

CPE Today · 2027 K2 Technology Conferences

Trust in the Age of AI: Security, Ethics & Fraud for CPA Firms

Security

November 3, 2027
Live online · Central Time

8 CPE
Credits, proposed

1 day
Group Internet Based

About the Conference

CPA firms hold exactly what attackers want: tax data, bank credentials, and client trust. This conference opens with a map of the threats firms face today, from ransomware and business email compromise to vendor breaches and deepfake impersonation, and what IRS Publication 4557 and the FTC Safeguards Rule require of your firm. It closes with fraud in the age of AI, walking through payment diversion, check washing, payroll redirect, synthetic vendors, and tax identity theft, and the red flags and internal controls that protect firms and their clients.

In between, you will apply the AICPA Code's confidentiality provisions and IRC Section 7216 consent requirements to cloud platforms, outside IT providers, and AI tools, and build or update your written information security plan with a risk assessment and an incident response playbook. Sessions cover the risks of client data in public AI models and unsanctioned tools, multi-factor authentication, passkeys, and password managers, the verification procedures that stop voice cloning and fake executive requests, and secure portals, encryption, and e-signature for client communications. You will earn credits in Information Technology, Behavioral Ethics, and Auditing.

Who Should Attend

- Partners and firm administrators responsible for security, compliance, and client data.
- Tax preparers who must maintain a written information security plan.
- IT and operations staff who support accounting firms.
- CPAs who want 8 CPE credits, including 2 in Behavioral Ethics.

What You'll Take Away

- Identify the threats CPA firms face today and what IRS Publication 4557 and the FTC Safeguards Rule require.
- Apply AICPA confidentiality provisions and IRC Section 7216 consent requirements to technology decisions.
- Build or update a written information security plan with a risk assessment and incident response playbook.
- Set a firm AI policy that addresses client data, unsanctioned tools, and unchecked output.
- Tighten access with multi-factor authentication, passkeys, and a firm-wide password manager.
- Recognize AI-assisted fraud schemes and apply the verification procedures and internal controls that stop them.

Proposed Agenda

Day One

8:00 AM – 9:40 AM **The Threat Landscape for CPA Firms**

Information Technology · Basic · 2 CPE

CPA firms hold exactly what attackers want — tax data, bank credentials, and client trust — and the attacks are getting faster and more convincing. This keynote maps the threats firms face today, from ransomware and business email compromise to credential theft, vendor and supply-chain breaches, and deepfake impersonation. You'll leave knowing what IRS Publication 4557 and the FTC Safeguards Rule actually require...

- Identify the threats CPA firms face today, including ransomware, business email compromise, credential theft, vendor and supply-chain breaches, and deepfake impersonation.
- Explain why the tax data, bank credentials, and client trust that CPA firms hold make them attractive targets.
- Identify the safeguards IRS Publication 4557 and the FTC Safeguards Rule require of a firm.
- Evaluate where the firm's current practices fall short of those requirements.

Prerequisites: None · Advance preparation: None

9:40 AM – 9:50 AM Break

9:50 AM – 11:30 AM

CHOOSE ONE OF 2 SESSIONS

Ethics in a Digital Practice

Behavioral Ethics · Intermediate · 2 CPE

Cloud platforms, outside IT providers, and AI tools raise ethics questions the profession's rules were not originally written for. This session applies the AICPA Code's confidentiality provisions and IRC Section 7216 consent requirements to everyday technology decisions, examines independence considerations when working with tech vendors, and addresses when and how to disclose AI use to clients. Participants will...

- Apply the AICPA Code's confidentiality provisions to decisions about cloud platforms, outside IT providers, and AI tools.
- Determine when IRC Section 7216 requires client consent before tax return information is shared with a technology provider.
- Evaluate independence considerations that arise when working with technology vendors.
- Determine when and how to disclose the use of AI to clients.

Prerequisites: A working knowledge of the AICPA Code of Professional Conduct. · Advance preparation: None

Build or Refresh Your WISP

Information Technology · Basic · 2 CPE

Every tax preparer is required to have a written information security plan, but many firms have one that is outdated, generic, or missing entirely. In this hands-on workshop, participants build or update their WISP step by step, conduct a practical risk assessment of their own firm, and draft an incident response playbook. You'll leave with working documents tailored to your practice, not just a template.

