McLarens

Universities under attack: why authorised push payment fraud is becoming a growing cyber risk

Universities have long been viewed as attractive cyber targets. They hold large volumes of sensitive data, operate complex IT systems and process millions of pounds of payments each year. Yet while ransomware and data breaches often dominate the headlines, another threat is gathering pace: authorised push payment (APP) fraud.

Rather than exploiting technical vulnerabilities alone, APP fraud targets people and processes. By compromising email accounts, manipulating invoices or impersonating trusted colleagues, criminals persuade organisations to transfer money willingly into fraudulent accounts. For insurers, educational institutions and claims professionals alike, it is becoming an increasingly important area of cyber risk.

A different kind of cyber attack

A typical scenario begins with a compromised email account. Fraudsters monitor conversations between finance teams and suppliers before intervening at precisely the right moment. An invoice is intercepted, legitimate bank details are replaced with fraudulent ones, and payment is made to an account controlled by criminals.

In one claim McLarens handled, a university lost hundreds of thousands of pounds after finance staff unknowingly communicated with hackers through a compromised internal email account. Authorisations appeared genuine, payment instructions were approved, and the transfers were made.

These are not isolated incidents. Business email compromise attacks have been rising steadily for several years, and the rapid adoption of generative AI is making them harder to detect.

Why universities are exposed

Educational institutions present a combination of characteristics that make them attractive targets.

Many continue to operate legacy technology alongside newer digital platforms. Procurement, research funding, supplier management and payroll often span multiple departments, campuses and systems. Large finance teams process significant transaction volumes, while universities regularly make substantial payments to research partners, contractors and suppliers throughout the year.

The nature of university funding can also create opportunities for criminals. Research grants, capital projects and collaborative programmes frequently involve high-value payments, sometimes with changing suppliers or banking arrangements. Those legitimate changes provide cover for fraudulent ones.

The risk is not confined to universities. Independent schools face similar challenges, particularly around fee collection. McLarens has seen cases where hackers compromised finance email accounts before sending parents revised payment instructions offering discounts for early settlement.

The human factor remains the weakest link

Many successful APP frauds rely on social engineering rather than sophisticated hacking. Criminals exploit trust, urgency and routine. An email appears to come from a colleague. A phone call seems to be from a senior executive. Increasingly, AI-generated audio and video 'deepfakes' can reinforce that deception.

In some cases, employees simply fail to follow established procedures. In others, compromised or coerced staff can inadvertently enable criminal activity by providing access to systems or credentials.

More broadly, the latest Cifas Fraudscape 2026 report shows fraud becoming increasingly sophisticated across every sector. A record 444,993 fraud risk cases were recorded in the UK's National Fraud Database during 2025, a 6% increase on the previous year. Together, identity fraud and account takeover accounted for almost three-quarters (72%) of all cases recorded. Combined with the growing availability of generative AI tools capable of producing convincing emails, invoices and supporting documentation, the findings reinforce a broader shift towards fraud that exploits trusted relationships rather than technical vulnerabilities alone.

That trend closely mirrors McLarens' own experience. In 2024, McLarens' fraud team reported a 300% increase in suspected fake documents submitted for analysis across its UK & Ireland business over an 18-month period, including manipulated invoices, bank statements, identity documents and deepfake audio and video. As AI-generated fraud becomes more sophisticated, organisations are finding that traditional checks alone are no longer enough to identify increasingly convincing attempts at deception.

Processes matter as much as technology

Ultimately, robust payment controls remain one of the most effective defences against APP fraud.

Independent validation through a known telephone number, confirmation via established contacts, or use of account verification services should become standard practice for significant payments.

Equally important is ensuring that staff feel able to report mistakes immediately. Delayed reporting after clicking on a phishing link can provide attackers with valuable time inside a network before security teams become aware of the compromise.

Fighting AI with AI

The same technology making fraud more sophisticated can also strengthen organisations' defences.

In response to the growing sophistication of AI-enabled fraud, McLarens has expanded its fraud investigation training and is trialling AI-powered document analysis technology to complement traditional forensic investigation. Rather than replacing experienced investigators, these tools help identify subtle inconsistencies, analyse metadata and detect signs of digital manipulation that may otherwise go unnoticed.

That reflects a broader reality facing organisations across every sector. As AI lowers the barriers to producing convincing fake invoices, contracts and payment requests, manual checks alone are becoming increasingly difficult.

An evolving challenge

For insurers, APP fraud illustrates how cyber risk continues to evolve beyond technology alone. Coverage may sit within dedicated cyber policies, crime policies or hybrid products, but the underlying drivers increasingly centre on governance, human behaviour and operational resilience.

For universities and other educational institutions, staff awareness, disciplined payment processes and independent verification remain essential.

Authors

Brendan Gillooly
Head of Investigation

+44 (0)7771 524716
brendan.gillooly@mclarens.com

Nigel Collins
Cyber, Technology and Engineering Lead

+44 75 0311 9154
nigel.collins@mclarens.com