CAXTON
EVERY PAYMENT • ONE PLATFORM

PRACTICAL STEPS TO SAFEGUARD WEALTH, REPUTATION, AND LEGACY

The Family Office Guide to Deepfakes & Cyber Threats

caxton.io/business

INTRODUCTION

For family offices, **trust is the foundation of everything.** It underpins **financial decisions, relationships,** and the smooth running of **day-to-day operations.** But in today's world, even **trust can be convincingly faked.**

Deepfake technology — the use of artificial intelligence to r**eplicate voices and faces** — is no longer science fiction. It is being used right now by cybercriminals to **impersonate trusted individuals, authorise fraudulent transactions, and damage reputations.**

Family offices are particularly attractive targets. They manage significant wealth, often operate with leaner governance frameworks than large corporates, and **rely heavily on personal relationships.** These characteristics, combined with the high value of individual transactions, make them uniquely exposed to **sophisticated cyber threats.**

In September, **Caxton, together with our partners Fladgate and OneCollab,** hosted a webinar to **explore these risks.** We shared real-world cases where family offices were targeted, demonstrated how easily a deepfake can be created from just 30 seconds of publicly available audio, and discussed **practical steps to reduce vulnerability.**

This **guide** distils those insights into **clear, actionable takeaways.** It is designed to help family offices **strengthen resilience** — not just through technology, but through **culture, governance, and vigilance.**

Because when it comes to protecting **wealth, reputation, and legacy across generations,** one simple truth remains:

seeing isn't believing.

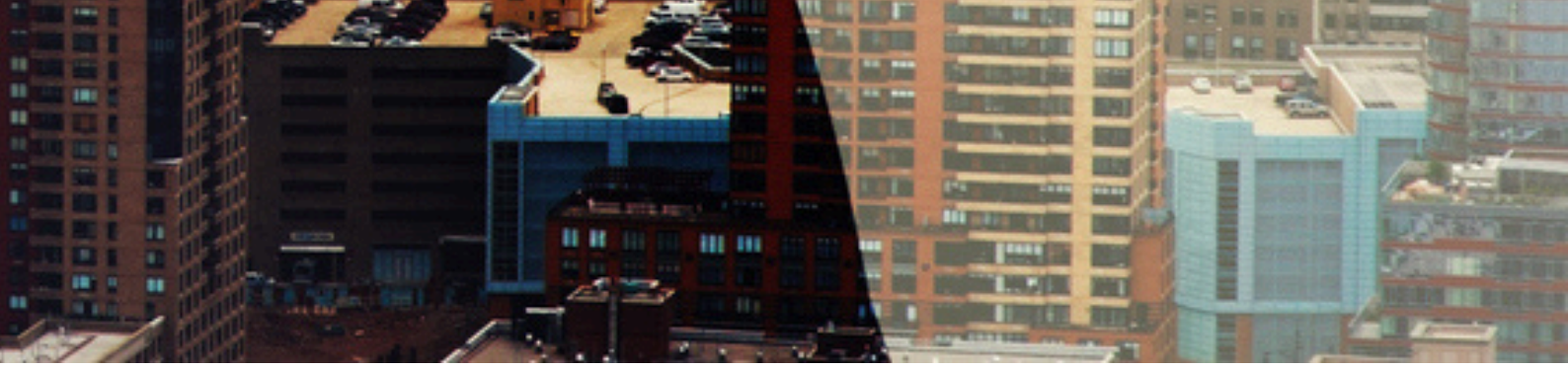
CONTENTS

CAXTON

fladgate

OneCollab

The New Threat Landscape for Family Offices



THE NEW THREAT LANDSCAPE FOR FAMILY OFFICES

What are Deepfakes?

Deepfakes are **highly realistic** but **artificially generated audio, video, or images** created using **artificial intelligence.** A short sample — sometimes just 30 seconds of speech or a few still photos — is enough to build a convincing clone of someone's voice or face.

Originally seen as a novelty, deepfakes have become a **powerful tool for cybercriminals.** They can **impersonate trusted individuals** in real time, **persuade staff** to make **fraudulent transfers,** or **damage reputations** by spreading **false content online.**

Why Family Offices Are Vulnerable

Family offices are uniquely exposed to **deepfake-driven attacks** because of the **way they operate:**

- **Cross-generational use of technology:** Younger family members may be highly active on social media, while older generations may be less digitally fluent. Both ends of the spectrum are vulnerable in different ways.
- **Reliance on personal networks:** Family offices depend on trust-based relationships. A familiar face or voice often carries enough weight to bypass normal scrutiny.
- **High-value transactions:** Large payments are routine, making it harder to distinguish between a genuine urgent request and a fraudulent one.

