Financial crime

Managing the risks of financial crime in the education sector

BARCLAYS

Contents

Introduction

All educational institutions – from universities and colleges to academies and private schools – are susceptible to financial crime in an ever-growing variety of forms.

The education sector attracts fraudsters and cyber criminals for two main reasons. Firstly, the sector is perceived as cash-rich, as evidenced by very visible multi-million investment in new facilities at many universities and private schools, while students are often assumed to have wealthy parents.

Secondly, education is generally regarded in the criminal world as a relatively 'soft touch'. While specialist finance teams working in the sector are increasingly aware of financial crime, this does not always extend to the wider education community of staff and students.

Employees of educational institutions are often viewed by criminals as a key stepping stone to penetrating their security. Fraudsters also increasingly prey on students – who, as typically young people often getting their first taste of independent life, are particularly vulnerable. This brings an added layer of responsibility for institutions.

In addition, in an increasingly global education market, UK educational institutions need to pay particular attention to the risks of involvement in high-risk jurisdictions, including sanctioned countries.

All of this requires institutions to have robust risk management policies and procedures in place to mitigate the risks of financial crime. Constant vigilance is needed to stay one step ahead of the criminals.

This report highlights a number of potential financial crime risks, or '**red flags**', that should alert institutions to the need to take action to mitigate those risks.

Banks' responsibilities

Quite rightly, the banking sector is under ongoing pressure to ensure it is not being used as a conduit for criminal proceeds or being abused, for example, to remit funds to terrorist groups. As well as their obligations to customers, the threat of significant damage to reputation through regulatory censure and fines (and ultimately potential loss of banking licence) is a strong motivator for all banks to manage financial crime risk. As one of the leading financial partners to the UK education sector, Barclays is committed to supporting institutions that can demonstrate they are managing risk appropriately.

Through our sector specialist relationship directors and financial crime experts we ensure that fraud awareness is on the agenda at all meetings with our education clients.

We hope that this guide provides your institution with valuable insight and empowers you to operate with confidence. Our aim is to raise awareness among leadership teams, staff and students, explain institutions' responsibilities and set out the actions they need to take to protect themselves. We hope that educational institutions will use this guide as a best practice resource as and when needed.

Barclays will continue to liaise with government and regulatory bodies to inform future legislation and provide guidance and support to clients both directly and through organisations such as the British Universities Finance Directors Group.

We look forward to working closely with our clients and industry specialists in 2020 and beyond.

Richard Ahern
Global Head of Financial Crime, Barclays Corporate Banking
richard.ahern@barclays.com

Richard Robinson
Head of Education, Barclays Corporate Banking
richard.robinson9@barclays.com

> Employees of educational institutions are often viewed by criminals as a key stepping stone to penetrating their security

Obligations for managing financial crime risks

Both educational institutions and their financial partners are subject to financial crime legislation.

The banking sector has been increasingly in the spotlight as governments attempt to fight financial crime. Banks have been increasing their due diligence requirements on their customers or reducing their appetite to support activity perceived as high risk in a proportionate and responsible way.

There is also an increasing trend towards public/private partnerships in the fight against financial crime. The financial services industry, universities, educational bodies, governments and regulators are working together to prevent the banking system from being used for criminal purposes.

Banks are now subject to enhanced regulatory obligations due to the potential for abuse of financial institutions by criminals, such as laundering and moving the proceeds of crime and funding terrorism.

Banks are obliged to carry out due diligence to gather information about their clients, including educational institutions, such as:

- Where they operate
- Who they deal with
- Who controls them
- Their sources of funds.

Institutions operating internationally, including in high-risk or sanctioned countries, may be asked to undertake enhanced due diligence. This may include requests to review governance policies, procedures and training materials used to manage financial crime risks.

Universities, colleges and schools should be aware of the regulatory framework and international guidance covering anti-money laundering (AML), anti-bribery and corruption (ABC), counter-terrorist financing (CTF), sanctions and export controls. All of these result in know your customer (KYC) requirements with which banks in the UK must comply to prevent criminals and terrorists accessing financial services.

