Eye on ED Episode 9: Student Loan Scams and How to Avoid Them

[Intro] This is Eye on ED, your source for information about audits, investigations, and other work by the U.S. Department of Education Office of Inspector General. Tune in for the latest news on our efforts to find and stop fraud, waste, and abuse in Federal education programs, operations, and funding.

[Ryan Traher] Hello everyone, and welcome to another episode of Eye on ED, the official podcast of the U.S. Department of Education Office of Inspector General. I'm your host, Ryan Traher.

I bet that everyone listening today either took out student loans to help pay for their college degrees, helped their child obtain a student loan, or knows someone who did. And most people with student loans would like to consolidate their loans, pay them down, or when possible, eliminate that debt altogether.

Dishonest companies, cyber criminals and fraudsters know this, too. And that's why they've targeted student loan borrowers with schemes and scams aimed at separating you from your money, stealing your personal information, or both. The impact of falling victim to these scams can be severe—your identity stolen, credit cards and loans taken out in your name, your bank account zeroed out, and your credit score ruined.

Student loan schemes and scams are not new, and the U.S. Department of Education Office of Inspector General has been fighting them and alerting people to them for decades. In today's podcast, we're going to talk about student loan scams—how to spot them, how to avoid them, and what to do if you think you've been a victim of one. And to lead our discussion is Rob Mancuso, Assistant Inspector General for Investigation Services. Rob's team of law enforcement professionals is leading the OIG's efforts to help identify and stop these student loan scammers. Rob, thank you for being here today to talk about this important issue.

[Rob Mancuso] Thanks, Ryan. I'm really happy to be here.

[Ryan Traher] So let's jump right in. Fraud campaigns that target everyday Americans are not new, and that includes those that target college students and student loan borrowers. Why do dishonest companies and cyber criminals target students and student loan borrowers?

[Rob Mancuso] Great question Ryan. For the most part, it's no different from why anyone is targeted in a fraud scheme—to get your money or to get your personal information, like your Social Security number and date of birth. They like to target college students and student loan borrowers because they see them as vulnerable to their scams. They are busy with their studies or new jobs, or perhaps they are paying bills on their own for the first time, and like you said, they're always looking for ways to reduce their loans or eliminate them altogether. So fraudsters use the fact that you may have a student loan as the lure.

[Ryan Traher] To get your money or personal information.

[Rob Mancuso] Yes. Let's start with money. With student loan schemes, these bad actors and identity thieves come to you with offers to help you consolidate your student loans, reduce your payments, or eliminate your student debt altogether for a fee—either up front or monthly. The "for a fee" is

important as in most cases, these are services that you can do on your own for free through Federal Student Aid, and these criminals are banking on the fact that you may not know that.

Then there are fraudsters who are after your personal information—your birthday, your Social Security number. They use this information for other financial fraud and identity theft schemes, like taking credit cards and other loans out in your name or selling the information on the dark web.

[Ryan Traher] Can you tell us about some of the types of scams that are out there?

[Rob Mancuso] One that we've seen and investigated in the past are offers for loan consolidation. The way these work is that you may receive an email, text, or phone call that says that you are eligible for student loan forgiveness programs that in reality, you may or may not actually be eligible for, and they promise they can save you hundreds of dollars a month. Then they ask for your FSA account information.

[Ryan Traher] And by FSA account information you mean FSA ID, right?

[Rob Mancuso] Yes. The FSA ID is a username and password combination you use to log in to U.S. Department of Education online systems. The FSA ID is your legal signature for financial aid and shouldn't be created or used by anyone other than you—not even your parents, a school official, or a loan company representative. Please never share this information with anyone, because once the scammers take over your FSA ID, they change your email address and contact information, and you've lost control of your account. Your loan servicer cannot contact you, so you're no longer aware of what's going on with your loan—whether payments are made, or your in default.

[Ryan Traher] Great information, Rob, thank you. Tell us more about some of the scams that are out there.

[Rob Mancuso] So criminals and bad actors always look for opportunities to rip off the public and like they use times of crisis, trending topics, and economic challenges—when people are scared, desperate, and quite frankly at their most vulnerable—to propagate scams. Most recently, a scam started when the White House announced its plans for debt forgiveness. Fraudsters targeted people saying that they could enroll you right into that program, which of course they could not. There were so many fraud schemes that used the student loan forgiveness plan as a lure that our office issued a public service announcement in October. We alerted the public to student loan forgiveness schemes to help build awareness of these fraudulent efforts. Other Federal and State agencies have done the same, because the first step to avoid becoming a victim of a student loan scam is knowing that they are out there—that cyber criminals and identity thieves are trying to lure you into their traps.

[Ryan Traher] So what do these schemes and scams look like?

