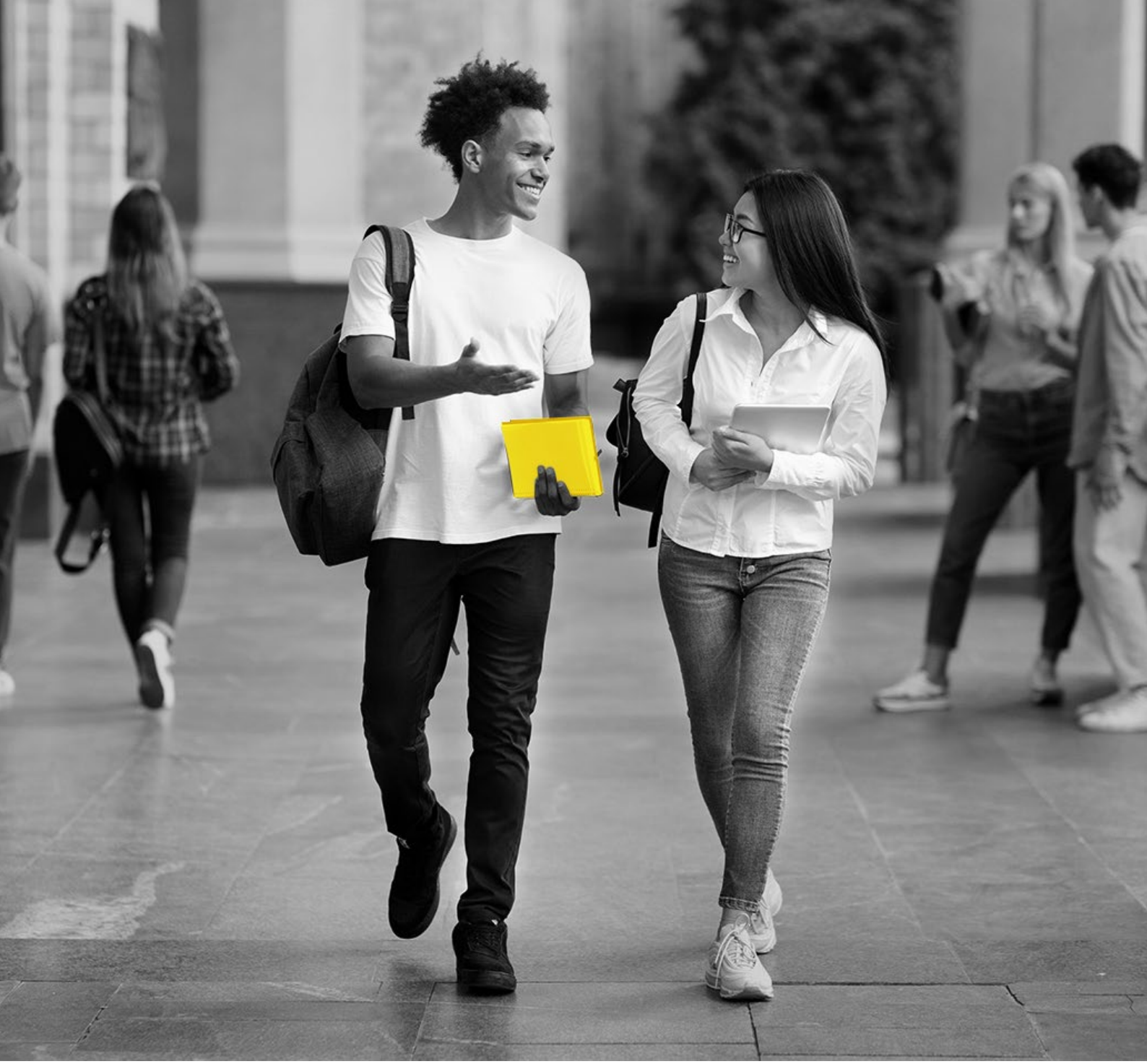
Always maintain vigilance.

And help defend your institution against fraud.

A guide for education institutions to help spot and prevent student refund fraud.

WesternUnion\WU | Business Solutions



At Western Union Business Solutions, we understand that handling student refunds is a standard function that many universities deal with on a regular basis. In most cases the university can refund money to a student directly back to the source in which it was paid, but there can be instances where this may not be possible. For example, the money may need to be sent back to the parent of the student instead, meaning the bank account details on record may not match and the university would need to collect the new beneficiary details. In these cases, universities should follow due diligence before processing a refund to make sure the request is legitimate, and they aren't facilitating a potential fraudulent attack. Alex Beavan, Head of Fraud Investigation at Western Union Business Solutions outlines what red flags universities should be aware of to help mitigate risk.

Examples of Fraudulent Scenarios

One of the more common frauds encountered by those processing payments is refund fraud, which in some instances is known as the transfer scam. In short it is a process of 'cleaning' monies from the proceeds or crime. Effectively it is getting the financial institutions involved to inadvertently money launder on behalf of the fraudster. The regulatory, reputational, and monetary implications of this are obvious but there are ways to mitigate.