Banks expect their customers to have due diligence processes in place to ensure both the bank and customer meet their regulatory obligations to prevent financial crime.

Educational institutions should bear in mind that while they might not be directly exposed to regulatory risk, their financial service provider might be – and any transactions which put a bank at risk of contravening its obligations might impact the services it is willing to provide to an educational institution on an ongoing basis.

Setting a financial crime policy framework

Educational institutions should have a comprehensive financial crime policy agreed by the senior management team to cover the legislation applicable to them and the operational and reputational risks they face.

Legislation

The role of a policy is to set an institution-wide, pre-determined course of action and risk limits. It is a guide to accepted organisational strategies, objectives and operating standards.

UK higher education institutions have obligations and legal requirements under the Companies Act 2006 and various financial crime acts and legislation. The financial crime legislation includes but is not limited to:

- Bribery and corruption – Bribery Act 2010
- Money laundering – Universities Act 2011 and obligations of banks under the Money Laundering Regulations 2017 and amendments applied under Money Laundering and Terrorist Financing (Amendment) Regulations 2019
- Terrorism – Terrorism Act 2000 and Proceeds of Crime Act 2002
- Sanctions – including UK, EU, UN and US sanctions regulations.

Effective policies

A financial crime policy should be a meaningful document which fundamentally guides the operations of an educational institution. Procedures (or operating frameworks) should provide the institution with clear and easily understood plans of action to implement the policy. Procedures should allocate responsibility and provide clear decision-making processes.

The policy should reflect an institution's risk appetite, objectives and operating standards.

Training

Employees need to be trained to ensure they fully understand what they need to do in order to be compliant with an institution's financial crime policy.

General training on financial crime should explain what typical criminal offences are, how they are committed, the usual criminal touchpoints with the institution and how it deals with these risks. It should also cover what is expected of employees and the process for reporting breaches.

Tailored training should be provided for specific groups – for example, those dealing with funds or operating internationally. All training should be monitored to ensure completion rates and effectiveness.

Employees need to be trained to ensure they fully understand what they need to do in order to be compliant

Risk-based approach

A risk-based approach can be used in setting the detail of the policy, procedures and training required. For example, staff operating in sanctioned countries will need to be significantly more aware of terrorist financing risk than UK-based staff and receive enhanced training.

Educational institutions need to keep up to date and abreast of emerging financial crime themes and threats targeting the sector. This can be through training and awareness programmes delivered by relevant industry bodies and through dialogue with financial partners.

Due diligence

Just as a bank must perform due diligence on the people and businesses it comes into contact with, so should an educational institution. Due diligence is key to mitigating financial crime and banks will expect appropriate and proportionate due diligence procedures to be in place.

Universities, colleges and schools therefore need to have risk-based processes in place to ensure they know enough about prospective students, beneficiaries, employees, volunteers, affiliated organisations, partners and suppliers. A risk-based approach means the greater the risks, the more due diligence required.

For example, educational institutions should know where student fees come from and why payments are routed in a particular way. They should know the people and organisations they work with and look out for unusual circumstances.

Institutions operating in or recruiting from sanctioned or otherwise high-risk countries must ensure they comply with applicable sanctions and export control laws. Additionally, dealing with a "politically exposed person" may create further financial crime risks, particularly corruption.

Institutions need to be comfortable that partners operating on their behalf are also acting in compliance with their regulatory obligations.

All due diligence procedures and reasons for decisions should be recorded.

A risk assessment should ask the following questions:

- What are the inherent risks to your institution?
- Who are you transacting with and how?
- What jurisdictions and regulatory environments are you operating in?
- What issues have been identified in the past and what are your institution's plans for the future?
- How are risks being mitigated and what controls should you have in place?
- What is your residual risk and is it within your institution's risk appetite?

Key financial crime risks for educational institutions

Money laundering

The amount of due diligence required to counter money laundering will vary depending on factors such as the nature of the activity, the involvement of third parties and the jurisdiction in which the institution operates.