[Rob Mancuso] They can come in different shapes and forms but mostly they come in the form of unsolicited texts, emails, direct messages on social media, and even phone calls. They'll promise to help you obtain student loan forgiveness, reduce your student loan debt, consolidate your student loans, or eliminate your student loans completely. For college students or parents, they could be offering help to pay for college, or even saying the student has won a scholarship that they never applied for.

Look, these messages can be very, very convincing. They may look like they're from your bank, alma mater, student loan servicer, or even the U.S. Department of Education. They will rely on emotion or urgency in the hopes of tricking you into thinking it's legitimate, and to get you to respond quickly. I know that we all want to save money, but if something looks too good to be true, it probably is.

[Ryan Traher] Is there any type of language fraudsters use that could tip off people that what they are seeing is likely a scam?

[Rob Mancuso] Yes. They may use common words and phrases like, "Act immediately to qualify for student loan forgiveness before the student loan forgiveness program is discontinued." Or "Your student loans may qualify for complete discharge. Enrollments are first come, first served." Or "We'll work fast to help you eliminate your student loan debt."

[Ryan Traher] How do scammers get our emails or phone numbers in the first place?

[Rob Mancuso] Now that's a tricky one. A lot of times, they're just sending emails and texts to anyone and everyone (we call that phishing), in hopes of luring someone who actually has a student loan into responding.

Based on our investigative work, we've also seen evidence that they may also get people's personal information from large scale data breaches. Another method is social media. There's a wealth of information online (for example, Facebook groups at a college or university that students are part of) that scammers can use to conduct more targeted attacks.

[Ryan Traher] Tell us more about phishing scams.

[Rob Mancuso] A basic definition of phishing is that it is a type of online scam that targets consumers by sending them an e-mail that appears to be from a well-known source, such as an internet service provider, a bank, or loan servicing company. Phishing scams ask you to provide personal identifying information, and then they use your information to open new accounts, like credit cards or student loans in your name. Or they take over your existing accounts.

[Ryan Traher] So the bad actors are out there trying to lure college students and student loan borrowers into their traps through these scams. How can people avoid them?

[Rob Mancuso] First, beware of unsolicited phone calls, emails, texts, or social media messages from anyone claiming that they can help you obtain student loan forgiveness or help move your application through the process. The same goes for unsolicited offers to consolidate or refinance your loans for a fee. There's nothing these companies can do that you can't do for yourself—for free.

Second, protect your personal information and passwords, including your FSA ID. Don't share them with anyone—even people who say they work at a financial aid office or your student loan servicing company. No legitimate company would ever ask you for your FSA ID.

Third, don't click on links or attachments embedded in emails, particularly those from people or companies you don't know. You can hover your mouse over links to see where they are directing you. Also look for misspellings in the email address, body of the message, or in links. A common scam tactic is to use addresses that are almost, but not quite, identical to legitimate ones.

And finally, empower yourself by educating yourself! There are real Federal loan consolidation and forgiveness programs available through the U.S. Department of Education. So, if you want to lower your monthly loan payment, consolidate multiple Federal student loans, switch to a new repayment plan, or see if you qualify for loan forgiveness, empower yourself by contacting your student loan provider or the Federal Student Aid office directly and learning more about these programs. That doesn't take much time, and more importantly, it will help you protect your money and your personal information.

[Ryan Traher] Those are four great tips. Tell us about what is being done to stop these scammers.

[Rob Mancuso] Thankfully, a lot. Federal and State governments are taking actions to stop online scammers, including strengthening internet safety rules, and providing better tools to the public to fight cybercrime. Even within our own office, we participate on cyber task forces with other Federal, State, and local law enforcement agencies.

[Ryan Traher] Can you give us an example of the work you've done to stop scammers?

[Rob Mancuso] Absolutely. I'll share with you a case our office worked with the California Attorney General's Office—and it was a big case, involving millions of dollars. A debt relief business that called itself the Student Loan Relief Department contacted about 380,000 student loan borrowers promising to reduce or eliminate the borrower's student loans. They masqueraded themselves as a legitimate source of help and feigned association with the U.S. Department of Education to gain the loan holders' trust. Their scam was so convincing that the borrowers agreed not only to pay a fee of up to $1,300 that these borrowers thought was being applied towards reducing their student loan debt, but they also handed over their FSA ID, giving these criminals access to their personal information.

Many of these victims assumed that action was being taken on their student debt that many stopped making payments on their actual loans, which resulted in late payment notifications, increased loan balances, and sometimes, defaulting on their student loans. Thanks to our work and partnership with the California Attorney General's Office, we were able to hold these fraudsters accountable, and they were sentenced to prison and ordered to pay hundreds of thousands of dollars in restitution. But this is just one example of the type of fraud schemes that are out there.

