PROTECTING ASSOCIATION FUNDS

Reducing the Risk of Fraud, Embezzlement, and Financial Misconduct

A focused guide for association board members

NEW ENGLAND CHAPTER community ASSOCIATIONS INSTITUTE

Delegate the work. Define the authority. Verify the results.
Good governance depends on clear roles, reliable information, professional guidance, and routine accountability.

Community association boards remain responsible for safeguarding homeowner funds even when day-to-day financial work is delegated. Effective oversight requires clear authority, independent information, regular review, and prompt follow-up. Verification is not distrust—it protects the association, the board, the manager, and the homeowners whose money is being administered.

Ten Practices That Matter Most — Board Checklist

☐ **1. Know where every dollar is held.**
Maintain a current inventory of every financial account including operating, reserve, investment, capital project, loan, and/or insurance-proceeds accounts. Consolidate investment accounts with banks that participate in CDARS (Certificate of Deposit Account Registry Service) and ICS (Insured Cash Sweep).

☐ **2. Keep accounts under association control.**
Use the association's legal name and tax identification number. Ensure timely, independent board visibility through secure view-only access or bank-generated statements/activity delivered directly to designated board members.

☐ **3. Separate critical duties.**
Avoid allowing one person to initiate, approve, release, and reconcile the same transaction. Use compensating controls when staffing is limited.

☐ **4. Document financial authority.** Use written approval limits and procedures for invoices, transfers over a specified dollar amount, reserve withdrawals, new vendors, and payment-instruction changes.

☐ **5. Review the money every month.**
Compare financial reports to independent bank information and review material variances, reserve activity, receivables, major expenses, unusual transactions, and unresolved questions.

☐ **6. Protect electronic transactions.**
Use unique credentials, multifactor authentication, transaction limits/alerts, and dual approval where appropriate. Verify payment changes or wire requests by calling a trusted, predetermined vendor number—not a number supplied in the request.

☐ **7. Review access and continuity.**
At least annually, confirm authorized signers, online users, permissions, and who can continue each critical financial process when a volunteer or service provider changes.

☐ **8. Match insurance to actual exposure.**
Review applicable crime/fidelity or Employee Dishonesty protection, insurer-required controls, intended people/methods of loss, and the highest amount of funds expected during the policy year.

☐ **9. Use independent professional review.**
Use qualified management, legal, accounting, banking, and insurance professionals. Audits/reviews do not replace regular board oversight; suspected fraud may require a targeted forensic examination.

☐ **10. Act promptly when something does not make sense.**
Late records, conflicting explanations, unexplained transfers, missing support, unusual urgency, or resistance to independent confirmation warrant follow-up.

A Practical Oversight Framework

Use these 6 steps to put the checklist into routine practice.

The goal is a repeatable system that provides transparency without unnecessary duplication, access risk, or continuous monitoring.

STEP 1 — Know the accounts and exposure

- Inventory all bank accounts, including operating, reserve, investment, capital project, loan, and insurance-proceeds accounts.
- Confirm each account is titled in the association's legal name and tax identification number.
- Identify the highest amount of funds expected during the year and update the inventory when major projects, loans, claims, or assessments change the exposure.

STEP 2 — Establish independent bank visibility

- Receive bank-generated statements or equivalent independent account information directly at a regular cadence. Secure view-only access may also be used when appropriate.
- If view-only access is used, limit it to designated users, require unique credentials and multifactor authentication, prohibit transaction authority, review access at least annually, and remove access promptly when roles change.
- Review account information with the full financial package rather than reacting to isolated real-time balances.

STEP 3 — Review a complete monthly financial package

- Review the balance sheet, income-and-expense or budget comparison, general ledger, disbursement/check activity, bank statements and reconciliations, reserve activity, and significant receivables.
- Compare reported cash to independent bank information; obtain explanations for material variances and track open questions until resolved.
- Review the vendor list periodically and investigate unfamiliar vendors or payments; fictitious vendors are a classic fraud technique.

STEP 4 — Control payments, vendors, and electronic changes

- Separate initiation, approval, release, and reconciliation whenever practical, and document approval limits.
- Do not change payment instructions solely in response to an email, text, invoice, or caller. Verify new banking information, payment changes, and wire-transfer requests using a trusted phone number established before the request.
- Use transaction alerts, multifactor authentication, and dual approval where appropriate. Some insurers may ask whether a documented callback procedure is in place.

STEP 5 — Review management, continuity, and insurance annually

- Confirm that the management agreement defines financial authority, reporting, record ownership, banking arrangements, transition obligations, and insurance requirements.

- Review signers, online users, permissions, and continuity plans; make sure more than one person understands each critical process.

- Review crime/fidelity or Employee Dishonesty coverage with a qualified insurance professional and confirm intended people/methods of loss, limits, deductibles/exclusions, notice requirements, and insurer-required controls.

- Treat audits and reviews as valuable independent checks, not substitutes for regular board oversight. Because these engagements are generally periodic, problems can begin and continue between reporting dates unless the board also performs timely monthly review.

- Distinguish a financial-statement audit from a fraud or forensic examination. A financial-statement audit focuses on whether the statements are materially fairly presented and includes consideration/testing of internal controls; a suspected fraud may require a separate, targeted forensic engagement by professionals with appropriate investigative and accounting expertise.

STEP 6 — Escalate warning signs and preserve evidence

- Warning signs include late or frequently revised reports, resistance to independent confirmation, unexplained transfers, missing support, duplicate or unfamiliar payments, unexpected cash shortages, unusual urgency, secrecy, or conflicting explanations.

- If a discrepancy may involve misconduct, consult legal counsel promptly before confronting a suspected person, restricting access, communicating with owners, or making public statements.

- Secure accounts as appropriate, preserve statements/emails/invoices/logs and original electronic records, notify the bank and insurer as directed, use qualified accounting or forensic professionals when needed, and strengthen controls after the matter is resolved.

Board meeting quick check

☐ Do we know every account and the highest amount we expect to hold this year?

☐ Can the board trace reported cash to independent bank records and track exceptions until resolved?

☐ Could one person create a vendor, initiate or approve payment, and reconcile the same transaction without independent oversight?

☐ Does our insurance reflect who can access funds, how a loss could occur, and our maximum expected exposure?

☐ If something looks wrong, do we know who will preserve evidence and contact counsel, the bank, the insurer, and accounting professionals?

This resource was developed by a task force of CAI New England Chapter members including Kenneth Bloom, CPA | Bloom Cohen Hayes LLC; Matthew Gaines, Esq.| Marcus, Errico, Emmer & Brooks P.C.; David Haynes | HUB International New England; Patrick Holland, CMCA, AMS | Barkan Management Company; Sean Jordan, CMCA, AMS; and Scott Wolf, CMCA, AMS, PCAM | Brigs, LLC, AAMC and provides general educational information and does not constitute legal, accounting, insurance, or management advice. Requirements vary by state, governing documents, banking arrangements, contracts, lender obligations, and policy terms.