Real-World Impact

These are **not hypothetical risks** — they are **already happening to family offices:**

Case 1: The £250,000 Car Purchase

A family office staff member received an email from their finance director instructing them to pay for a car. The request looked legitimate and was supported by a follow-up call from someone sounding exactly like their director. In reality, it was an audio deepfake. **The payment — £250,000 — was authorised, and the money was lost.**

Case 2: The Cryptocurrency Scam

A UBO (ultimate beneficial owner) discovered videos of himself circulating on TikTok and Instagram, apparently endorsing a new cryptocurrency. The videos were deepfakes. Although there was **no financial loss,** the **reputational risk was significant.** Quick detection, rapid takedown, and clear communication minimised the damage, but the episode underlined how exposed prominent individuals are.

Case 3: The 30-Second Voice Clip

In our live demonstration, a short audio sample was enough to create a convincing clone of a trusted principal's voice. Within minutes, we generated a fake phone call authorising a high-value transfer. For family offices, the lesson is clear: **it takes very little for criminals to build a credible impersonation.**

The Cost of Getting it Wrong

THE COST OF GETTING IT WRONG

For family offices, the **stakes could not be higher.** The consequences of a successful deepfake attack are **immediate and wide-ranging:**

Financial Loss

Significant sums can disappear in minutes. Fraudulent transfers linked to deepfakes are already reaching seven figures. Once funds are moved, recovery is often impossible.

Reputational Damage

Even if a family office is not legally liable, reputational harm can be lasting. Fake endorsements, leaked content, or reports of scams linked to a principal can erode trust in advisers, partners, and networks. In the discreet world of private wealth, reputation is everything.

Emotional Impact

Fraud is not only financial. It can strain relationships within families, undermine confidence in trusted team members, and create a climate of suspicion. For family offices, where discretion and trust are paramount, this damage can be just as painful as financial loss.

Note: The examples shared here are anonymised but all based on real-world cases.

5 Practical Safeguards for Family Offices

5 PRACTICAL SAFEGUARDS FOR FAMILY OFFICES

1 Build a Culture of Vigilance

Cybersecurity isn't just a technical issue — it's **cultural. Leadership** must set the tone from the top. If **principals and executives** don't take it **seriously, neither will staff.**

- Make **cybersecurity awareness** part of everyday conversation.
- Provide **regular training** not just for employees, but also for **family members,** who may be more **vulnerable to scams.**
- **Encourage questioning:** it's always better to **double-check** than to make an **expensive mistake.**

2 Strengthen Governance & Workflows

Strong governance makes it harder for cybercriminals to succeed. Even the most sophisticated deepfake will fail if the **right checks are in place.**

- Apply the **"four eyes, not two"** principle — no major transaction should ever be authorised by a single person.
- Ensure **independent verification:** each approver must review as if they were solely responsible.
- Reconcile all accounts regularly against **bank records** (not just ledgers). Simple reconciliations are a powerful safeguard.
- Make **cybersecurity and reconciliation reporting** a standing item at every board meeting.

5 PRACTICAL SAFEGUARDS FOR FAMILY OFFICES

3 Verify, Don't Assume

Deepfakes succeed when people act in haste. Slow down and verify requests.

- **Never trust** phone numbers or details listed in an email — always use **verified contact details** already saved.
- For urgent or unusual requests, **confirm face-to-face** or **via secure video call.**
- Avoid relying on **one-line emails or text messages** for payment instructions.
- **Add personal pass phrases** that you don't write down to confirm transactions – and know what to do if you get the wrong one.

4 Get the Basics Right

Many incidents happen because simple controls aren't consistently applied with the specialist skillset required to implement, monitor, and evidence correctly.

- Use **multi-factor authentication (MFA)** everywhere — and enforce it.
- Replace **passwords with passkeys** wherever possible.
- **Restrict access by geography and role** — not everyone needs access to everything.
- **Regularly test & report on your controls:** are they working as intended, or just assumed to be?

5 Plan for Response, Not Just Defence

Even the best defences can be breached. The difference between a near miss and a disaster often lies in how quickly an organisation responds.