Institutions should conduct risk assessments to identify whether they operate in high-risk areas and focus their risk mitigation processes on those jurisdictions. Due diligence also needs to be conducted on partners and employees on the ground in jurisdictions in which they operate in order to prevent funds from being diverted for terrorist or other criminal purposes.

Red flag: donations and sources of funds

Receiving large donations from anonymous donors is a potential red flag indicating possible money laundering. Institutions should have processes in place to mitigate this risk, such as establishing and documenting how the funds were raised, and why the donation is to be made anonymously.

Conditions attached to donations may be another red flag. Is the donor asking for money to be spent in a particular area for example?

Other sources of funds, such as legacies, trusts and bursaries, or funding for students who are the children of Politically Exposed Persons and/or sanctioned individuals may also create a money laundering risk.

> Institutions should conduct risk assessments to identify whether they operate in high-risk areas

Other red flags

Other red flags for potential money laundering include:

- All forms of third-party payments, whether by cash, credit card, inter-bank or cross-border transfers with no clear rationale or justification
- Use of complex company structures/shell companies to pay course fees
- Students paying course fees in full but then withdrawing from the course close to the start date or soon after, requesting a refund of fees
- Unusual or unexplained large payments (particularly in cash) being paid directly into an institution's bank account purporting to be tuition fees for a student
- Payments received in cash via a remote bank branch without prior notification
- Over-payment of course fees and subsequent request for a refund.

Bribery and corruption

Universities, colleges and schools need to ensure they have procedures in place to prevent bribery and corruption, for example when dealing with third parties that provide services on their behalf.

Bribery and corruption rules cover cash payments, gifts, travel, entertainment, training programmes, work experience, charitable contributions and sponsorships.

In most countries, it is a criminal offence to offer, promise, give, request, accept or agree to receive a bribe of any kind, in any form, either directly or indirectly. In the UK, the key legislation is the Bribery Act 2010. Additional local laws may be applicable, depending on the jurisdiction in which an institution operates.

The UK Financial Conduct Authority (FCA) can impose heavy fines on an educational institution for lack of sufficient anti-bribery and corruption controls. The FCA may take action for insufficient controls regardless of whether any bribery or corruption has actually taken place.

A culture of transparency and effective reporting lines is key to combating bribery and corruption, so that staff are encouraged to share relevant information they may become aware of with the relevant people within the institution.

Red flags

Red flags for potential bribery and corruption include:

- Third party payments received in settlement of invoices
- Unexpected interest in specific student applications from members of staff, or requests to circumvent normal application requirements
- Using third party agents to identify prospective new students from certain jurisdictions, such as Nigeria, Ghana, Russia and the former soviet states, Malaysia, Indonesia, Hong Kong and China
- An entirely non-face-to-face relationship with a student's parent
- Student fees coming from an account in a different jurisdiction to the student's country of origin.

Bribery and corruption risks may also arise where UK educational institutions have "associated" institutions overseas, typically structured as a franchise relationship, particularly in higher-risk jurisdictions where information on source of funds is more opaque.

Institutions should be particularly aware of the potential risks of providing bursaries, sharing resources with local state educational institutions or raising funds via development teams or parents' associations.

Other sources of funds, such as legacies, trusts and bursaries, or funding for students who are the children of Politically Exposed Persons and/or sanctioned individuals may also create a money laundering risk.

Sanctions and export controls

Economic sanctions can restrict dealings with certain individuals or entities, apply restrictive measures against a whole country, or control exports of particular products.

Sanctions are primarily introduced by the UK, EU, US or the United Nations Security Council, but can be introduced by any country. Institutions operating internationally should therefore be aware they may be subject to more than one set of rules.

Banks are often subject to sanction laws in multiple jurisdictions and institutions should be aware of the information a bank may require to ensure sanctions compliance.

Failure to comply with sanctions restrictions can have severe repercussions for UK educational institutions, including:

- Restrictions on business activity, e.g. loss of access to US markets
- Significant financial penalties
- Regulatory censure
- Civil and criminal charges.

Restricted persons

A key sanctions risk for educational institutions is inadvertently dealing directly or indirectly with a restricted person or entity. Indirect dealing includes when a third party is acting on behalf of the restricted person. Restricted persons include identified terrorists and criminals.

