

STOP STUDENT LOAN SCAMS

It's crucial for borrowers to be informed and vigilant

Student loan scams target individuals seeking financial aid for education. Fraudsters promise easy loans or debt forgiveness in exchange for upfront fees or personal information. Instead of providing genuine assistance, they disappear with the money and misuse students' personal data, causing financial losses and identity theft.

Student loan scams are widespread and growing. In March 2024, the [U.S. Federal Trade Commission \(FTC\)](#) announced it sent over \$4.1 million in refunds to 27,584 consumers who were victims of a student loan debt relief scam.

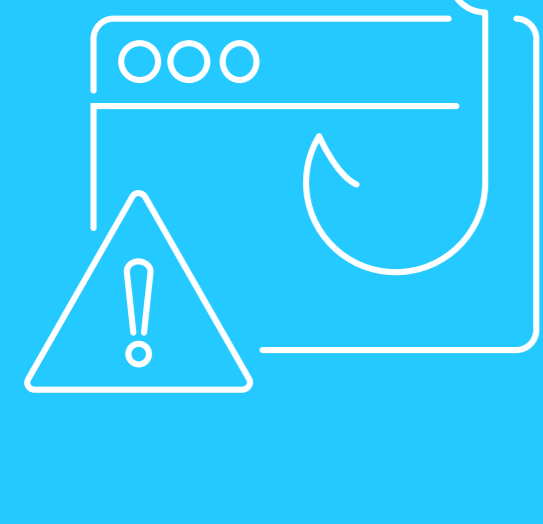
Student loans scams are a top 5 topic for scammers

They make up about 10% of all robocalls



Types of Student Loan Scams

Here are the most common types of student loan scams to watch out for:



Phishing scams

Fraudsters impersonate legitimate lenders, loan servicers, or government agencies. They make fake emails, phone calls, or websites to trick students into providing personal information such as social security numbers, bank account details, or login credentials. This information is then used for identity theft or other fraudulent activities.



False relief or forgiveness programs

Scammers offer fake programs that claim to fully erase or forgive student debt, tricking borrowers into paying upfront fees or providing personal information.



Debt relief scams

Scammers may promise to lower interest rates or monthly payments, but instead, they charge exorbitant fees and do little to help the borrower.

Red Flags of Student loan Scams

Recognizing the warning signs of student loan scams is key to avoid being scammed. Look out for:



Unsolicited communication:

Be wary of cold calls, emails, or messages claiming to offer student loan help

Requests for personal information:

Avoid providing sensitive personal information to unknown or unverified entities



Pressure tactics:

Scammers may use high-pressure sales tactics, such as claiming you must act quickly or risk losing out on an opportunity

Lack of official documentation:

If the service lacks transparency about their operations, affiliations, or credentials, it could be a warning sign. Legitimate programs will provide clear, written information about their services and policies



Requests for upfront fees:

Legitimate lenders and government agencies do not require upfront fees for assistance

Promises of immediate loan forgiveness:

Be wary of promises of immediate or guaranteed loan forgiveness. Legitimate loan forgiveness programs often have strict eligibility criteria and require a thorough application process



Tips to Avoid Student Loan Scams

- ✓ Don't respond to suspicious communications
- ✓ Verify the legitimacy of lenders and offers
- ✓ Never pay upfront fees for assistance
- ✓ Safeguard personal and financial information
- ✓ Understand what protections your financial institution (FI) offers
- ✓ Report suspected scams to authorities

Tips to Protect Customers from Being Scammed



FIs play a vital role in protecting customers from scams and fraud. By taking a proactive approach, they can shield customers from this growing threat and maintain trust and confidence. Some ways to strengthen fraud prevention include:

- ➡ Use typology-based fraud detection and prevention technologies to identify and stop scams in real time
- ➡ Have cutting-edge biometric data and dark web intelligence available for analysis
- ➡ Take a preventative approach that offers scam-specialized alert handling and customer risk triage
- ➡ Monitor and detect high-risk activities with purpose-built machine learning features

Explore how NICE Actimize protects your customers from student loan and other scams.

Safeguard Customer Assets >

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.