10 Ways to Guarantee Fraud in Your Family Office

By Charlie Carr, CFP®

Years ago, a family office president told me that his predecessor had stolen money from the family, leaving him with the difficult task of rebuilding the family's trust. Another president told me he would never do anything underhanded but wanted controls strong enough that the family would never have reason to suspect him.

In 2017 and 2018, I spoke at family office gatherings on the above topic. The title caught people's attention, but the underlying point was serious: certain practices make an office far more susceptible to fraud. Most of those practices have withstood the test of time, although the risks and the tools available to address them continue to evolve. The items below are numbered for convenience, not in order of importance.

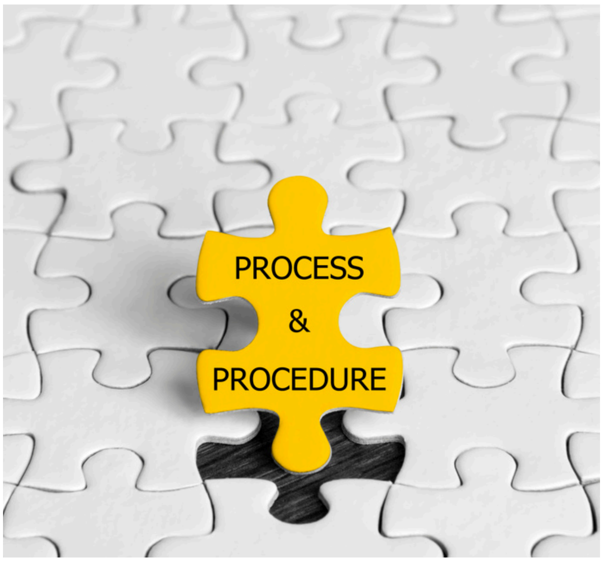
1. Weak Email and Cybersecurity Practices

Criminals continually probe your network for the easiest access point – often a malicious link that gives them entry once a family member or staff member clicks it.

One of the most effective training tools remains ethical phishing: have an outside firm send simulated phishing emails and use the results to train both the family and your staff. Family office leaders often say they cannot send such emails to family members, only to staff. When we share that with family members, they adamantly disagree.

Public Wi-Fi carries a similar risk. At an airport, hotel or coffee shop, it is easy to log on without protection. Use a virtual private network (VPN) on public Wi-Fi, or skip it and use your phone as a hot spot.

We saw a family office where every employee kept a sheet listing each family member's checking accounts and login information on their desk. We have also seen offices share one password for the general ledger, making it impossible to know who changed a transaction, and passwords written on sticky notes or slipped under keyboards. Each person should have an individual login, supported by multi-factor authentication and strong, unique passwords stored in an approved password manager.



2. Do Not Bother With Written Procedures

Written policies and procedures provide at least three benefits: operational consistency, disaster preparedness and succession planning. If a key employee has a health issue, will anyone know what that person was working on or how to complete it? Written procedures also help prevent theft. Staff members may otherwise follow different processes for reimbursements, wire changes or payroll updates – inconsistencies that bad actors exploit.

The process of creating the policies and procedures is often as important as the documents themselves. It forces the office to decide who may initiate a transaction, who must approve it, what evidence is required and what happens when the normal process cannot be followed.

3. Weak Investment Diligence and Governance

Strong offices have formal investment governance: an investment committee with defined authority, investment policy statements for trusts and entities and a process for monitoring investments. Due diligence should address the sponsor's background and conflicts, independently confirm the custodian and destination of funds, and test assumptions behind projected returns. "A friend is investing" is not due diligence.

4. Trust Your People and Do Not Verify

Family offices are built on trust. Long-time employees often become "like family," and that closeness can gradually take the place of proper controls. Good controls do not question someone's character; they keep one person from carrying responsibility that should be shared and protect an honest employee from suspicion if something goes wrong.

Background checks should apply to family office staff, people working in family members' homes, and key partners and advisors, including those bringing private investment opportunities. They should be repeated periodically rather than treated as a one-time exercise. I once served on a non-profit board with someone who had been fired from his job for stealing. We caught it only because we repeated background checks every two years.

Offices also frequently ask for references and then fail to check them. At the other end of employment, access to systems, bank accounts, credit cards and physical facilities should be revoked quickly when someone leaves. Trusting people is much easier when the right safeguards are in place.

