



How UK Family Offices Look to an External Cyber Security Scan

What a non-intrusive external assessment of 132 family-office websites found, and why the cheapest control in the report is also the most urgent

Purpose

To explain in plain English what an outside observer can see of this sector's web estate, to report what our assessment found, and to set out realistic actions a small office can take without a security team.

Source	One list of 132 tracked family-office websites , counted by website rather than by legal entity or brand. No website on this list appears on any other finance list we track, so no firm is counted twice across our finance reporting.
Evidence	One assessment, 28 September 2026, every website scanned the same way in a single run. Four produced no usable score and are excluded from every figure. That leaves 128 reported : 113 with an exact score and 15 with a floor score.
Method	Non-intrusive external assessment using publicly observable information: websites, domain records, certificates, public threat intelligence and publicly reachable services. No logins, password attempts or intrusive probing.
Limits	Nothing here says any firm has been broken into. Nothing here is a legal or compliance judgement. Everything here is what was visible from outside on one day.
Prepared by	Huro Data Technologies Ltd / MyDomainRisk
Date	28 September 2026

Research and external assessment: [MyDomainRisk](#) | Huro Data Technologies Ltd

For information: Our scans use bounded, external, non-intrusive checks. They do not attempt exploitation, credential testing or intentional modification of target systems.

Executive summary

The four things that need attention

1. Eighty-one firms of 128 cannot stop email being forged in their name, and 45 of those publish no usable instruction at all. In a sector whose core business is moving family money on written instruction, this is the most direct fraud route in the report and the cheapest thing on this page to fix.

2. Twenty-seven firms have a port answering the internet that probably should not be. Twenty-six of the 27 include a file-transfer login. A database product was actually identified on five, and all five of those sit on shared hosting servers that also carry unrelated organisations' websites.

3. One firm is named on ransomware leak sites, by three different groups. It needs entity and date matching in restricted handling before anyone draws a conclusion from it.

4. Four firms run software carrying a weakness on the public list of those being exploited. One of the four is an Apache web-server flaw that can expose files and, in some configurations, allow code to run. That is the one to check first.

Everything above is small in count and serious in kind. None of it means a firm has been broken into, and every item needs private validation first. **Eleven firms of 128 are in good order and 25 sit in the lowest band,** 18 of them on an exact score.

What we found, worst first

What it is, in plain English	Why it matters	Firms
Named on a ransomware leak site	A criminal group has published the name. May be historical or a similar entity; validate first.	1
A database product answering the internet all five on shared hosting servers	Databases hold client and family records. Reachable from the internet is rarely intended.	5
Software weakness on a public list of those being exploited	Four firms, one entry each. The Apache entry is the serious one; two are a flaw that only takes a site offline.	4
Any risky port answering, counted against the firm a service identified, or an address used only by that firm	Doors that normally face inwards. The 12 database ports sit inside this 15.	15
The same risky ports, on an address shared with others	Nothing identified running. Reported separately because only the provider can confirm or close it.	12
Certificate or encryption problem	Fourteen accept outdated encryption; one has a certificate fault.	15
No instruction to a browser about content security	The most common single gap on the readable sites, 102 of 113.	102
Cannot stop email being forged in the firm's name	A forged instruction to move money is this sector's defining risk.	81

Rows overlap and must never be added; the 15 counted against firms and the 12 on shared addresses are the 27 observed. Three firms also carry a poor-reputation listing on a public threat feed.

Executive summary, continued

The credential result is the surprise, and it needs reading carefully

Almost nothing in the stolen-password collections

Across all 128 websites the criminal credential sources returned **no staff account records and no client account records at all**. Five firms had a single record each for a member of staff on an outside platform, and one firm's own login address appears in the logs. That is five records in a sector where comparable finance lists carry hundreds.

Read it as a measured result, not as safety. These are small organisations with few staff and few public-facing accounts, so there is simply less to harvest. It is not evidence that no office has been compromised, and it says nothing about the personal devices and personal email accounts through which family-office work frequently passes.

