

Healthy Practices for Online Payments & Digital Finance Systems

Core Principle

The #1 Protection Against Fraud: No one person should be able to create, change, approve, and reconcile financial transactions alone.

Fraud most often occurs when:

- One employee has unchecked control
- Account changes are not independently reviewed
- Or financial activity is not regularly verified

Strong controls are not about distrust.

They are about:

- Protecting the mission
- Protecting donors
- Protecting staff
- And protecting organizational sustainability

Top Recommendations for Nonprofits

1. Require Dual Approval for Banking Changes

Any change to:

- Bank accounts
- ACH instructions
- Online giving payouts
- PayPal/Venmo transfers
- Vendor payment information
- Or grant disbursement

Accounts should require:

- A second reviewer
- Written documentation
- And independent verification

Best Practice

- Require Executive Director or Board Treasurer approval for all banking-related changes

2. Separate Financial Duties

Separate responsibilities whenever possible:

- Entering bills,
- Approving payments
- Releasing payments
- Reconciling accounts
- Reviewing reports

Why This Matters

Fraud becomes much harder when multiple people are involved in the process.

Even small nonprofits can create basic separation through:

- Board oversight
- Outsourced bookkeeping
- Or dual approvals for larger transactions

3. Limit Administrative Access

Only a very small number of trusted staff should have:

- Administrator permissions
- Banking access
- Payout controls
- Or authority to change linked accounts

Important Safeguards

- Remove access immediately when staff leave
- Review permissions quarterly
- Avoid shared usernames /passwords
- Use role-based permissions whenever possible

High-Risk Systems

Special attention should be given to:

- PayPal
- Venmo
- Bill.com
- Online donation systems
- ACH banking systems
- Payroll systems
- Donor management platforms

5. Reconcile ALL Online Financial Systems Monthly

Do not only reconcile the bank account.

Also reconcile:

- PayPal balances
- Venmo balances
- Online donation systems
- Bill.com activity
- ACH activity
- And payment platforms

Key Question

- “Did the money actually go where we intended it to go?”

4. Require Two-Factor Authentication (2FA)

Enable 2FA on:

- Banking systems
- Accounting software
- Payroll system
- Donation platforms
- PayPal
- Bill.com
- And all financial technology systems

Why This Matters

- Compromised passwords are a leading cause of financial fraud.
- 2FA is one of the simplest and most effective protections available

6. Ensure Board-Level Financial Oversight

Boards should:

- Review financial statements monthly
- Ask questions
- Monitor unusual variances
- And ensure internal controls exist

The board does not need to manage operations directly—but it should ensure that:

- Reconciliations occur
- Controls are functioning
- And no employee has unchecked financial authority

Top Risk Indicators

Operational Red Flags

Watch carefully for:

- One employee controlling the entire payment process
- Delayed financial reporting
- Missing documentation
- Resistance to oversight
- Unusual secrecy
- Staff refusing vacations
- Shared passwords
- Lack of reconciliation

Digital Payment Red Flags

Pay special attention to:

- Undocumented bank account changes
- Unexplained PayPal or Venmo transfers
- Unknown ACH recipients
- Donation totals not matching deposits
- Unusual vendors
- Grants marked “paid” but not received
- Payment changes lacking documentation or approval

Immediate Actions Nonprofits Can Take Right Away

If an organization can only implement a few changes immediately, prioritize these:

1. Enable 2FA Everywhere

Turn on two-factor authentication for all financial systems.

2. Require Dual Approval for Banking Changes

No employee should be able to independently change payout or banking information.

3. Review Linked Accounts Quarterly

Verify:

- Donation payouts
- ACH destinations
- Vendor banking details
- And grant disbursement settings

4. Reconcile Online Platforms Monthly

Review all digital payment systems — not just bank statements.

5. Ensure No One Person Controls the Entire Process

Separate duties and add secondary review wherever possible.

Final Takeaway

Healthy financial controls are not about creating bureaucracy.

They are about:

- Protecting donor trust
- Protecting staff and leadership
- Preventing preventable harm
- And ensuring nonprofit resources stay focused on mission impact

Most fraud is not caused by sophisticated schemes.

It happens when:

- Oversight is informal
- Access is unrestricted
- Or organizations assume - “it could never happen here.”

Simple, consistent practices can dramatically reduce risk and strengthen organizational resilience.