

AP Fraud Bootcamp: Crowd-Sourced Cases & Expert Solutions

Presented by:

Debra R Richardson, MBA, CFE,
APM, APPM, CPRS



November 2026 | JW Marriott Austin | Austin, TX



Do you need NASBA CPE credits?

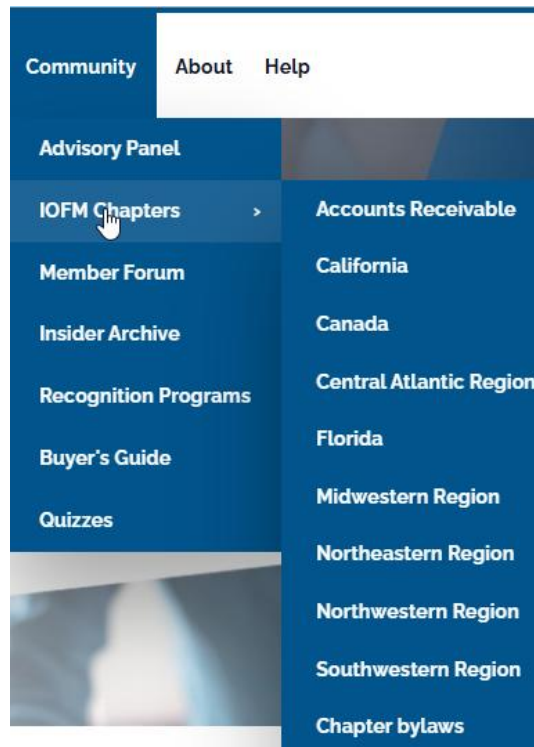
- Navigate to website: iofm.cnf.io
or scan the QR code →
- Check-in and check-out of your sessions to track your attendance for NASBA CPEs
- Certified with IOFM? No need to check-in and out of sessions. Self-report CEUs on IOFM.com instead after the event!



November 2026 | JW Marriott Austin | Austin, TX



Do You Belong to an IOFM Chapter?



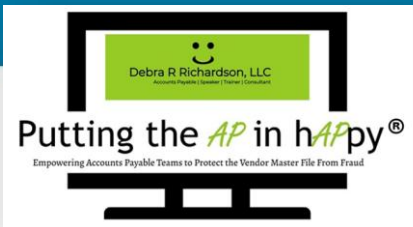
Benefits:

- 1. CEU Requirement for Certification(s):** Leaders earn 3 CEUs per meeting hour and attendees earn 1 CEU per meeting hour. *Earn by watching on-demand – 3 Available*
- 2. Leadership:** Help to plan events, create members' only resources and activities that will enhance careers and knowledge
- 3. Career:** Add the membership to your LinkedIn Profile and join Chapter Groups
- 4. Networking / Engagement:** Meet other like-minded professionals to discuss pain points and resolutions
- 5. Discounts** – Get discounts on E-Learning and New Memberships



November 2026 | JW Marriott Austin | Austin, TX





The Speaker

**Debra R
Richardson, MBA,
CFE, APM,
APPM, CPRS**



November 2026 | JW Marriott Austin | Austin, TX



An accounts payable speaker, consultant, and trainer with over 20 years of experience in AP, AR, general ledger, and financial reporting for Fortune 500 companies including Verizon, General Motors and Aramark.



For over a decade, I have focused on Accounts Payable including Global Vendor Maintenance for 140K+ active vendors across seven ERPs, managing a team processing over 2,000 vendor requests per month.



Now I work with AP teams to implement authentication techniques, internal controls, vendor validations and best practices to prevent fraud, regulatory fines and bad vendor data.



I host a weekly podcast: "Putting the AP in hAPpy".

**Clean-Up Your Vendor Data
Clean-Up Your Vendor Processes
Pay the Right Vendor**

training.debrarrichardson.com



Agenda

- How Fraudsters are Evolving
- How Vendors Are Evolving
- Fraud Prevention Techniques
- Crowd Sourced Submissions
- Actionable Takeaways



November 2026 | JW Marriott Austin | Austin, TX



How Everyone Is Evolving to Avoid Fraud



November 2026 | JW Marriott Austin | Austin, TX



Getting Around That Confirmation Call / Data Request

Send Email or Invoice or “Stuff”
Real Website With Fraudulent
Contact Information

Pre-Text Vendor For
Information Asked on
Confirmation Call

Send Email From Within
Real Vendor Account
Requesting Change



Victims Contact Fraudsters Instead
of Vendor

Pass Authentication Requests

Assumes Requestor is Authentic
Based on Use of Historical Email
String – Does Not Make Call

The Confirmation Call is not a Silver Bullet



November 2026 | JW Marriott Austin | Austin, TX



Getting Around Bank Account Ownership Validation

Opening Bank Accounts Using Vendor Information

- ☒ Account Name
- ☒ Street Address, City, State, and Zip Code
- ☐ Bank Account Number
- ☐ Routing Number
- ☒ Tax Identification Number (TIN)



New Bank Account

Bank Account Ownership Validation is not a Silver Bullet



November 2026 | JW Marriott Austin | Austin, TX



Nacha Is Trying to Prevent Fraud Too

Fraud Monitoring by Originators, TPSPs and ODFIs

(Effective date - Phase 2: June 19, 2026 for all non-Consumer Originators, TPSPs, and TPSs that did not fall under the requirement threshold for Phase 1.)