- Have a clear response plan covering **who to call, what steps to take, and how to communicate.**
- **Work with trusted advisers** — legal, IT, and communications — to ensure plans are practical and rehearsed.
- **Monitor for misuse of principals' names and likenesses online**, so reputational attacks can be caught early.
- **Learn from incidents.** Every close call should improve your systems and culture.

Bottom line:
By combining culture, governance, and technical hygiene, family offices can dramatically reduce their exposure to deepfakes and cyber threats. None of these steps are complex, but together they create a powerful defence — and protect the trust that family offices are built on.

Questions Every Family Office Board Should Ask

QUESTIONS EVERY FAMILY OFFICE BOARD SHOULD ASK

Strong governance starts with asking the right questions. Use this **checklist** to assess whether your family office has the **right safeguards in place:**

Culture & Training	Y	N
Do our **principals and board** actively champion **cybersecurity** as a **priority?**		
Are **all staff trained regularly** on **cyber risks** — including **deepfakes?**		
Have **family members** (especially younger or older generations) received **tailored training?**		
Governance & Workflows	**Y**	**N**
Do we apply the **"four eyes, not two"** principle for all significant payments and transactions?		
Are **reconciliations** carried out regularly against **bank records,** not just ledgers?		
Is **cybersecurity** a standing item at board meetings?		
Verification & Communication	**Y**	**N**
Do we have clear rules about **verifying unusual or high-value requests** in **person** or via **secure video?**		
Do staff know never to rely on **numbers or details** listed in an email for **verification?**		

QUESTIONS EVERY FAMILY OFFICE BOARD SHOULD ASK

Technical Hygiene	Y	N
Is **multi-factor authentication (MFA)** enforced across all systems and accounts?		
Have we implemented stronger controls, such as **passkeys and access restrictions?**		
Do we **test our controls regularly** (including backups & restoration) to confirm they are actually working?		
Incident Response & Monitoring	**Y**	**N**
Do we have a clear **cyber incident response plan,** with roles and responsibilities defined?		
Are we monitoring for **misuse of family members' names, images, or voices online?**		
Do we review and learn from any **attempted or successful attacks?**		
Do we have **insurance coverage** that can bring in additional support if needed, and are we still in **alignment with the policy?**		

Tip:
If you answered "no" to more than one of these questions, your family office may be more vulnerable than you realise. Start by addressing the basics — culture, governance, and simple verification — and build from there.

Conclusion & Next Steps

CONCLUSION & NEXT STEPS

Family offices are built on **trust** — yet today, even **trust can be convincingly faked.** Deepfakes and cyber scams are no longer future risks; **they are happening now,** and **family offices** are firmly in the crosshairs.

The good news is that the vast majority of incidents can be **prevented with the right culture, governance, and simple safeguards.** From ensuring **"four eyes, not two"** on payments, to making **cybersecurity** a standing board agenda item, to **training family members** as well as staff — these practical steps make all the difference.

But **protection** is not just about **technology.** It's about **people, vigilance, and the systems** you put around them. When combined, these measures help secure not only **wealth,** but also **reputation** and **legacy across generations.**

At **Caxton,** together with our partners **Fladgate and OneCollab,** we are committed to supporting family offices with **trusted advice** and **discreet, practical solutions.**

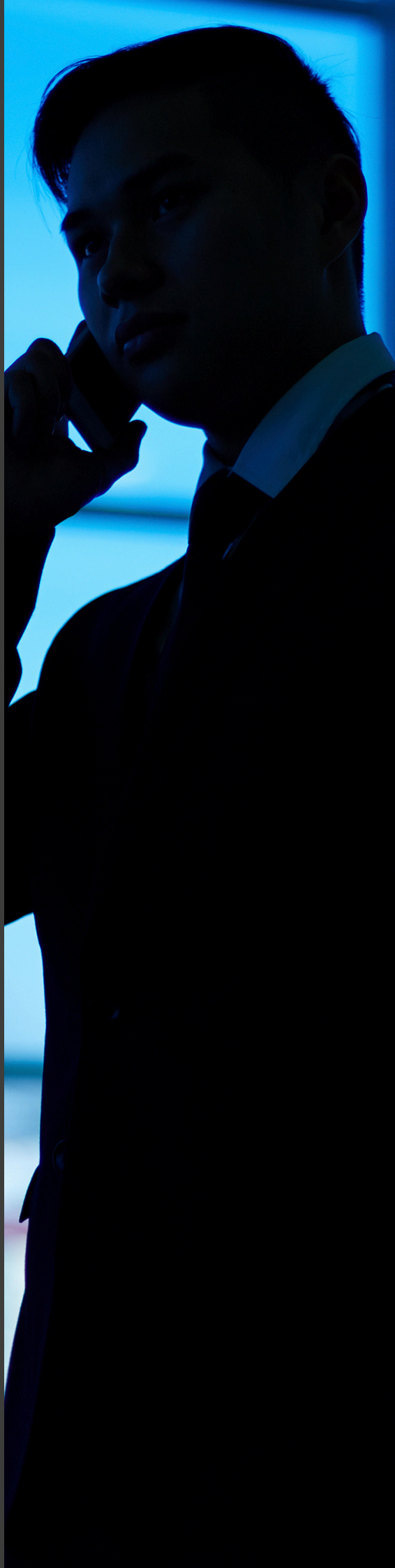
Your next step:

- ☑ **Download** our one-page **Family Office Cyber Checklist** (included with this guide).
- ☑ Arrange a **confidential conversation** with our team or partners to discuss your **family office's current resilience and governance framework.**

Because when it comes to safeguarding your family office, one principle remains true: Seeing isn't believing.

CAXTON

EVERY PAYMENT • ONE PLATFORM



For further information contact:

Caxton Payments Ltd

0207 042 7611

Ryan.McLoughlin@caxton.io

For a confidential conversation about your family office's cyber resilience, contact **Michael Oldham:**

BOOK YOUR CONFIDENTIAL CALL

CAXTON.IO/BUSINESS

CHECKLIST:

Family Office Cyber Checklist

Essential questions to protect **wealth, reputation & legacy:**

Section 1: Culture & Training

- [ ] Stay alert to slippage and avoid **creeping costs.**
- [ ] Are all staff **trained regularly** — including on **deepfakes?**
- [ ] Have family members received **tailored cyber-awareness training?**

Section 2: Governance & Workflows

- [ ] Do we enforce the **"four eyes, not two"** rule on all significant transactions?
- [ ] Are reconciliations carried out regularly against **bank records?**
- [ ] Is cybersecurity a **standing item** & reported on at every board meeting?

Section 3: Verification & Communication

- [ ] Do we have clear rules for **verifying unusual or high-value requests** in person or by secure video?
- [ ] Do staff know never to trust **phone numbers or details inside an email** for verification?

Section 4: Technical Hygiene

- [ ] Is **multi-factor authentication (MFA)** enforced across all systems?
- [ ] Have we implemented **passkeys and access restrictions?**
- [ ] Are all critical systems, including cloud and on-prem, backed up with **immutable copies?**
- [ ] Do we **test our controls regularly** to confirm they work?

Section 5: Incident Response & Monitoring

- [ ] Do we have a clear **cyber incident response plan** with roles defined and clear points of contact on who to call?
- [ ] Are we monitoring for **misuse of family members' names, images, or voices** online?
- [ ] Do we review and learn from **attempted or successful attacks?**

Tip:
If you've ticked "no" more than once, your family office may be more vulnerable than you realise. Start by strengthening culture, governance, and verification — and work with trusted advisers to build resilience.

CAXTON fladgate OneCollab

For a confidential conversation about your family office's cyber resilience, contact ***Michael Oldham.***

KEY TAKEAWAYS

Seeing Isn't Believing: Deepfakes & Cyber Threats to Family Offices

Caxton, Fladgate, and OneCollab hosted a webinar exploring the rising **risks of deepfakes and cyber threats** for family offices. Here are the essential **insights:**

1 Culture & Vigilance Are the First Line of Defence

- Most cyber incidents stem from **human error,** not technology failure.
- A culture of vigilance, led from the boardroom, is critical. If **leadership** doesn't prioritise cybersecurity, neither will the team.
- **Regular training and awareness** must extend beyond staff to family members, who may be more vulnerable to scams.

2 Real-World Family Office Attacks Are Already Happening

- **Horror Story 1:** A family office lost £250,000 after fraudsters used an audio deepfake of a finance director to approve a transfer. The fraud succeeded because checks were by-passed and the request wasn't verified in person.
- **Horror Story 2:** A UBO was impersonated in deepfake social media videos promoting cryptocurrency. Early detection, rapid takedown, and proactive communication limited reputational damage — but vigilance made the difference.
- **Live Demo: T**he session included a chilling demonstration of how a deepfake call can convincingly impersonate a trusted principal to authorise a high-value transfer.