Educational institutions should not provide or make available services, funds or benefits to restricted individuals and entities. It is therefore vital that institutions check the names of donors, beneficiaries, suppliers and partners against restricted persons lists maintained by the relevant government authority (see useful contacts).

Banks will be concerned about facilitation risk, which would be a breach of sanctions law if the bank processes a payment on behalf of an educational institution that facilitates prohibited activity or benefits restricted persons.

Certain countries, including Iran, Syria, North Korea, Crimea, Cuba and Venezuela, are subject to broad sanctions and institutions should understand what activities are prohibited and take care that neighbouring countries are not used as a conduit to evade sanctions.

Students from sanctioned countries

UK educational institutions soliciting students or marketing themselves in a sanctioned country should consider who is providing those services in-country and whether they have undertaken appropriate due diligence on them.

Institutions engaged in exchange programmes with institutions in a sanctioned country should find out if they are government-owned or controlled and check whether export controls are in place.

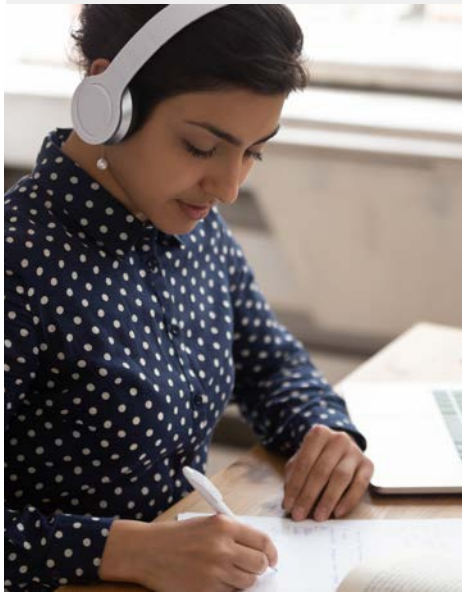
For students based in the UK who are a national of or normally resident in a sanctioned country, institutions should consider:

- Who is funding the student? For example, are they funded by a UK-based bursary or scholarship, or from other sources which do not involve the sanctioned country?
- The method of fee payment? For example, are these received from an individual located in a sanctioned country or from the student in the UK?
- What currency is being used?

Red flag: distance learning

Distance learning reduces the transparency of the recipient of course material, making it more difficult to ensure that institutions are not ultimately receiving funds from a sanctions target.

Where distance learning students are located in broadly restricted countries, banks may require pre-notification to ascertain whether they are able to facilitate payments. Approval will generally be considered on a case-by-case basis, subject to the information available.



Terrorist financing

Educational institutions are prohibited from facilitating any activity for UK Home Office Prescribed Terror Groups, which are banned by UK law. They also have a duty to disclose any known or suspected terrorist activity to the National Crime Agency (NCA). Under the Terrorism Act 2000 failure to disclose a known or suspected offence is a criminal offence.

Universities, colleges and schools therefore need to have controls in place to ensure they are not being used to launder money for terrorist purposes or to fund terrorism.

For example, where a UK educational institution uses a third-party agency in a high-risk jurisdiction to recruit students, the third party may embezzle money to fund a terrorist group and attempt to conceal this.

Due diligence processes, audit trails for money paid or for building works, for example, are essential to ensure that funds are used for their intended purpose.

On-campus activities organised by affiliated but not directly controlled entities like student societies can give rise to potential legal and reputational risks. Could these events be raising funds for terror purposes under the guise of a community group, club or society, for example? Events involving guest speakers, even if staged off-campus, may still create a risk where they are associated with the name of the institution.

Key financial crime risk mitigation measures

Institutions should have policies and procedures in place to help mitigate these risks, including:

- Ensuring that employees do not accept cash payments for student course fees, accommodation or living expenses.
- Only accepting payments by electronic means with a transparent and readily identifiable audit trail, e.g. bank-to-bank transfer or credit card.
- Always verifying sources of funds and obtaining appropriate evidence of the origin of those funds.
- Applying enhanced due diligence where funds originate from unknown third parties or shell companies.
- Adopting a continuous programme of training and awareness for both employees and students.
- Understanding the financial crime controls in place at any third-party service provider to the institution, in the context of the service provided, for example, an online payments service provider.

