-paid assistant principal position. The scheme was temporarily successful – a Board-paid assistant principal was, according to the report, provided to the school on the basis of the falsified enrollment numbers.

The programmer and principal later falsified grades for the newly-created ghost students after their initial lack of grades dragged down school averages and attracted the attention of a CPS Network Chief, according to the report. The number of ghost students fluctuated over the next year, dropping approximately 30 at one point and re-adding 20 to 25 at another.

The assistant principal position alone caused CPS to “improperly fund” $105,000 per year. Based on the investigation, the principal in question retired and was barred from ever being rehired by CPS. Disciplinary action against the programmer is pending.
Student Loan Fraud

Two (2) individuals were found guilty obtained Federal Student Assistant (FSA) funds by recruiting more than 50 straw students to apply for aid and caused the fraudulent disbursement of more than $200,000. The straw students applied for FSA at American River College, Sacramento City College and Consumnes River College. These applications contained false statements regarding the eligibility of the applicant. For the most part, all of the students signed up by Wilder and Huddleston withdrew from classes shortly after receiving the funds or received failing grades. While some of those students may have used the funds for legitimate educational expenses, Wilder and Huddleston demanded approximately half of those funds for their own purposes. Wilder has been ordered to pay $19,411 in restitution.
Questions?