Primarily all financial institutions should seek to refund monies back to the remitter. For instance where a student asks a university to refund the monies that have been 'sent in' on their behalf for student fees for example, this money should be sent (remitted) back to the bank account / debit card / credit card from whence it came. But in some instances that is not possible. Some of the reasons why the student may want the refund sent elsewhere could be for the purposes of crime. As such, it is important that we spot potential instances of such intent and conduct the relevant compliance checks to mitigate the risk.

Let us look at some examples of criminal intent in respect of refunds:

Scenario One

John Smith is a student studying at a university in the UK. He has been spoken to by a fraudster who wants him to process a payment to allegedly pay for his student fees. However, the bank account he will be using has been 'hacked' and any payments from that account will be unauthorised. The fraudster sorts the payment and it is processed successfully. However, the fraudster wants to get his hands on 'clean' money and asks John to organise a refund and get the university to send it to a bank account in the UK that the fraudster controls. The reason given for the refund is that the money belonged to a relative who has since died, and John needs to send it to the solicitor in the UK controlling the estate.

Scenario Two

Helen Parker is a fraudster who is controlling several students based at a university in the UK. She regularly gets them to refund payments she organises from stolen bank accounts and cheque accounts. She controls the accounts where the refunds go and pays the students a small fee for their trouble. Helen has made over £1million from this laundering ring. She targets one university because they do not check to see if the same email addresses are used, the same refund bank account is used and how many refunds students are doing.

Scenario Three

Simon Jones is a terrorist who is part of a right-wing group. He also dabbles in fraud and has access to many stolen credit cards. He uses one of those cards to pay for his university fees but then organises a refund to an account that his right-wing group controls. The university processes the payment and effectively cleans the money and pays it into the account of a terrorist group. This group then uses that money to plant a bomb on a tube.

As you can see these are examples from a simple fraudulent refund to the extreme of inadvertently funding terrorism. But these examples have taken place in various forms. They highlight the red flags that exist in respect of these scams, and what universities need to do to mitigate the risk.

Red flags to look out for before processing a refund

The following red flags may be seen in respect of refund frauds:

- Repeated refund requests by the same student.
- The excuse given for the refund request is vague and not able to be confirmed by anyone.
- The account name is highly unlikely to be the same family name as the student.
- The account where the money is asked to be refunded to is in another country and/or another name to the original remitter.
- The details of the account where the refund will be sent will also be vague about from the account name and number.
- The IP address and email address in respect of the email from who is trying to instigate the refund may not match those held in respect of the student.

To help mitigate the risk of such frauds it is vitally important that universities send the refund back to the original remitter's account. There may be circumstances where that is not possible, but in the first instance an attempt should be made to make such a transfer. In the unlikely event that this transfer is unsuccessful then a university should begin to check the circumstances of this student's refund request and see if any of the red flags above are noted. It is imperative that if there is any doubt as to the validity of the refund then the payment should not be made. Keeping proper records of previous refunds and contact details such as email address will help with any investigation.

If a university suspects that refund scams are taking place, then they should contact Law Enforcement and consider making a regulatory report to your regional financial intelligence unit such as the NCA in the UK.

Contact us now:

T: 01733 871 880*
E: clientqueriesеducation@westernunion.com
W: business.westernunion.com/education

Western Union WU | Business Solutions

Western Union Business Solutions accepts payments and provides foreign exchange services on behalf of its educational institution clients and not as a payment service provider for student payors.

This document is a financial promotion and has been prepared and approved by Western Union International Bank GmbH, UK Branch. The information contained within this document does not constitute financial advice or a financial recommendation, is general in nature and has been prepared without taking into account your objectives, financial situation or needs.

Western Union Business Solutions is a business unit of the Western Union Company and provides services in the UK through Western Union's wholly-owned subsidiary, Western Union International Bank GmbH, UK Branch (WUIB). WUIB (Branch Address: 200 Hammersmith Road, London, W6 7DL) is a branch of Western Union International Bank GmbH (registered in Austria, company number FN256184t, VAT Number ATU61347377, with its registered office at The Icon Vienna (Turm 24), Wiedner Gürtel 13, 1100 Vienna, Austria), which is licensed by the Austrian Financial Market Authority (Finanzmarktaufsicht). WUIB is subject to limited regulation by the UK Financial Conduct Authority and Prudential Regulation Authority. Details about the extent of WUIB's regulation by the Financial Conduct Authority and Prudential Regulation Authority are available from WUIB on request.

This document has been prepared solely for informational purposes and does not in any way create any binding obligations on either party. Relations between you and WUIB shall be governed by the applicable terms and conditions. No representations, warranties or conditions of any kind, express or implied, are made in this document. 579183516-2020-10