How International Students Can Avoid Tuition Payment Scams

As an international student, you are a natural target for scammers who will attempt to steal your tuition and educational payments. There have been several recent reported examples of students and their families being defrauded by individuals or organizations making false claims to have an affiliation with your university, offer you a tuition discount, a currency exchange discount, or make other promises. This is their attempt to confuse students before they are fully aware of their institution's official payment process. To avoid the risk of fraud and loss of your money, follow these best practices when making your tuition payment.

Take online security precautions

If paying your university online, make sure the website is secure. The address of any site you may use to share personal or financial information should begin with https (for example, https://www.flywire.com), which ensures the data you provide is protected through encryption. Avoid using public or unsecured Wi-Fi when sharing sensitive information. If you get an email from a suspected scammer, NEVER click on any hyperlinks.

Always verify who you are speaking to

Scammers may pose as a government agent and threaten to revoke your visa unless you send a payment to them immediately. They may request your personal information, which you should never disclose until you have verified that the requestor is an actual government agent authorized to do so. If you receive any communications from a person posing as a government agent, your first step must be to research whether their requests are valid.

Do not share your information

Credit card information, personal information (i.e., name, date of birth), and banking details should never be handed out to anyone without a contract or relationship with your university, and payment enablers that are not verified as authorized by your university should be ignored. These scammers may claim to have relationships with universities and colleges that do not exist, include fake testimonials from seemingly credible sources, show "official" documents with artificial co-branded university logos, etc.

Be careful of anyone asking for sensitive information

University officials should already know most of your details. This person may be fishing for your information to use fraudulently. As a best practice, always confirm with your university whether or not a payment processor is affiliated with them. It may help to check the institution payment website (e.g., by reviewing the payment portal and reviewing the "how to pay" section) to verify as an initial step.

Be wary of aggressive, suspicious characters

Is someone promising you a discount on your payment or volunteering to pay on your behalf? Be careful! If the offer seems too good to be true, then it probably is. If you take them up on their offer and share your personal, banking, or financial information and entrust them to pay on your behalf, you run the risk of losing your payment in full and set yourself up for further fraud risks later on. Fraudsters are very calculating; you could be approached on-campus, in a student visa application queue, or at an event for admitted students and their families in your home country.Even fellow students may be employed or rewarded by other payment processors having no affiliation with your school.

Report suspicious activity

If you suspect you are being targeted for fraud, you should note the information the scammer is attempting to get from you, stop communicating with them immediately, and report this to your university as well as the police.

Use Flywire

Flywire is the approved international payment processor at your institution and trusted at more than 1,600 institutions around the world. Our mission is to reduce the cost and hassle of sending your educational payments abroad by making sure your payment reaches your institution quickly and safely. Both you and your university will be able to track the status of your payment on Flywire's encrypted website.

Last but not least, check the university's website or reach out to administrators at the institution who can help verify the approved payment process. They can also identity the authenticity of someone requesting money or your personal information.

Start your university experience on the right foot — be smart and be safe.

flywire