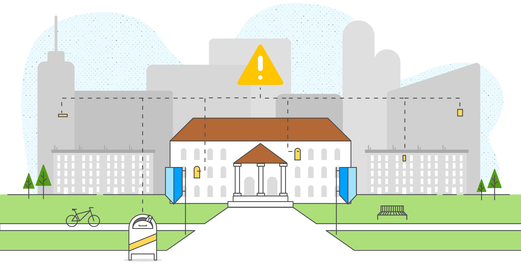
HOW TO STOP HIGHER EDUCATION AP FRAUD

Payment fraud is everywhere and impacts every kind of organization, including academia. In higher education, large payment runs to vendors and student refunds run up against antiquated Accounts Payable processes and technology, creating a heightened risk of payment fraud. The impacts can be significant, with ACFE estimating a median loss of $100,000 to fraud incidents.

Take a closer look at types of fraud your AP department is most likely to be impacted by and what you can do now to reduce your exposure.



#1 FRAUDULENT VENDOR & STUDENT ENROLLMENTS

RISK

Fraudulent actors will attempt to bill you and/or get enrolled in your payment network of choice by providing false bank account details and other financial data.

PREVENTION

Work with a partner who can **spot red flags and anomalies in data** to shut out those trying to fraudulently enroll, **using behavioral analytics and machine learning** as a bulwark.

#2 CREDENTIAL THEFT & ACCOUNT COMPROMISE

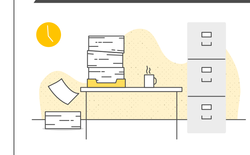
RISK

Bad actors use Business Email Compromise and other **schemes to steal email and account credentials** in attempt to divert funds to their own bank accounts, preying on a lack of vigilance and security.

PREVENTION

Installing **multi-factor authentication** on every step of an account change—and setting permissions so only specific users can make those updates in the first place—is an excellent way to **block out these fraud attempts**.

#3 FRAUDULENT INVOICES



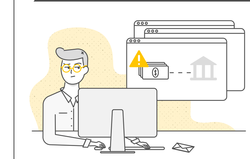
RISK

Verifying vendor identity and invoice validity is critical. A Lloyds Bank survey found **52% of businesses globally had experienced attempted invoice fraud** in 2019, underscoring the need to verify who you're paying.

PREVENTION

Onboard as many of your suppliers as possible via a **secure network**, so you always know who you're paying. If the details don't match, you're not making a payment, cutting down on complexity and the number of approvers needed.

#4 IN-HOUSE FRAUD



RISK

Every organization has to worry about **embezzlement and other in-house schemes**. Reputational and monetary costs can be huge.

PREVENTION

Setting proper permissions for invoice and payment processing cuts the risk significantly, especially if payments above a certain threshold need additional signoff every time.

#5 INTERCEPTED & MISROUTED PAYMENTS

RISK

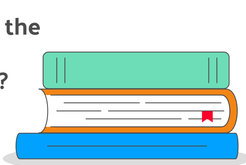
Even after all your careful work, **checks can be intercepted and payments can be misrouted** if you haven't verified who you're paying. This kind of fraud is now easier to perpetrate with remote staff.

PREVENTION

Take all the steps we've already outlined and **switch all your payments to digital** (such as virtual card, ACH, or push to debit) and your chance of **accidentally sending a payment** to a fraudster **drops close to zero**.

Looking to understand the scope of invoice and payment fraud in 2020?

READ OUR REPORT



Fraud prevention tips for higher education brought to you by Paymode-X

Powered by Bottomline