Best Practices

Six steps to avoid payment scams.

There are many risks and unique challenges to consider as families prepare to send students abroad for international studies. Education institutions continue to report increases in unauthorized tuition payment companies (or individuals) stealing entire tuition payments from students. These scammers may even claim to have an affiliation with education institutions. To avoid the risk of fraudulent payment scams, consider these six steps when making tuition payments:

1 Take online security precautions

If you're paying your tuition 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, which ensures the data you provide is protected through encryption. Additionally, 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.

2 Don't share personal info

Never share personal information or login credentials with anyone, including those who offer to pay your tuition with a discount. Credit card information, personal information (i.e., name, date of birth), and banking details should also never be handed out to anyone without a contract or relationship with your university, and payment enablers that aren't verified as authorized by your university should be ignored. These scammers may claim to have relationships with universities and colleges that don't exist and show "official" documents with artificial co-branded institution logos.

Be careful of anyone that is asking you to provide sensitive information, as 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's payment website to verify as an initial step.

3 Always verify the requestor

Scammers may pose as a government agent and threaten to revoke your visa unless you send a payment to them immediately. They may also 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 is to research whether their requests are valid.

4 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, entrusting 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 in selecting their methods of introduction to international students—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.

An unwitting student may be offered a job, which involves asking the student to receive money into his/her bank account directly or via check and then being asked to transfer the money to another account, letting the student keep a portion as a commission. People recruited by criminals to help transfer stolen money are known as “money mules” and are enlisted online for what they think is legitimate employment, not aware that the money they are transferring is the product of crime. The real benefit to the criminals is not the work carried out by the mule, but that the criminals are distanced from the risky, visible transfer.

5 Always 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.

6 Use trusted payment providers

Flywire is the trusted payment provider for almost 2,000 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 institution will be able to track your payment on Flywire’s encrypted website.

Flywire has been solving complex payment problems for education institutions since 2009. Today, we continue to empower opportunities by connecting over a million students with almost 2,000 institutions to improve the payment experience worldwide. By combining our industry expertise with our powerful global payment network, Flywire s comprehensive receivables solution makes transactions faster, more secure, less expensive, and more transparent.

Learn more about Flywire at
www.flywire.com

flywire