Why some firms have a floor score rather than an exact one

Some websites answer an automated visitor with a protection page rather than the real homepage. That is a security control working, not a fault, but it means we cannot read the instructions the site sends to a browser, and those form part of the score. For **15 firms** that was the only gap, so we publish a **floor score**: every unread instruction counted as absent, "at least this much", so **the true figure can only be the same or higher**.

Scores	Firms	Average
Exact scores	113	60.7
Floor scores, counted at their floor	15	50.4
All published figures	128	59.5

Use 60.7 for the sector's measured position and 59.5 for the most cautious one. Were every unread instruction present and correct, those 15 firms would average 73.1 rather than 50.4. **That is an upper bound on what the evidence permits, not a prediction.** Only 12% of this list returns a protection page, so unlike some estates we have measured, very little of this position rests on evidence we could not gather.

A floor score is not a bad score. Fifteen firms carry one and each could sit substantially higher. They are never compared with exact scores or used to rank a firm.

What is going well

No firm carries a known-breach record and none is flagged as unsafe by browser makers. **122 of 128 publish a record naming which servers may send mail for them**, certificates are in good order with a single fault across the estate, and 113 accept only modern encryption. The weaknesses in this report are configuration weaknesses, and nearly all of them are cheap.

Why this matters for family offices in particular

Every sector we assess has the same catalogue of settings. What changes between sectors is which of those settings carries real consequence, and for a family office the answer is unusually clear.

The business is instructions, and instructions arrive by email

A family office exists to act on the family's instructions: move funds, settle a bill, release a payment to a new account, authorise a transfer before a deadline. Those instructions arrive and are confirmed by email, frequently between a small number of people who know each other well and who are used to acting quickly.

That is precisely the arrangement a payment-redirection fraud is built to exploit. **The single control that stops a forged message reaching the inbox under the office's own name is a published instruction costing nothing to set, and 81 of 128 offices have not set it.**

Three structural features that shape everything else here

These are small organisations. Many run with a handful of staff and no in-house technology function at all. The website is usually a brochure built once by an agency and rarely revisited, which explains most of the configuration gaps in this report and also means most of them can be fixed by one conversation with whoever hosts the site.

The hosting is shared. Twenty-six of the 27 port findings involve a file-transfer login, and the database ports sit beside it in the standard layout of a shared hosting server. This is not a sector running its own infrastructure badly. It is a sector sitting on commodity hosting whose defaults nobody has reviewed.

The confidentiality is the asset. A family office holds who the family is, what they own, who advises them and when money moves. Much of that is material no public register carries, and the harm from its disclosure is not primarily financial.

A way of picturing what we did

Imagine somebody walking down a street. They never go inside, never try a door. They notice what is visible from the pavement: a window left open, a side gate unlatched. None of that means the house has been burgled. It means somebody passing can see opportunities, and most take a minute to put right.

That is this assessment. We looked at each website from the public internet, the way any visitor would. We did not log in anywhere, try any password, or look at anything not already on public view. Standing in the street also tells you nothing about the alarm or the internal locks, which is why nothing here is a verdict on any firm's security.

Three cautions that apply to every number in this report

A score is a floor, not a verdict. It records what was visible from outside on one day. **Counts are of websites, not of problems.** A firm with five instances of one issue counts once. **Rows in a table overlap and must never be added.** Where two rows describe the same evidence from different angles, the table says so.

1. The words used in this report

Security reporting runs on jargon. Everything measured here can be described in ordinary language, and this page does that once so the rest of the report can be read without a glossary.