- Identify the components of a written information security plan for a tax practice.
- Conduct a practical risk assessment of the firm's systems, data, and procedures.
- Develop or update a WISP tailored to the firm's practice.
- Design an incident response playbook the firm can follow after a security event.

Prerequisites: None · Advance preparation: None

11:30 AM – 12:20 PM Lunch

12:20 PM – 1:10 PM

CHOOSE ONE OF 2 SESSIONS

AI Risks and Concerns

Information Technology · Basic · 1 CPE

AI tools are already in your firm, whether or not you've approved them. This session examines the real risks — client data leaking into public models, staff using unsanctioned "shadow AI" tools, and hallucinated output making its way into client deliverables. Participants will learn the essential elements of a firm AI policy that enables productive use while protecting clients and the firm.

- Identify how client data can leak into public AI models.
- Recognize the risks of staff using unsanctioned "shadow AI" tools.
- Determine review steps that keep inaccurate AI output out of client deliverables.
- Identify the essential elements of a firm AI policy that enables productive use while protecting clients and the firm.

Prerequisites: None · Advance preparation: None

Identity and Access

Information Technology · Basic · 1 CPE

Most breaches start with a stolen or weak credential, which makes identity the front line of firm security. This session covers multi-factor authentication done right, the shift to passkeys, deploying a firm-wide password manager, and closing the access gaps left when staff and contractors depart. You'll leave with a practical checklist for tightening who can get into what across your firm's systems.

- Explain why identity is the front line of firm security.
- Determine how to configure multi-factor authentication effectively across firm systems.
- Evaluate the move from passwords to passkeys for firm accounts.
- Plan the deployment of a firm-wide password manager.

Prerequisites: None · Advance preparation: None

1:10 PM – 1:20 PM Break

1:20 PM – 2:10 PM CHOOSE ONE OF 2 SESSIONS

Deepfakes and Social Engineering

Information Technology · Basic · 1 CPE

A few seconds of recorded audio is now enough to clone a partner's voice, and attackers are using it to authorize wires and extract client data. This session shows how voice cloning, fake executive requests, and AI-polished phishing actually work, with real-world examples targeting accounting firms. Participants will learn verification procedures that stop these attacks regardless of how convincing the request appears.

- Recognize how voice cloning, fake executive requests, and AI-polished phishing work.
- Identify the warning signs in requests that target accounting firms.
- Apply verification procedures that confirm a request regardless of how convincing it appears.
- Establish verification steps for wire authorizations and client data requests.

Prerequisites: None · Advance preparation: None

Securing Client Communications

Information Technology · Basic · 1 CPE

Every document exchanged with a client is a potential exposure point, and plain email attachments remain the norm at too many firms. This session compares secure client portals, email encryption options, and e-signature platforms, and establishes file-sharing practices that protect sensitive data without frustrating clients. You'll leave with clear standards for how your firm sends, receives, and stores client...

- Identify the exposure created by sending client documents as plain email attachments.
- Compare secure client portals, email encryption options, and e-signature platforms.
- Establish file-sharing practices that protect sensitive data without frustrating clients.
- Develop firm standards for sending, receiving, and storing client information.

Prerequisites: None · Advance preparation: None

2:10 PM – 2:20 PM Break

2:20 PM – 4:00 PM

Fraud in the Age of AI

Audit · Basic · 2 CPE

Old fraud schemes are being supercharged by new technology, and CPAs are often the first to see the evidence. This closing keynote walks through today's most damaging schemes — payment diversion, check washing, payroll redirect, synthetic vendors, and tax identity theft — and shows how AI makes each faster and harder to spot. Participants will learn the red flags to watch for and the internal controls that...

- Identify current fraud schemes, including payment diversion, check washing, payroll redirect, synthetic vendors, and tax identity theft.
- Explain how AI makes each scheme faster and harder to detect.
- Recognize the red flags that signal each scheme.
- Evaluate internal controls that protect the firm and its clients from these schemes.

Prerequisites: None · Advance preparation: None

All times Central Time. Proposed agenda — sessions, times and credits may change before the conference. Registration details, final credits and NASBA disclosures are published on the conference page.
https://www.cpetoday.com/conferences/2027/trust-in-the-age-of-ai