ABC University – a theoretical case study*

To illustrate the risks of financial crime, consider the example of a fictitious university called ABC University recruiting students from Afghanistan, Bangladesh, India, Pakistan and Syria. The university receives grant funding from numerous private foundations and corporations, as well as individuals, based in these jurisdictions.

The following mock scenario highlights a number of potential financial crime risks, or red flags, and the actions ABC University would need to take to manage those risks.

Scenario: Working with a local recruitment partner in Syria

ABC is using a third-party organisation to support the local recruitment of Syrian national students in Aleppo.

The third-party organisation has specifically requested payment in US dollars. In addition, the head of the third-party organisation is a director of a government education agency and, in exchange for supporting ABC, requests that it donates 12 laptop computers to the organisation.

Red flag: politically exposed person

There is a potential risk in this scenario that the third-party organisation is connected to a politically exposed person (PEP). The director's PEP status should be identified as part of ABC's due diligence checks.

Although the involvement of a PEP does not prohibit a donation, ABC should be aware there may be additional bribery, corruption and money laundering risks because the PEP is in a position of political influence. ABC should undertake due diligence to ensure that the PEP is not suspected of involvement with corruption.

Red flag: government connection

A further red flag is that the director of the organisation is a director of a government agency within Syria. There are a number of designated persons under UK/EU/USA sanctions legislation in the Government of Syria, and the Syrian Government itself is so designated. ABC should ensure the director is not designated and is not acting on behalf of the Government of Syria.

Red flag: request for donation

In relation to the suggested laptop donation, ABC should have effective internal controls to approve and monitor donations, understand the position around the use of the laptops, and confirm the project complies with US and EU sanctions and anti-bribery and corruption law.

Issues to consider include:

- Are there any export control issues relating to the laptop technology?
- What will the laptops be used for? If laptops are supplied and misused in Syria, then ABC may face regulatory censure
- Is the activity dependent on the donation of the laptops? ABC should ensure that the donation does not amount to a bribe.

*"ABC University" is not in reference to any real institution, for the purpose of this document.

Case study: ABC University continued

Red flag: dollar payments

Sending funds in US dollars to Syria is currently subject to US sanctions, even if the funds are sent from the UK, as most major banks will route dollar payments through a US branch or correspondent bank. As such, ABC needs to understand its sanctions compliance (both in the UK and USA), gain appropriate approvals from sanctions authorities (if required and available), and liaise with its bank for approval to send the funds.

Key takeaways:

Questions to consider

1. Do you have a financial crime policy and is it robust enough?
2. How do you assess the financial crime risks associated with your activities and how are these risks mitigated? Is any residual risk within your organisation's risk appetite?
3. What day-to-day monitoring, oversight or controls do you have in place over your operations to prevent financial crime?
4. Do you consider all of the following risks in addition to fraud risk?
   - Money laundering
   - Terrorist financing
   - Economic sanctions
   - Bribery and corruption
   - Export controls.
5. What training and guidance do you provide to your staff to ensure understanding and compliance with your financial crime policy, particularly for those dealing with high-risk jurisdictions?
6. Do you understand the risks involved in the different jurisdictions in which you operate?
7. If you operate through partners, what due diligence do you undertake on them to ensure they are operating to your standards? What ongoing monitoring do you have in place?
8. What are your sources of funding and payment and what due diligence do you undertake on those sources? Does your due diligence consider:
   - Country of origin and associated risk
   - Government funding – where the institution is working with government agencies, what additional checks are undertaken to satisfy anti-bribery and corruption regulations?
   - Student fees – how do you verify the sources of student fee payments and screen them to avoid financial crime?

Guidance for employees on cyber fraud

Employees of universities, colleges and schools are often targeted by cyber criminals, who see them as an easy way to penetrate the security of the institution in order to commit various forms of fraud. The key types of financial crime targeted at employees are outlined below.