The technical term	What it actually means
Email authentication SPF, DKIM, DMARC	A published instruction telling other mail systems what to do with a message that claims to come from the firm but fails the checks: refuse it, send it to spam, or do nothing.
Certificate	The file that proves a website is who it says it is and encrypts the connection. A fault in it is visible to every visitor.
Legacy encryption old TLS protocols	An outdated way of scrambling the connection that is still accepted alongside the modern one. Invisible to visitors, useful to an attacker already positioned to exploit it.
Browser instructions security headers	Short directions a website sends with each page telling the browser how to behave: refuse insecure content, do not let other sites embed this one, do not guess file types.
A port answering	A door on an internet address that responds when knocked. Some are meant to be open, such as the one serving the website. Others, for file transfer, databases or remote administration, usually are not.
File transfer login FTP	An older way of uploading files to a website. It is a login prompt facing the internet, and where encryption is not enforced it sends the password across unprotected.
Version-inferred weakness	The software announced its version number, and that version is publicly known to have a flaw. It does not show the flaw is reachable or unpatched, because suppliers routinely fix without changing the version.
Known-exploited list	A public list of weaknesses criminals are actively using. A weakness on it is more urgent than one that is not, and this report counts only entries found on the list, never those merely checked against it.

One abbreviation, two meanings

In this report **CAA records** means Certification Authority Authorization, a domain record naming which companies may issue certificates for the domain. It is unrelated to any regulator.

2. Where these firms sit in the rules

This sector's regulatory position is genuinely mixed, and the report does not assume otherwise.

Many single family offices sit outside the regulatory perimeter, because serving one family's own wealth is not ordinarily a regulated activity. **Multi-family offices and those providing investment services to others are typically authorised** and carry the full obligations that follow. This assessment looked at websites, not at permissions, so **it does not know which firms on this list are authorised and makes no claim about any of them.**

Where the rules do apply, they apply here

For an authorised firm, the FCA's operational-resilience rules treat client-facing services and trustworthy communications as dependencies to be identified, owned and either tolerated or fixed.^[1] A mail domain that cannot refuse a forgery in the firm's name is exactly such a dependency.

Data protection applies whether or not a firm is FCA-authorised. Every office on this list holds personal data about the family, its members and its advisers, which brings the UK GDPR and the cookie rules into scope on the strength of that alone.^[2] The consent findings in section 8 sit under that regime, not under financial regulation.

Why a small office is not thereby a low-risk one

Firm size governs capacity to respond, not attractiveness to an attacker. The money a family office moves and the confidentiality it holds are not proportional to its headcount, and a fraud attempt costs the same to attempt against two people as against two hundred. The practical consequence runs the other way: a sector-wide instruction lands unevenly on offices with no technology staff, and most will need a supplier to act rather than a deadline.

How this differs from the statistics you may have seen

Most sector cyber statistics are surveys. They ask organisations what they have in place and depend on what respondents know and will report. This study asked nobody anything. Every figure is an observation taken from outside, on one day, using the same routine on every website.

The two approaches answer different questions and neither replaces the other. A survey tells you what a sector believes about itself. An external assessment tells you what it is showing to the world.

3. What we measured, and how to read the numbers

Each website was checked against the same set of external tests and given a score out of 100 where enough evidence came back. **Good** is 75 or more, **needs improvement** is 50 to 74, and **at risk** is below 50.

Coverage	Websites
Tracked websites	132
Appearing on any other finance list we track	0
Excluded, completed without a score	4
Reported	128
Exact scores	113
Floor scores	15

No scan failed. Of the four excluded, three could not have their certificate and browser instructions assessed and one returned no internet-exposure evidence. They are excluded from every figure on the owner's instruction rather than counted as zeroes, and nothing in this report describes them.

This list stands alone

No website here appears on any other finance list we track, so nothing in this report overlaps another and no figure needs an adjustment for double counting. **The numbers describe 128 distinct family-office websites and nothing else.** One comparison is drawn, with the published UK wealth and investment management assessment, and it is confined to section 4 continued and quoted as rates only.

Four rules this report follows throughout

Counts are of websites, not of problems. A firm with five instances of the same issue counts once. One unpatched piece of software can generate dozens of technical observations, which is why we report affected firms rather than observations.

Rows in a table overlap and must never be added. The clearest case: 15 firms have a risky port counted against them and 12 of those have a database port, but the 12 sit inside the 15.

Every percentage names its denominator. Most are shares of the 128 reported websites. Some checks could only answer for fewer, and those tables say so, in the form 100 / 113 readable with the rate beside it. Where a check returned an unknown, the denominator is the number that answered, because an unknown is not a pass.