5. Let One Person Control Everything

In a small office, one person may receive invoices, maintain vendor information, enter bills, initiate wires, record transactions and reconcile the bank accounts. This may be efficient, but it also allows the same person to create a false transaction and conceal it.

Segregation of duties does not necessarily require more employees. A family principal, outsourced accountant, bank or other advisor can provide independent approval or review. The essential principle is that no one person should control a transaction from beginning to end – or control both the records and the reports the family sees.

6. Treat Payment Request as the Authorization

For years, some of the largest losses wealthy families have experienced have come from failing to verify payment instructions. A vendor sends new wire instructions, and the office changes them – but the message did not come from the vendor. A family member emails asking to wire money for new artwork – but the family member did not send it. A title company sends wire instructions the day before a real estate closing – but the instructions are fraudulent.

Never use the communication that requested the payment to authenticate the payment. If the request came by email, do not reply to that email or call a number contained in it. Use a previously established phone number or another independent channel. Require verification for every change in payment instructions and consider two-person approval above defined thresholds. As impersonation becomes more convincing, including through artificial intelligence, disciplined verification matters even more.

7. Exempt Family Members From the Rules

Controls often work until a family member says, “I am standing at the dealership—wire the money now,” or “My friend has an investment we need to fund today.” Employees may be understandably reluctant to question the people they serve, and fraudsters know it.

The family should agree in advance that staff are expected to verify unusual requests, even when the request really came from a family member. A few extra questions may reveal that the family member’s email was compromised, that someone is impersonating a relative, or that the family member is being pressured or deceived.

Controls should protect family members, not merely protect the family from employees.

8. Let Everyone Choose Their Own Technology

Some offices still refuse to use cloud tools or artificial intelligence, because avoiding them sounds safer. Most software now requires the cloud, severely limiting your options and your ability to innovate efficiently. It’s harder to pick the best estate attorney or tax accountant when a staff member must drive thumb drives to their offices instead of leveraging cloud tools.

The opposite extreme is equally risky: letting each person choose their own technology – personal AI accounts, password tools, USB drives or file-sharing sites. The answer is to govern modern technology. Define which tools are approved, what information may be entered, how access is granted and removed, how output will be reviewed, and what security settings are required. Providing approved professional tools is generally safer than leaving each person to improvise.

9. Do Not Look for Fraud Until Something Goes Wrong

Prevention matters, but strong controls assume that something may eventually get through. Bank reconciliations should be performed or independently reviewed by someone other than the person processing transactions. Statements and reporting should be available to someone who does not control the underlying records.

Exception reports can reveal duplicate payments, new or changed vendors, unusual journal entries, payments just below approval limits and unexpected credit card activity. Access and activity logs should also be reviewed. The goal is not to investigate every transaction; it is to identify the small number that deserve another look.

Credit cards warrant particular attention. Of the fraud we have uncovered over the years, credit cards arise more than any other area. In one case, someone charged a family member's NetJets expense to a company credit card and then separately submitted the same expense for reimbursement. We also saw an executive assistant's card paid without review because no one wanted to second-guess the executive office. Strong offices require documentation and independent review, regardless of whose card it is.

10. Never test your controls

Family offices are understandably private. That instinct can keep them from asking an outsider to review their practices and advise them on best practices or control risks. The right review depends on the office. It may include a broad operational assessment, accounting controls review, cybersecurity assessment, penetration test or insurance review.

We saw an office that needed to restore its network from backups and discovered that the backups did not work. A backup is useful only if it can be restored. The same is true of a procedure that no one follows or an approval that is routinely bypassed. Test the process before a crisis tests it for you.

Strong Family Office Controls Protect Everyone

Is this a comprehensive list? Absolutely not! After a few decades of working with family offices, these are among the vulnerabilities we see most often. The appropriate controls will vary with the office's size and complexity, but even a small office can create practical checks and balances.

Fraud prevention is not about distrusting good people. Good controls protect honest employees from suspicion, protect family members from their own mistakes, and make it harder for an outsider or insider to exploit a moment of weakness. They also give the next family office president a better starting point than the one in my opening story.

Charlie Carr, CFP® is president of Big Canyon Advisors, LLC, which advises family businesses and family offices (BigCanyonAdvisors.com).