CEO impersonation fraud

CEO impersonation fraud usually involves criminals sending a request – by email, letter or phone – that purports to come from a senior person within an organisation. These are typically sent to the accounts department, requesting an urgent payment to a supplier or partner.

Fraudsters can spoof email addresses to make them appear to be from a genuine contact, including someone from within an institution.

This type of fraud often occurs when the senior person in question is out of the office and may instruct the recipient that the transaction is urgent, confidential or sensitive in order to discourage verification.

All staff should be made aware of this type of fraud and measures to prevent it, including:

- Ensuring that any payment requests with new or amended bank details received by email, letter or phone are independently verified, including internal emails from senior management.
- Ensuring that staff are not pressured by urgent requests, even if they appear to originate from someone senior.
- Being cautious about how much information is revealed about the institution and key officials via social media platforms and out-of-office automated replies.
- Considering removing information such as testimonials from an institution's or a suppliers' websites or social media channels that can help fraudsters identify an institution's supplier.

Phishing

Phishing is an email-based fraud that involves criminals, posing as legitimate sources, sending emails that aim to trick people into divulging sensitive information or transferring money into other accounts.

Alternatively, phishing emails may be designed to contain and deliver malware via an attachment or a link. If the link is clicked or the attachment opened, the criminal may then be able to gain access to an institution's IT system.

Fraudsters are skilled at collecting enough information about employees and their institutions and can spoof email addresses to make them appear to be from a genuine contact, including someone from within the institution.

All staff should be made aware of this type of fraud, particularly those that make payments, and measures that can help prevent it, including:

- Being alert to the style, tone and grammar of emails received, especially where the email doesn't address the recipient by name.
- Never entering any personal or security information on a website accessed through a link in an email.
- Never clicking on links or opening attachments from unknown senders.
- Checking that website addresses for sites requesting sensitive information contain 'https' – the 's' stands for 'secure', although this does not guarantee the website is genuine.
- Never assuming that a sender is genuine because they know information about the recipient or the institution or the email address looks familiar.
- Being aware that a bank will never ask for a full password or PIN, provide details to make a payment or request access to an IT systems or individual PC.

Anyone receiving a suspicious email purporting to be from Barclays should forward it to internetsecurity@barclays.co.uk and then delete it straight away.

Telephone fraud and vishing

This type of fraud involves criminals using personal data and psychological manipulation to convince members of staff to either transfer money, or hand over confidential information which can be used to access funds later on. Fraudsters may pretend to be from the police, utility providers, delivery companies or a bank.

To make these scams more convincing, fraudsters may use specific information about an institution, such as a manager's name or recent activities, that they have discovered online.

All staff should be made aware of this type of fraud and guidance on spotting it, including:

- Immediately terminating a phone call if it arouses suspicion. The best way to check whether a call is legitimate is to talk to a trusted contact at the organisation – using a different phone, as the fraudster can sometimes keep the original line open.
- Never assuming a caller is genuine because they know information about the institution or an individual employee.
- Being aware that a bank will never send texts that link to online banking log-in pages or ask for confirmation of account or security details.
- Remembering that a bank will never ask for a full password, PIN, payment authorisation codes, or provide details to make a payment, or request access to an institution's IT system or an individual PC.

Key takeaways:

Questions to consider

1. Does your institution's financial crime policy recognise that employees of universities, colleges and schools are specifically targeted by cyber criminals?
2. Is there easy-to-access general guidance available to employees on their responsibilities to help prevent financial crime?
3. Are employees aware of CEO fraud? Does your institute have policies and best-practice measures to help prevent it?
4. Do you warn employees about phishing fraud? Do they know what steps to take to guard against this threat?
5. Have you told employees what telephone and vishing scams are – and how to spot them?

Protecting students from financial scams

Students can be particularly vulnerable to financial crime scams, especially those experiencing life away from home and the guidance of parents for the first time. To help keep students safe, it is vitally important to raise their awareness of financial crime risks.