Stolen passwords come in three separate populations, covering different people and fixed by different parties. Section 6 sets them out and they are never combined into one headline number.

4. The estate: 128 reported websites

From here on every figure describes the 128 reported websites.

Band	On exact scores 113 websites	Including floor scores 128 websites
Good, 75 and above	11 (10%)	11 (9%)
Needs improvement, 50 to 74	84 (74%)	92 (72%)
At risk, below 50	18 (16%)	25 (20%)

Exact average **60.7**, median **62**. Counting the 15 floor scores at their floor gives **59.5**, median **61**. Those floors average 50.4 and would average 73.1 if every unread instruction turned out to be in place. **The seven extra at-risk results in the right-hand column are floor figures and may all sit higher.**

The shape of this distribution is the finding

Eleven of 113 exactly scored firms reach the top band. Eighty-four sit in the middle, and eighteen are confirmed in the lowest. **This is not a sector with a few bad outliers.** It is a sector where the middle itself sits low, which is what you would expect when most of the estate is brochure websites on commodity hosting that nobody has revisited since they were built.

That is also the encouraging reading. A distribution with no long tail of catastrophic cases, and a middle held down by ordinary settings, moves a long way on cheap work rather than on a security programme.

What the score alone does and does not tell you

A score is built from many ordinary settings, so a firm can sit in the top band and still carry one of the serious findings in section 5. **The bands measure hygiene. The serious findings measure consequence, and they are not the same thing.** The firm named on ransomware leak sites, the five with a database product answering and the four carrying a known-exploited weakness should be read from section 5, not from this table.

Point sum 6,860 across the 113 exact scores; published sum 7,616 across all 128. Percentages are rounded and may not total exactly 100.

4 continued: how this compares with UK wealth and investment management

One comparison is worth drawing, against the nearest sector we measure on the same routine: our published **UK wealth and investment management** assessment of 26 September 2026, **184 scored websites** from a wealth manager list and an investment manager list with each firm counted once. **No firm appears in both that population and this one.** Every figure below is a rate, because the populations differ in size.

Measure	Family offices 128 scored	Wealth and investment 184 scored	Direction
Exact-score average	60.7	71.2	Worse
In the top band, of exact scores	10%	28%	Worse
Forged email not refused	63%	29%	Much worse
No usable email policy at all	35%	7%	Much worse
Consent mechanism, of readable sites	12%	55%	Much worse
Named on a ransomware leak site	1%	3%	Better
Staff or outside-service credential record	4%	47%	Much better
Client-account records held	0%	56%	Much better

Where family offices are worse, and why it is not a surprise

On configuration, family offices are behind on almost everything: ten points on the average, close to a third of the top-band rate, and much wider gaps on the settings that cost nothing. These are things an agency sets once and nobody revisits.

Three differences carry consequence rather than hygiene. Risky ports counted against the firm run **12% against 3%**, version-inferred weaknesses 10% against 4%, and five family offices have a database product answering the internet where one firm does on the larger list. All three trace to shared commodity hosting, which this sector uses and that one largely does not.

Where family offices are better, and what that is worth

The credential gap runs the other way, and it is the largest difference on the page. Four per cent of family offices carry a staff or outside-service record against 47% of wealth and investment firms, and no family office holds client-account records against 56% of that population. Those firms hold 953 staff records and 75,696 client-account records where family offices hold none of either.

Read it as a consequence of size and shape, not of better practice. A firm with six staff and no client portal has almost nothing to harvest, and the same offices are behind on every control they do operate.

Comparator figures are the published UK wealth and investment management assessment of 26 September 2026, same scan method, quoted as rates only. Its wealth-manager component alone (89 scored) sits a little below the combined figure; the combined population is used here because it is the published one. The two credential rows are separate because the comparator publishes them that way and gives no single figure covering all three populations. Content security policy is absent on 90% of readable sites here against 43%. The lists are level on SPF records (95% each); floor scores run 12% here against 18%, the lowest band 16% against 7%, certificate authority records 2% against 12% and legacy encryption 11% against 7%. **No firm is ranked across the two populations and the averages are never combined.**

5. The findings that carry real consequence

These are the items that would matter on a Monday morning. They are small in number and they do not follow the score bands: a firm can sit in the top band and appear here.