This rule amendment will require all non-Consumer Originator, Third-Party Service Provider, and Third-Party Sender that did not fall under the requirement threshold for Phase 1, to establish and implement risk-based processes and procedures reasonably intended to identify ACH Entries initiated due to fraud.

- The amendment is intended to reduce the incidence of successful fraud attempts.
- Regular fraud detection monitoring can establish baselines of typical activity, making atypical activity easier to identify.

The Nacha Rules currently require Originators to use a commercially reasonable fraudulent transaction detection system to screen WEB debits and when using Micro-Entries.

- These rules are intended to reduce the incidence of unauthorized debits resulting from transactions initiated online, which can experience increased volume and velocity.

[Read More](#)



November 2026 | JW Marriott Austin | Austin, TX



Vendors Are Trying to Prevent Fraud Too

- **Removing Contact Information From Website**
 - Fraudsters can “Stuff” fraudulent contact information on vendor websites
 - Avoids pre-texting of vendor employees by fraudsters
- **Proactive Process to Avoid Sending Banking Through Email**
 - Bank Account Certificates
 - UPIC Numbers
 - Instructions to Client to Collect Banking

Flipping the Script: Vendors Are Reducing Their Payment Fraud Risk When Providing Banking Information With This Tactic



Debra R. Richardson, MBA, CFE, APM, APPM, CPRS
Training Vendor Management Teams To Avoid Fraud, Fines and Bad Vendor Data | Plug Up the Gaps in Your Vendor Process | Certified...

October 19, 2025

[Read Article](#)



November 2026 | JW Marriott Austin | Austin, TX





THERE'S NO SILVER BULLET

@bryanMlathers



November 2026 | JW Marriott Austin | Austin, TX



Fraud Prevention Techniques



November 2026 | JW Marriott Austin | Austin, TX



Authentication - Are They Who They Say They Are?

Identifying Information - Requester

- Before Responding to Inquiry/Giving Documents
 - Random Invoice Information
 - Random Purchase Order Information
 - Existing Banking
 - Tax ID
 - Gesture
 - Safe Word
 - Within Department
 - Between Departments
- Secure Email
- Confirmation Call (*do it better*)

Identifying Info – Data on Forms

- Bank Country
 - Vendor and Vendor Bank
- Require
 - Existing Banking
 - Historical Payment Info
 - Employee They Have a Relationship With
- Formula to Matching Email Addresses



November 2026 | JW Marriott Austin | Austin, TX



Validations – Is the Vendor Information Valid / Accurate?

Validations - Data

- Legal Name + Tax ID
- Address Standardization/Format

Validations - Does it Match to Vendor?

- Legal Name + Tax ID
 - SEC Edgar Database for Public Companies
- Address
 - Secretary of State – US Vendors
- Micro Entry
- Bank Account Ownership



November 2026 | JW Marriott Austin | Austin, TX



Confirmation Call(s) – Do it Better

- 3 Confirmation Calls
 - New Vendor Add
 - Existing Vendor Change
 - Receipt of Payment



November 2026 | JW Marriott Austin | Austin, TX



Keep Up To Date With New Scam Alerts

[Debra R Richardson New Scam Alerts](#)

[FBI Internet Crime Complaint Center Alerts](#)

[US Postal Inspection Service News, Alerts, Wanted Posters](#)

[IRS Tax Scams/Consumer Alerts](#)

[Better Business Bureau \(BBB\) Scam Tracker, Report a Bad Ad and New Scams](#)

**VENDOR PROCESS
TRAINING CENTER**
NEW SCAM ALERTS
Keep Up To Date On New Frauds



Email Address *

Subscribe

* indicates required

←

[Sign-Up for New Scam Alerts](#)



November 2026 | JW Marriott Austin | Austin, TX



How To Combat



Victim of Fraud? Report:

FBI: <https://www.ic3.gov>

FTC: <https://FTC.gov/Complaint> or <https://IdentityTheft.gov>

IRS at <https://www.irs.gov/help/report-fraud>

Social Security: <https://www.ssa.gov/scam/>



November 2026 | JW Marriott Austin | Austin, TX



Password Manager



Train Your Staff



Authentication



STOP - C-Suite Level
request payments via email



Check Sender Domain
www.whois.com/whois
[ICANN Lookup](#), [Virus Total](#)
[Google Safe Browsing](#)



Create an Internal Request
Form to collect vendor
contact info, then reach out
to the vendor directly.