Internet security

Students should be aware that their personal data can be at risk through the use of smartphones, laptops and other digital devices connected to the internet, whether for study or social activity. This exposes them to the threat of fraud and scams. This risk is increased when they use free Wi-Fi, for example in cafés or public space, where any security weakness in the Wi-Fi network could be exploited by criminals to intercept their data.

Phishing and vishing

Students are often targets for both phishing (emails) and vishing (phone calls), with fraudsters often posing as their bank or some other official body. The advice for students to avoid these scams is the same as that for employees of educational institutions (see Guidance for employees).

A typical phone scam might involve a fraudster calling about a refund or problem with a payment card. They may ask the student to confirm their security and bank account details, supposedly to resolve the issue, and then use these details to take payments from the student's account.

Another common scenario is fake technical support impersonators claiming they have detected a fault with a student's laptop computer and seeking remote access to fix the problem. They may suggest the student needs to buy a piece of software straightaway to solve the problem. Students should be made aware that such out-of-the blue calls are unlikely to be legitimate, so if they're unsure of a caller's credibility, they should hang up.

Online shopping scams

The popularity of booking tickets, getting student discounts from restaurants or buying course books online makes it easier for fraudsters to advertise fake products or services that may never arrive once the student had paid. Some tips to help students avoid this type of scam include:

- Taking care to research a private seller or even a legitimate-looking brand, for example by reviewing other customer's feedback
- Never opening a link in an unexpected email.
- Checking URLs or email addresses of unsolicited emails, including the spelling, to make sure they are genuine – for example, barcleys-bank.co.uk is incorrect; the correct URL is barclays.co.uk.
- Insisting on viewing high-value items like vehicles in person before paying.
- Using secure payment methods rather than direct bank transfers.

Students should be aware that their personal data can be at risk through the use of smartphones, laptops and other digital devices connected to the internet

Accommodation scams

Rented accommodation is another area where criminals can take advantage of students. Typically, fraudsters might advertise a property that belongs to someone else – or even a property that doesn't exist at all. They may make excuses as to why the student can't view the property but insist on rent or a deposit up front, promising to forward keys via a courier service, which then never arrive.

To avoid falling victim to this kind of scam, students should:

- Only use reputable high street rental agents and always view a property inside and out before entering into any agreement or parting with any money.
- Ask to see legally required documents such as energy performance and gas safety certificates.
- Check that the rent is typical of properties in the area – if it seems too good to be true, it probably is.

Money muling

The 'money mule' trap involves students being offered payment in exchange for receiving money temporarily into their bank account. They will then be asked to withdraw the cash to hand over or transfer it on. This type of scam is on the increase, targeting students who are short of cash and may be tempted by offers to make 'easy money' on job search or social media websites.

Allowing their bank account to be used in this way is illegal and could land students with a criminal record or even a prison sentence. Students caught up in money muling are also likely to have problems opening a new bank account or obtaining credit in the future.

Advice to students to help avoid involvement in money muling includes:

- Being wary of unsolicited offers to make 'easy money'
- Researching companies offering such 'job' opportunities and making sure their contact details are genuine
- Being especially cautious of 'job offers' from overseas as it will be harder to check whether they are legitimate.

Fee payment scams

Another fraud targeting students, particularly overseas students, focuses on tuition fee payments. Criminals may present themselves as a government agency and request payment for an "international student tariff", in some cases even threatening to revoke a student's visa if the payment is not made.

In other cases, fraudsters may create a fake email which appears to be from a genuine UK educational institution, requesting payment for fees or informing a student of a change in bank account details to pay fees.

To avoid this type of scam, students should:

- Be wary of anyone who offers to make a tuition payment on their behalf.
- Avoid companies advertising tuition payment services that are not endorsed by the institution.
- Look for warning signs that an agent is not legitimate, such as requests for large upfront payments, offers to create false documents, refusal to provide references or charging fees for services that an educational institution provides for free, for example, accommodation support.
- Not share personal, banking or financial information with anyone who lacks a verifiable relationship with the relevant institution.

