PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

June 2026

Private Foundations Bulletin

Strengthening Fraud Prevention and Risk Governance in an AI-Enabled Environment

By Anan Samara, EA, Partner, Joan McCarthy, Supervisor and Sarah F. Vindigni, CPA, Supervisor

Private foundations operate in an environment where fraud schemes are becoming increasingly sophisticated, driven by advances in technology, cybercrime and artificial intelligence (AI). As stewards of charitable assets, foundations must protect their financial resources while maintaining the trust of donors, grantees, regulators and the public.

Effective fraud prevention requires more than a single control or policy. It requires a comprehensive framework that combines strong governance, active oversight, sound internal controls and ongoing vigilance. As discussed in our recent bulletin, Private Foundations: Should Consider an Artificial Intelligence Governance Policy, boards and management are increasingly expected to understand and oversee emerging risks associated with technology, cybersecurity and AI. Fraud prevention is now part of that broader governance responsibility.

The following considerations can help foundations strengthen their defenses and reduce exposure to fraud and operational risk.

Governance and Oversight

Strong governance is the foundation of an effective fraud prevention program. Foundations should maintain a diverse board of directors or trustees that includes individuals with expertise in finance, accounting, legal, nonprofit operations, risk management and technology oversight. Establishing an audit or finance committee can provide dedicated oversight of financial reporting, internal controls, compliance matters and emerging risks.

As discussed in our May 2026 bulletin regarding AI governance, boards are increasingly expected to understand how emerging technologies may impact organizational risk, compliance, operations and fiduciary responsibilities. While trustees are not expected to be technology experts, they should actively oversee how technologies such as AI are being used within the foundation and whether appropriate safeguards have been established.

Fraud prevention, cybersecurity and AI governance are becoming increasingly interconnected. Effective oversight requires leadership to ask important governance questions, including:

- Do we have sufficient internal controls to prevent and detect fraud?
- How are emerging technologies, including AI, being used within the organization?
- Are responsibilities for financial oversight, technology governance and risk management clearly defined?
- Have we established policies and procedures to address cybersecurity, payment authorization and data protection risks?
- Are management and employees receiving appropriate training and guidance?

Board and committee meeting minutes should carefully document significant discussions, decisions and approvals. Effective oversight also requires active engagement throughout the year—not solely during scheduled meetings—to ensure emerging risks and control concerns are identified and addressed promptly.

Segregation of Duties

Segregation of duties remains one of the most effective safeguards against fraud. Key responsibilities – including authorization, recordkeeping, custody of assets and reconciliation – should be assigned to different individuals whenever possible. Separating these functions reduces the likelihood that a single individual can initiate and conceal an unauthorized transaction.

Additional controls that can strengthen oversight include:

- Dual approval requirements for significant disbursements
- Independent review and approval of journal entries
- Monthly bank and investment account reconciliations
- Clearly documented expense reimbursement and corporate credit card policies
- Regular monitoring and review of financial transactions

For smaller foundations with limited personnel, complete segregation may not always be feasible. In these situations, compensating controls such as increased board oversight, independent reviews and periodic monitoring of transactions can help mitigate risk.

Payment Authorizations, Vendor Due Diligence and AI-Enabled Fraud Risks

Fraudsters increasingly use AI-generated communications, voice-cloning technology and sophisticated phishing techniques to impersonate vendors, grantees, executives and trusted business partners. What once appeared to be isolated cybersecurity incidents have evolved into highly convincing fraud schemes capable of bypassing traditional verification processes.

As a result, foundations should implement formal procedures for validating payment instructions, banking information and vendor requests. Any request to establish or modify banking details should be independently verified through a documented call-back procedure using a previously established and trusted phone number. Verification should never rely solely on information provided within an email request.

Many financial institutions now warn that failure to independently validate wire instructions may result in unrecoverable losses. Foundations should establish written procedures that require secondary verification before processing any wire transfer, ACH payment or banking change request. These procedures should be consistently documented and followed regardless of the perceived urgency of the request.

Vendor due diligence should also extend beyond financial stability and reputation. Foundations should understand how vendors protect sensitive information, manage cybersecurity risks and govern their use of emerging technologies, including AI. Foundations should consider evaluating:

- Information security and cybersecurity practices
- Data privacy and confidentiality protections
- AI governance and acceptable-use policies
- Third-party risk management programs
- Business continuity and incident response capabilities

Foundations that have adopted AI governance policies should ensure payment authorization procedures specifically address AI-enabled impersonation risks, business email compromise schemes and fraudulent requests involving changes to banking instructions. Effective vendor management, combined with independent payment verification procedures, can significantly reduce exposure to financial loss and reputational damage.

