# BEWARE OF TUITION FEE FRAUD – DON'T BECOME A VICTIM

## What is Tuition Fee Fraud and how does it work?

Recently scammers have been reaching out to students to befriend them and tell them there is a way to reduce the cost of university tuition fees. They promise a discount or a better rate of exchange if you pay them – and claim in return they will pay your fees to Cranfield.

The person approaching you might be another student (studying at Cranfield or elsewhere) or could be a friend, 'cousin', 'uncle' or family acquaintance. They will offer to arrange a discount for you by paying on your behalf – either asking you to pay your money to someone else or make a payment through a website which may look completely genuine.

**Offers like these are usually part of a card scam, where payments are made to a student's university account using stolen cards.**

The person will make the payment towards your fees as agreed, so everything may seem legitimate at first. However, the payment will either be declined, or it will become reclaimed from Cranfield once it is realised that the payment card was stolen or cloned. The reclaim of the funds from Cranfield can be up to 120 days after the payment has been made.

**The result is that you have lost your money and unknowingly become involved in illegal activity. Your will still owe your Tuition Fees to Cranfield.**

To avoid such fraud, you should pay your fees directly to Cranfield using your own funds or credit cards. You can find details of how to do this here Make a payment (cranfield.ac.uk)

## Top tips to avoid being a victim of financial Fraud

1. **Never disclose security details, such as your PIN or full banking password:** banks and other trusted organisations will never ask you for these in an email, on the phone, by text or in writing. Unless you're 100% sure who you're talking to, don't disclose any personal or financial details. Always question uninvited approaches in case it's a scam. Instead, contact the company directly using a known email or phone number.
2. **Don't assume an email, social media message or a phone call is authentic:** just because someone knows your basic details (name, address, or your mother's maiden name) it does not mean they are genuine. Fraudsters may try to trick you by telling you that you've been a victim of fraud. **Remember**: the fraudster can make any telephone number appear on your phone handset, so even if you recognise the number or it seems authentic, **do not assume they are genuine**.
3. **Don't be rushed or pressured into making a decision:** under no circumstances would a bank or organisation a financial transaction on the

spot; they would **never** ask you to transfer money into another account for fraud reasons.

4. **Listen to your instincts:** if something feels wrong then it usually is right to question it. They may appear trustworthy, but they may not be who they claim to be.

5. **Stay in control:** have the confidence to refuse unusual requests for personal or financial information (such as . It's easy to feel embarrassed when faced with unexpected or complex conversations. It is ok to stop the discussion if you do not feel in control.

6. **Requests to move money:** A genuine bank or organisation will never contact you out of the blue to ask for your PIN, full password or to move money to another account. Only give out your personal or financial details to use a service that you have given your consent to, that you trust and that you are expecting to be contacted by.

7. **Clicking on links/files:** Don't be tricked into giving a fraudster access to your personal or financial details. Never automatically click on a link in an unexpected email or text.

8. **Money laundering/'money mules':** students will be targeted through adverts to earn quick and easy money but behind these are organised crime groups who want to 'borrow' your bank account and will be using you as a 'money mules'. They will use your account to transfer stolen money into it and back out again, often providing you with a cut of the cash for doing so. This means they have involved you in money laundering, a serious criminal offence with a maximum sentence of 14 years in prison. HM Revenue and Customs has published advice on how to protect yourself and what to do if you or someone you know has been approached.

9. **Only pay tuition fees directly to the university and not through third parties:** Remember if an offer or inducement seems too good to be true, it usually is. Do not be tricked into giving a fraudster access to your personal information (including university email address and log on details) or financial details. Never automatically click on a link in an unexpected email or text.

## What happens next

- If you have unfortunately been a victim of fraud, the funds that were transferred to Cranfield will be reclaimed by the bank or card provider. When this happens your student debt is re-instated, so you will still owe the university your tuition fees.

## What to do if you are a victim of fraud

- Tuition fee fraud is a crime committed against you the student, and you may decide to report this to the police. The University cannot report the matter for you, but support can be provided by the Student Support team (studentsupport@cranfield.ac.uk).

- You can report the crime to Action Fraud

- If you believe another Cranfield student to be involved in the fraud, then you should contact the Student Complaints team by email at studentcomplaints@cranfield.ac.uk to report the misconduct. Copies of emails and screen shots should be supplied, where available.

## Further information

Further information can be found at;

- Action Fraud – National Fraud & Cyber Crime Reporting Centre (UK)
  +44(0)300 123 2040
- Fraud, tricks and scams – VISA Fraud (UK Government guidance)
- UKCISA – Money Fraud (UK Council for International Student Affairs)
- DCPCU – Dedicated Card & Payment Crime Unit