3 Governance and Workflows Reduce Risk

- **Four eyes, not two:** No single individual should authorise significant transactions. Independent verification must be built into workflows.
- **Reconciliations matter:** Regular account reconciliations are a simple but often overlooked safeguard.
- **Face-to-face or video verification:** When in doubt, confirm sensitive requests via video or in-person conversation, not just email.

KEY TAKEAWAYS

Seeing Isn't Believing: Deepfakes & Cyber Threats to Family Offices (continued)

4 Technical Hygiene Is Non-Negotiable

- Basics such as **multi-factor authentication (MFA), passkeys** instead of passwords, backups, and access controls prevent the majority of attacks.
- Cybercriminals often succeed because firms think controls are in place, but they're not **consistently enforced or monitored.**
- **Regular reporting to the board level is key.** Cybersecurity should be a standing item on every agenda.

5 Practical Steps for Family Offices

- Establish clear **governance and reporting frameworks.**
- Build a culture of **questioning and double-checking.**
- **Train all stakeholders** — including family members — to recognise risks and scams.
- Implement **simple but effective controls:** MFA, reconciliations, layered authorisation, backups, and video verification for sensitive requests.
- Stay proactive: use **monitoring tools** to detect misuse of principals' names and likenesses online.
- Have a simple 1 page list of who to call and when, in the case of a **breach or an incident.**

CAXTON fladgate OneCollab

For a confidential conversation about your family office's cyber resilience, contact **Michael Oldham:**

BOOK YOUR CONFIDENTIAL CALL

SAFEGUARDS

5 Practical Safeguards for Family Offices

Family offices face a unique challenge: **balancing discretion and efficiency** with the need for **robust security.** While technology plays an important role, the biggest risks often come down to **people, culture, and governance.** Here are **five safeguards** every **family office** should put in place:

1 Build a Culture of Vigilance

Cybersecurity isn't just a technical issue — it's **cultural.** Leadership must set the tone from the top. If principals and executives don't take it seriously, neither will staff.

- Make **cybersecurity awareness** part of everyday conversation.
- Provide **regular training** not just for employees, but also for family members, who may be more vulnerable to scams.
- **Encourage questioning:** it's always better to double-check than to make an expensive mistake.

2 Strengthen Governance & Workflows

Strong governance makes it harder for cybercriminals to succeed. Even the most sophisticated deepfake will fail if the right checks are in place.

- Apply the **"four eyes, not two"** principle — no major transaction should ever be authorised by a single person.
- Ensure **independent verification:** each approver must review as if they were solely responsible.
- **Reconcile all accounts regularly** against **bank records** (not just ledgers). Simple reconciliations are a powerful safeguard.
- Make **cybersecurity and reconciliation reporting** a standing item at every board meeting.

3 Verify, Don't Assume

Deepfakes succeed when people **act in haste.** Slow down and **verify requests.**

- Never trust phone numbers or details listed in an email — always use **verified contact details already saved.**
- For urgent or unusual requests, confirm **face-to-face or via secure video call.**
- Avoid relying on **one-line emails or text messages** for payment instructions.

SAFEGUARDS

5 Practical Safeguards for Family Offices (continued)

4 Get the Basics Right

Many attacks succeed not because systems are weak, but because **simple controls aren't consistently applied.**

- Use **multi-factor authentication (MFA)** everywhere — and enforce it.
- Replace passwords with **passkeys** wherever possible.
- Restrict access by **geography and role** — not everyone needs access to everything.
- **Regularly test your controls,** including backups: are they working as intended, or just assumed to be?

5 Plan for Response, Not Just Defence

Even the **best defences can be breached.** The difference between a near miss and a disaster often lies in how quickly an **organisation responds.**

- Have a **clear response plan** covering who to call, what steps to take, and how to communicate.
- **Work with trusted advisers** — legal, IT, and communications — to ensure plans are practical and rehearsed.
- Monitor for **misuse of principals' names and likenesses online,** so reputational attacks can be caught early.
- **Consider insurance** – they will have access to additional specialists that can step in during a breach.
- **Learn from incidents.** Every close call should improve your systems and culture.

CAXTON fladgate OneCollab

For a confidential conversation about your family office's cyber resilience, contact **Michael Oldham:**

BOOK YOUR CONFIDENTIAL CALL