Review Pay Cycle Reports
& Verify Invoices w/Recent
Remittance Changes



Confirm with the Vendor
AFTER the payment to
make sure they received it



Crowd Sourced Submissions

Real Case Studies



November 2026 | JW Marriott Austin | Austin, TX



Submissions

Call for Fraud Case Studies!



Maeve Kiley

IOFM Staff

IOFM Fall Attendee

IOFM Conference Alum

1d

Joined 5 months ago

This Fall, join Fraud Expert [Debra R Richardson](#) as she dives into AP Fraud.

Have a case that stuck with you? We want to hear it — no names, no companies, just the story. Your experiences will help shape her deep-dive session at the conference, so stick around to see your insights come to life in the room. Some responder profile details are required, but the explanation of what happened can be detailed or vague. This information will not be shared outside of Debra and is completely anonymous.

[Share your story here!](#)



November 2026 | JW Marriott Austin | Austin, TX



3

Industry	Manufacturing
Accounting / ERP System	SAP
# Vendors	~16,000
Fraud Amount	Attempted
Who Owns the Vendor Process?	Separate Master Data Management Team (Customers+Vendors)
Recent Fraud Attempts	Imposter via email, imposter of CEO on WhatsApp, Compromised vendor's servers
Fraud Story	Internal Request was forwarded based on what was perceived to be a request from our CEO via WhatsApp. The internal teammate forwarded the request to AP to assist in making a payment. The request contained ACH information. Fortunately, this was not successful. The forwarding teammate would not have had fraud training, but our IT team now assigns fraud training to the entire organization through Workday. That teammate should have questioned why the CEO was reaching out to them as they don't normally interact with him and they do not support payments in any way. AP is well trained and did raise suspicion that this was a fake request. The vendor was not already on file. The CEO would never reach out on WhatsApp. The CEO never makes payment requests. A simple Teams inquiry validated what AP believed, he did not make the request. PTP leadership and IT Security partnered to create a variety of controlled, fake attempts to get AP to break policy and issue a payment based on the test scenarios. One of those was similar to this attempt. We followed up with training sessions and policy reinforcement. Only 1 person on 1 scenario failed out of 90. One is all that is needed to have fraud succeed. That person was individually trained after the session. It is very important that your entire organization is trained to detect fraud attempts. The more hands these attempts pass through, the higher the risk. The urgency increases as more time passes. They are afraid to show lack of execution, speed and incompetence when someone as high as the CEO makes the request. This is where people start to make bad decisions and bypass processes/policy. Now, IT Security assigns fraud training to the organization utilizing our Learning platform in Workday.

Never accept emails from CEO's requesting payment, so if received, that is the red flag.



November 2026 | JW Marriott Austin | Austin, TX



Industry	Healthcare
Accounting / ERP System	Zycus/PeopleSoft
# Vendors	70,000
Fraud Amount	Attempted
Who Owns the Vendor Process?	Accounts Payable
Recent Fraud Attempts	I've seen multiple cases of a suppliers email account has been compromised and then they send bank account updates to the fraudsters account.
Fraud Story	How did it start? Email to update bank information What was the fraudster trying to get you to do? bank change Was the payment fraud successful? Partially. The bank account was changed and they payment was sent but the fraud was discovered the next day so the bank was able to recover the funds. What internal control was supposed to catch it, and why didn't it (or what did catch it)? Bank account changes are verified with a phone call to a phone number or record with the supplier other than the person in the email making the change request. This was done, not sure if the person that answered just said yes we changed our information. And we use a tool from our bank to confirm bank accounts but sometimes if the bank is small or does not report be get an inclusive result. What changed after the incident (policy, workflow, approvals, technology, training)? More stringent verifications.

Create
Scripts for
Confirmation
Calls.



November 2026 | JW Marriott Austin | Austin, TX



Industry	Energy
Accounting / ERP System	Oracle / MS Dynamics/D365
# Vendors	2100
Fraud Amount	\$25k-\$120K
	AP
Who Owns the Vendor Process?	
Recent Fraud Attempts	2-4
Fraud Story	Our very first payment fraud was a check that we mailed out from our HQ was intercepted and washed with a new address that was sent to a local address in the area. We did eventually get our money back from the bank due to the bank didn't address the safety systems that were in place. Since then, we have initiated stringent protocols, and I've separated myself from the vendor maintenance requests - I don't honor any emails sent to me for changes - they are all directed to an independent but monitored email that I have access too. There are many security functions/features that we have and now 1 of 3 AP associates have trained themselves to analyze invoices from our vendors, which she had caught numerous fraudulent invoices, including one that the vendor sent computer hardware to an unknown address/person and billed us, which we refused to pay. I'm wanting to keep updated and how to better be prepared for any fraudulent situations in AP.