Key takeaways:

Questions to consider

1. Does your institution's financial crime policy recognise that students of universities, colleges and schools are particularly vulnerable to financial crime scams?
2. Is there easy-to-access general guidance available to students, and their parents, on the potential threat posed by fraudsters?
3. Are all students made aware that their personal data is potentially at risk when online?
4. What measures can your institution take to make internet access secure on campus?
5. Does your institution explain to students the potential threat from phishing and vishing fraud?
6. Do students understand that they could be vulnerable to online shopping scams?
7. Do you warn students about accommodation scams? Can you work with genuine accommodation suppliers to tackle this threat?
8. Are your students attending your institution made aware of money muling?
9. Your students should know about possible fee payments scams – do you provide guidance on this topic?
10. What support is in place at your institution for those students who fall foul of any of the above financial crimes?

Working in partnership with your bank

We recommend that universities, colleges and schools should work closely with their bank and keep them up to date on how they are managing and mitigating financial crime risks.

Institutions that are the victims of security breaches, fraudulent activity or any type of scam should notify their bank as soon as possible.

Transparency and early involvement of a bank is particularly important for institutions operating in high-risk or sanctioned countries.

At Barclays, our specialist education sector relationship managers and financial crime experts have a great deal of experience in understanding the unique challenges facing educational institutions. They can provide invaluable support on effective financial crime policies, mitigation procedures, due diligence processes and staff training.

Useful information

Anti-bribery and corruption (ABC)

uk.gov - anti-bribery policy

https://www.gov.uk/anti-bribery-policy

Bribery Act 2010 guidance

https://www.gov.uk/government/publications/bribery-act-2010-guidance

UK anti-corruption strategy 2017 to 2022

https://www.gov.uk/government/publications/uk-anti-corruption-strategy-2017-to-2022

Foreign Corrupt Practices Act (US Department of Justice)

https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act

Anti-money laundering (AML)

Crown Prosecution Service: Proceeds Of Crime Act 2002 Part 7 - money laundering offences

https://www.cps.gov.uk/legal-guidance/proceeds-crime-act-2002-part-7-money-laundering-offences

Independent Schools' Bursars Association money laundering guidance

https://www.theisba.org.uk/news/2019/isba-publishes-revised-anti-money-laundering- guidance.aspx

High- risk jurisdictions

EU list of non-cooperative jurisdictions

https://www.consilium.europa.eu/en/policies/eu-list-of-non-cooperative-jurisdictions

Financial Secrecy Index

https://www.financialsecrecyindex.com

Financial Action Task Force list of high-risk and other monitored jurisdictions

http://www.fatf-gafi.org/countries/#high-risk

Department for International Trade

https://www.gov.uk/government/organisations/department-for-international-trade

Export controls

Department for International Trade

https://www.gov.uk/government/organisations/department-for-international-trade

Export Control Joint Unit

https://www.gov.uk/government/organisations/export-control-organisation

Overview of US Export Control System

https://www.state.gov/strategictrade/overview/

Sanctions

European Sanctions blog

https://europeansanctions.com/

European Sanctions map and guidance

https://www.sanctionsmap.eu/#/main

Sanctions, embargoes and restrictions

https://www.gov.uk/guidance/sanctions-embargoes-and-restrictions

HM Treasury Office of Financial Sanctions Implementation (OFSI

https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation

Office of Financial Sanctions Implementation (OFSI) licences

https://www.gov.uk/guidance/licences-that-allow-activity-prohibited-by-financial-sanctions

Terrorist financing

The Crown Prosecution Service: Terrorism

https://www.cps.gov.uk/terrorism

Terrorism Act 2000

http://www.legislation.gov.uk/ukpga/2000/11

Terrorism Act 2000 Part III Terrorist Property

https://www.legislation.gov.uk/ukpga/2000/11/part/III

Current list of designated persons, terrorism and terrorist financing

https://www.gov.uk/government/publications/current-list-of-designated-persons-terrorism-and-terrorist-financing

US Department of the Treasury

https://www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/default.aspx

Financial Action Task Force (FATF): Terrorist Financing

http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf

barclayscorporate.com

@BarclaysCorp

Barclays Corporate Banking