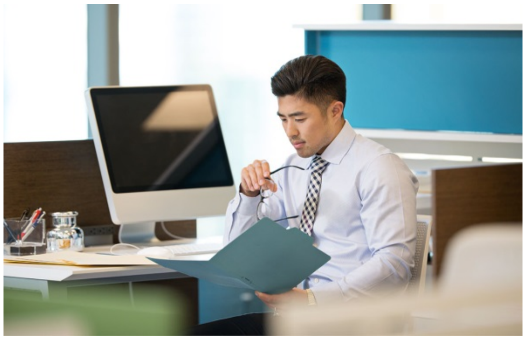
# How one company stopped vendor impostor fraud



In July of 2016, McGraw-Hill Education's accounts payable department received an invoice that seemed to come from one of its vendors.
The invoice was sent from the vendor's email address to the correct contact in the AP department.

The contact also received a follow-up fax from the vendor to confirm changes to the settlement instructions.

But the invoice wasn't from the vendor – a fraudster had stolen an invoice and attempted to redirect the payment.

"They actually used multiple layers of fraud to make it look that much more realistic," said Brian Richter, vice president and assistant treasurer of McGraw-Hill Education. The company provides a variety of educational tools, from textbooks to digital platforms.

Fortunately, McGraw-Hill Education recognized the invoice as fraudulent and didn't send a payment.

"We caught it because I don't allow anyone in accounts payables to alter vendor settlement instructions without a secondary authentication from the vendor," Richter said.

The company's response to the incident demonstrates how a strong, layered approach can help businesses protect themselves from vendor impostor fraud.

## Keeping an eye on vendor files

When McGraw-Hill Education received the fraudulent invoice, the changes to the settlement instructions raised red flags.

A dedicated team contacted the vendor directly to verify the changes. After speaking with the vendor, the team realized the invoice had come from an impostor.

Vendor files are a major target for fraudsters. Richter recommends that companies limit access to vendor files and train a specific team to handle all vendor file updates. McGraw-Hill Education also requires two approvers to make any changes to settlement instructions.

## Taking the next steps to stop fraud

After McGraw-Hill Education realized their vendor hadn't sent the invoice, Richter notified the appropriate authorities about the fraud attempt. He contacted a cybersecurity team in the United Kingdom and the bank where the fraudster tried to redirect the payment.

McGraw-Hill Education also emailed vendors to educate them about procedures for changing an address or settlement instructions. Vendors are never asked to make changes directly to an invoice. Those requests come separately in letters mailed to vendors, and they can contact McGraw-Hill Education directly to confirm any changes.

Richter is also looking at additional layers of security to stop vendor impostor fraud. In the future, vendors may be required to submit a bank letter to verify the account in their payment instructions.

Fraudsters are becoming more sophisticated about circumventing fraud protection measures, so it's critical for businesses to educate employees thoroughly, Richter said.

"If your employees don't understand why you have the policy and why you take the steps that you're taking, they won't be able to go to the next level to really understand what they're looking for and assess if this is a possible risk," he said.

## Takeaways for avoiding impostor fraud

As fraudsters use various fraud tactics, it's even more important that security measures include a multi-layered approach. McGraw-Hill Education caught a fraudulent invoice from an impostor posing as a vendor by:

- Flagging invoices with changes to settlement instructions, address changes or contact information
- Training a dedicated team to verify changes to vendor files
- Verifying changes directly with vendors, using contact information on file
- Limiting employees who have access to vendor files
- Reporting fraud to the appropriate authorities
- Educating customers about procedures for changes to invoices
- Educating employees about how to identify fraud

In addition, Wells Fargo recommends the following best practices:

- Using dual custody to verify details before payments are sent
- Monitoring accounts for unusual activity

For more information and resources to help safeguard your business from fraud, check out other Wells Fargo's Treasury Insights and the Fight Fraud websites. If you suspect fraud, contact your Wells Fargo representative, or call 1-888-937-9997, Monday through Friday, 5:00 a.m. to 7:00 p.m. Pacific Time, and ask to have a Wells Fargo Dealer Services Commercial Relationship Manager in your area contact you.