Payee Positive
Pay and Post No
Checks should
be in place at
the bank.



Industry	Public Relations
Accounting / ERP System	Tyler Munis
# Vendors	2726
Fraud Amount	100,000.00
Who Owns the Vendor Process?	Accounts Payable
Recent Fraud Attempts	EFT PAYMENT FRAUD
Fraud Story	Vendor sent an email requesting for EFT banking information to be updated. When we called the vendor at a number on their vendor record they advised that there are no changes to their banking information is fraud. Therefore, we did not move forward on the changing of vendors banking information based on email attempt.

Example of why you should still do the confirmation call!



8

Industry	Higher Ed
Accounting / ERP System	Workday
# Vendors	6000
Fraud Amount	600,000.00
Who Owns the Vendor Process?	Separate Vendor Team
Recent Fraud Attempts	invoice phishing
Fraud Story	We use Workday Strategic Sourcing as a supplier registration/onboarding tool. We received an email from a construction company telling us that the prior person with access left the organization and they needed access. Our team that manages granting that access noted that no one from that organization had access, so they sent a link to them and granted them access. The fraudster then added banking information, we use a validation supplier to validate banking information. It gave us a warning that it couldn't match the name to the bank account, but we had taken a stance that if the supplier updated it themselves in the Supplier portal and the name couldn't be validated, we would allow it. We would call for bank acct changes but not new setups as the assumption was the team that manages access to the portal has validated the supplier contact. In this case they didn't. We then processed a real invoice for that company and sent the money to the fraudster. Classic phishing that was successful.

Treat vendor self-registration portals as just one delivery method for vendor documentation. Keep your same controls in place.



November 2026 | JW Marriott Austin | Austin, TX



5 Times They Could Have Stopped The Fraud

**Report says procedural failures,
managerial cover-up led to Ocala's
\$492,000 cyber fraud incident**

1. Phone Call
2. Higher Risk Controls
3. Bank Names Don't Match
4. Bank Claim Alert
5. Police Reports

[Read Article](#)



November 2026 | JW Marriott Austin | Austin, TX



Did They Make The Right Changes?

Never Make
Remittance
Changes
Based on an
Invoice

[Read Article](#)

Ohio woman charged in phishing scam that cost Southern Door schools nearly \$68K

Jul 19, 2026 | 2:18 PM



Southern Door County School District, August 16, 2022. PC: Fox 11 Online

BRUSSELS, WI (WTAQ-WLUK) — In the wake of a phishing scam that cost the Southern Door County School District \$67,636 — and resulted in charges against an Ohio woman — the district said Wednesday it has taken multiple steps to protect against such incidents.

Laura Griffin, 50, was charged with two counts of theft by false representation. She is scheduled to make an initial court appearance July 27.

According to the criminal complaint, Griffin sent fake invoices for educational services. Two checks — for \$38,718 and \$28,918 — were issued.

In a statement Wednesday, Superintendent Kevin Krutzik said the district has recovered the losses through its insurance coverage, minus a deductible.

"Following the incident, we conducted a thorough review of our financial and cybersecurity practices and implemented several additional safeguards, including providing updated purchasing training, expanding the types of purchases that require a purchase order, and adding additional email security through Quantum Technologies to help protect against phishing, brand forgery, and account takeovers," he said.



November 2026 | JW Marriott Austin | Austin, TX





THERE'S NO SILVER BULLET

@bryanMlathers



November 2026 | JW Marriott Austin | Austin, TX



Actionable Takeaways



November 2026 | JW Marriott Austin | Austin, TX



Actionable Takeaways

1. Add authentication of the requester
2. Add authentication of the data
3. Identify Safe Words for your department and other critical departments that deal with vendor data, payments, invoicing, etc



November 2026 | JW Marriott Austin | Austin, TX



QUESTIONS?



Debra R Richardson,
MBA, CFE, APM,
APPM, CPRS



Email: debra@debrarrichardson.com



training.debrarrichardson.com



[@debrarrichardson](https://www.linkedin.com/company/debrarrichardson)



[Debra R Richardson, LLC](https://www.youtube.com/channel/UC...)

REMINDER!

If you checked in for NASBA CPE credit, check out at iofm.cnf.io



November 2026 | JW Marriott Austin | Austin, TX