[Ryan Traher]: Are there any other scams out there that target students or parents of that we should be aware of?

[Rob Mancuso]: Another education-related scam we've seen recently is in the area of scholarships. Criminals target students or their parents claiming that they have won a scholarship—a scholarship the student never applied for. The scammers may ask for your bank account number so they can put the scholarship money directly in your account, or ask for a credit card so they can cover the cost of shipping that check directly to you. Look—don't fall for this. No legitimate organization would randomly offer scholarships to students unsolicited, nor would they require your bank account number or credit card to get that award to you.

[Ryan Traher] Makes perfect sense.

[Rob Mancuso] Look, it's hard. College students or their parents are always looking for ways to help pay for college. Bad actors are preying on that. This is just one example. There are countless numbers of

scams out there with new ones popping up all the time. People—especially students—need to be aware of these efforts.

[Ryan Traher] What should someone do if they receive something that they think may be a scam?

[Rob Mancuso] The most important thing you can do is not respond! Don't fall for their sense of urgency. Don't respond until you have verified that the offer is legitimate. You can do this by calling Federal Student Aid, your school's financial aid office, or even your student loan servicer. Or you can take it upon yourself and look up the company online to see if there are complaints about the company.

[Ryan Traher] What do I do if I think I've been a victim of a scam?

[Rob Mancuso] Well Ryan, if you suspect that your personal information has been stolen as a result of a student loan scam, you really should take action quickly.

First, contact Federal Student Aid and your loan servicer to let them know about the situation.

Next, contact the credit reporting agencies and freeze your account so nobody else can open new credit accounts in your name.

And if you receive an email, text, or call that you believe is a scam, let us know! Contact the OIG fraud hotline at oighotline.ed.gov to report what you received.

[Ryan Traher]: So, Rob can you summarize for our listeners the three big things that they can do to protect themselves—their money, their personal information, or both—from student loan schemes and scams?

[Rob Mancuso]: Sure. Here are the big three!

1. **Be skeptical.** If something seems too good to be true, it normally is! Don't trust random or unsolicited emails, texts, and phone calls.
2. **Be knowledgeable.** Once you start being skeptical of things, it's important to be knowledgeable about what's going on and the types of fraud schemes out there. Knowing that criminals are out there trying to scam you will help you protect your money and your information.
3. **And lastly, act quickly.** Let's be honest, these scams are getting more and more sophisticated and any of us can fall for them. If you fall for one, it's important to know who to report it to and what actions to take, and we previously touched on what those actions would look like.

[Ryan Traher] You've given us a lot of great information here today, Rob. And for our listeners, everything that we have shared with you is available on our website as well as on our social media accounts, where we share information on new schemes and scams and highlight the results of our criminal investigations and other OIG work. So if you're not following us already, please be sure to do so! We're on Twitter and Facebook @EducationOIG and LinkedIn @Education-OIG.

Rob, thank you for being here today and talking with us about this important subject.

[Rob Mancuso] Thanks for having me, Ryan.

[Ryan Traher] And thanks to our audience for tuning in! Until next time, I'm Ryan Traher with the U.S. Department of Education Office of Inspector General, and this has been Eye on ED.

Guest Biography

Robert (Rob) Mancuso is the OIG's Assistant Inspector General for Investigation Services. In this position, Mancuso leads all OIG investigative operations, including information technology-based crimes and criminal activity. He has served in this position since January 2022 after having served as Assistant Inspector General for the OIG's Information Technology and Computer Crime Investigations (now OIG Technology Services).

Assistant Inspector General Mancuso began his Federal law enforcement career in 1998 with the Social Security Administration (SSA) OIG, where he helped to conceive, develop, and implement a project to identify weakness in SSA's death alert system, which ultimately identified millions of dollars in overpayments and projected savings to SSA. In 2001, Mancuso joined ED OIG as an investigator in its Washington Field Office and then served as an acting Desk Officer for a year. In 2004, Mancuso became a Program Manager and played an integral role in creating the ED OIG Computer Crime Investigation Division (CCID). In this position, Mancuso oversaw the transition and growth from CCID to the Technology Crimes Division, helped create the ED OIG Data Analysis and Referral Team, and supervised the investigation that led to the successful prosecution of the OIG's first unauthorized access (18 USC 1030) case.

In January 2008, Mancuso joined the U.S. Department of Transportation OIG where he helped start their Computer Crimes Unit, first as a Senior Computer Crimes Agent and then as its Assistant Special Agent in Charge. Mancuso re-joined ED OIG in August of 2015 as the Assistant Special Agent in Charge of the Technology Crimes Division and was shortly thereafter promoted to Special Agent in Charge.

Mancuso earned his Bachelor of Arts in Corporate Communications with a minor in Business from Elon College in North Carolina.