Technology and Cybersecurity Controls

Strong technology controls are essential to protecting foundation assets, financial systems, donor information, grantee records and other sensitive data. As cybercriminals increasingly leverage automation and AI-driven techniques, foundations should regularly evaluate whether their technology controls remain effective against evolving threats.

Foundations should consider implementing:

- Multifactor authentication (MFA) across all critical systems
- Role-based access controls that limit user privileges to business necessity
- Periodic user access reviews and prompt removal of terminated-user access
- Continuous monitoring of system activity and administrative privileges
- Alerts for new vendor setups, payment instruction changes and unusual transaction activity
- Automated fraud detection and exception reporting tools
- Regular software patching and vulnerability management procedures
- Secure backup and disaster recovery protocols

Employee awareness remains one of the most important defenses against fraud. Regular cybersecurity awareness training, phishing simulations and fraud prevention education can help personnel identify suspicious communications before financial losses occur.

Foundations should also periodically evaluate the cybersecurity posture of critical third-party service providers, including accounting platforms, grant-management systems, cloud service providers and other vendors with access to sensitive information. As discussed in our prior bulletin regarding AI governance, organizations should understand how technology providers utilize AI tools, what data may be processed by those systems and what safeguards exist to protect confidential information.

Technology controls are no longer solely an IT responsibility. They have become a core governance and risk management function that directly supports fraud prevention, regulatory compliance and fiduciary oversight.

We Can Help

PKF O'Connor Davies assists private foundations with strengthening governance, internal controls, fraud prevention programs and risk management practices in an increasingly complex and technology-driven environment.

Our multidisciplinary teams, including our Forensic Accounting and Investigations practice, provide advisory services involving fraud risk assessments, internal control evaluations, governance and board advisory services, cybersecurity and privacy risk reviews, vendor and third-party risk management, AI governance framework development and policy and procedure design.

As fraud schemes continue to evolve through cybercrime, business email compromise and AI-enabled impersonation techniques, foundations should periodically assess whether their governance structures, payment authorization procedures, technology controls and oversight practices remain effective. Our Forensics team includes Certified Fraud Examiners, Certified Financial Forensics and retired FBI professionals.

Whether your foundation is seeking to enhance fraud prevention controls, evaluate emerging technology risks, strengthen cybersecurity safeguards or improve overall governance and compliance processes, we can help develop practical solutions aligned with your fiduciary responsibilities and operational objectives.

Conclusion

Fraud prevention is essential to protecting a private foundation's assets, reputation and mission. By fostering strong governance, maintaining effective internal controls, implementing rigorous payment authorization procedures and proactively addressing emerging risks — including those associated with AI and cybercrime — foundations can strengthen their resilience against fraud and safeguard the resources entrusted to them.

AI governance, strong oversight, accountability and risk awareness remain critical components of managing emerging risks and fulfilling fiduciary responsibilities. Foundations that integrate governance, cybersecurity, AI oversight and fraud prevention into a cohesive risk management framework will be better positioned to protect both their assets and their mission.

For additional insights, we recommend:

- *AI Governance: What Foundations Need to Know*
- *Strategies to Prevent and Detect Fraud at Your Foundation*
- *Protecting Your Foundation from Disbursement Fraud*

Contact Us

We welcome the opportunity to answer any questions regarding fraud prevention, governance, cybersecurity, AI risk management or other accounting, audit, tax and advisory matters affecting private foundations. Please call 212.286.2600 or contact any member of our Private Foundation Services team.

Thomas Blaney, CPA, CFE
Partner, Co-Director of Foundation Services
tblaney@pkfod.com

Christopher Petermann, CPA
Partner, Co-Director of Foundation Services
cpetermann@pkfod.com

Joseph Ali, CPA
Partner
jali@pkfod.com

Elizabeth Gousse Ballotte
Partner
eballotte@pkfod.com

Scott Brown, CPA
Partner
sbrown@pkfod.com

Michael R. Koenecke, CPA
Partner
mkoenecke@pkfod.com

Anan Samara, EA
Partner
asamara@pkfod.com

This article was originally published on June 25, 2026.