

Student Loan Fraud Alert TIPS FOR CONSUMERS, REGULATORS & SCHOOLS



In the United States, an identity fraud crime is committed every two seconds. A growing subset of these crimes – student loan fraud – is causing real harm to borrowers, financial institutions and schools of higher education.

STUDENT LOAN FRAUD AND IDENTITY THEFT CAN OCCUR IN THE FOLLOWING WAYS:

- First Party Fraud When the "victim" is or knows the suspect committing the student loan fraud. Typically, the alleged victim reports a fraudulent loan taken out in their name, but they have received the education funding and is involved in illegally benefitting from the loan proceeds.
 - **Third Party Fraud** A suspect steals a person's name, Social Security number, Federal Student Aid (FSA) ID and/or password and uses the stolen data to log into a FSA account to illegally secure a student loan for their own gain. Usually the borrower listed on the application is not attending any school.
- Synthetic Fraud A criminal creates a new FSA account with a fake mailing address. They apply for loans as a student of a particular university, drop out of school and keep the federal or private loan funds provided to fund higher education.

As student loan fraud techniques continue to evolve in sophistication and complexity, loan servicers and lenders are monitoring to find new ways to detect and prevent these crimes. While this fraud ultimately impacts the federal government or financial institution providing the loan funding, there is also a negative impact on institutions of higher learning, that can unknowingly accept fraudulent student applications, preventing legitimate students from gaining acceptance.

WHAT CONSUMERS SHOULD DO:

Protect Your FSA ID and Password – Only provide a Social Security number when absolutely necessary. Take precautions when entering usernames, PIN and passwords. Change your FSA ID and password if it may be compromised.

Keep Mail Secure – Mailboxes at college dorms and off campus housing are rarely secure enough for confidential mail. Consider using your parent's home address or secure P.O. Box instead.

Sign up for Credit Monitoring – Reach out to the three major credit reporting agencies – Experian, Equifax and TransUnion – for free credit monitoring. You can determine the type and frequency of alerts you'd like to receive.

Review Your Credit Report – Obtain a free credit report annually through your bank or at <u>AnnualCreditReport.com</u> to ensure fraud is not being committed in your name. If you find fraudulent loans, accounts or lines of credit, initiate a dispute with each credit agency along with each lender or financial institution directly.

If You Find a Fraudulent Loan in Your Name:

Immediately Contact Your School – If caught quickly, the school can cancel the fraudulent loan. Ask them to also cancel or close the Master Promissory Note to ensure no additional loans are taken out.

Contact the Student Loan Servicer – Alert the loan servicer to the fraudulent loan. They can grant temporary forbearance while the loan is under review.

Meet with a Financial Aid Professional at the College – Review the paper trail and understand the type of loan fraud you're dealing with. This information can help you report the crime and provide proof that you didn't apply for the loan.

File a Police Report – File a fraud/theft report with your local police department. Be sure to keep a copy of the report.

Report the Fraud to the Federal Government – Fill out a report on the Federal Trade Commission's <u>IdentityTheft.gov</u>. If the fraudulent loan is a federal student loan, also report it to the Department of Education's <u>Office of the Inspector General</u>.



Student Loan Fraud Alert TIPS FOR CONSUMERS, REGULATORS & SCHOOLS



WHAT REGULATORS SHOULD DO:

Pay Attention to Student Loan Fraud – This growing area of fraud has a big impact on student borrowers, their families, lenders and institutions of higher learning alike.

Work with Lenders and Law Enforcement – Coordinate efforts to go after those committing student loan fraud. Identifying and prosecuting those who commit this type of fraud is an important tool to discourage potential fraud.

WHAT SCHOOLS SHOULD DO:

Monitor for Unusual Application Activity – Signs like surges in FAFSA applications on the same day, increases in students applying past the deadline, or an influx of applications over a short period of time may indicate fraudulent applications. For colleges serving local communities, look for an unusual number of students enrolling from states across the country.

Watch for Unusual Funding – A sudden increase in students applying only for private student loans, not filling out a FAFSA and forgoing other typical financial aid opportunities may indicate fraud. Also, look for multiple students using the same accounts, the same cosigner being used on multiple accounts and a student/borrower showing up under multiple lenders.

Pay Attention to Unusual Academic Activity – Look for a rise in class withdrawals and absences, especially among students with private student loans, it may be student loan fraud at work. Encourage faculty to notice this activity and report it.

Issue a Campus-wide Alert – When you notice fraud trends on campus, alert students, admissions, the registrar, the IT Department, academics and school leadership right away.

Coordinate with Frequent Lenders – Develop relationships with the lenders servicing student loans to communicate about and identify emerging trends in student loan fraud.

Leverage Your IT Department – Investigate unusual student account activity, such as a single IP address creating or accessing multiple accounts. Spot check out-of-state address authenticity and increases in requests for school email addresses.

Notify Lenders When a Fraudulent Enrollee is Suspected – it's important to coordinate efforts so an investigation can begin right away.

The Student Loan Servicing Alliance (SLSA) is the nonprofit trade association that focuses exclusively on student loan servicing issues.