Finding	Firms	Rate
Named on a ransomware leak site	1 / 128	1%
Risky ports counted against the firm a service identified, or an address used only by that firm	15 / 128	12%
of which a database port	12 / 128	9%
of which a database product actually identified	5 / 128	4%
Risky ports only on a shared provider address, nothing identified	12 / 128	9%
Software weakness read from a version number	13 / 128	10%
of which on the known-exploited list	4 / 128	3%
Poor public reputation on a threat feed	3 / 128	2%
Certificate, protocol or cipher issue	15 / 128	12%
Known breach records or browser-safety warnings	0 / 128	0%

One ransomware leak-site reference, and how to handle it

One firm appears on ransomware leak sites, named in posts by **three different groups**. On this evidence it is the single most consequential row in the report.

A listing is a criminal group's claim, not a verified fact. It can be historical, duplicated across sites, or refer to a similarly named entity elsewhere. The right response is restricted matching of entity, date and incident record with whoever handles incidents for the firm, and **it must not be published against a named firm without that validation.**

The software weaknesses, and what the four exploited entries are

Thirteen firms show software weaknesses on a reachable service, across **420 observations**. Every one was read from a version number and none was confirmed by the source. A version match does not show the vulnerable feature is in use, or that a fix has not been applied without changing the version, which suppliers do routinely. The count to report is thirteen firms, not 420 observations.

On the known-exploited list	Firms	What it would mean if it is real
Apache web-server flaw	1	Can expose files and, in some configurations, allow code to run. Check this one first.
HTTP/2 Rapid Reset	2	Overloads a web server so the site goes offline. Gives no access, and applies only where HTTP/2 is enabled, which this scan did not establish.
jQuery scripting flaw	1	Concerns code delivered to a visitor's browser rather than the firm's own systems.

The four were matched from the version the service reported, not confirmed on the site. They are not equivalent to one another, which is why they are listed separately rather than as a count of four.

5 continued: the exposed services, and whose server they sit on

Twenty-seven firms have a port answering that probably should not be. Each case was checked individually on two questions: did a named product, version or protocol actually answer on the flagged port, and do unrelated organisations resolve to the same address?

What was observed	Firms	Treatment
Database product identified MySQL, MariaDB or PostgreSQL, all on shared hosting servers	5	Counted against the firm
File-transfer server identified, no database product three of the five also show a database port	5	Counted against the firm
Nothing identified, address used only by the firm four of the five show a database port	5	Counted against the firm
Nothing identified, address shared with unrelated organisations	12	Reported separately

Rows are exclusive and sum to the 27 cases observed. The 15 counted against firms carry 29 distinct port observations between them and the 12 reported separately a further 21, six of which include a database port. An identified service is counted against the firm whatever else shares the address, which is why the five database cases stay in the headline despite sitting on shared servers.

This is one finding, not twenty-seven

A file-transfer login is present on 26 of the 27 cases. The database ports sit beside it, in the positions a standard shared-hosting server uses. Every one of the five firms whose database product was actually identified is on such a server, and so are the twelve reported separately.

That makes this a hosting question before it is a firm question. **A handful of commodity hosting configurations, not twenty-seven independent mistakes, account for almost the whole of this sector's exposed-service surface.** It is still the firm's data on those servers, and the firm, not the host, carries the consequence if something goes wrong with it.

A file-transfer login matters for two reasons. It is a login prompt facing the open internet, so it attracts automated password guessing continuously. And where encryption is not enforced on it, the password crosses the internet unprotected every time the site is updated.

A port answering is not the same as a vulnerability. A service may be deliberately published, restricted to known addresses, or run by the host on the firm's behalf. What it does mean is that the door is visible and somebody should confirm what is behind it. For almost every firm here that is a single written question to the hosting provider.

Three firms carry an elevated public reputation finding on a threat feed, in each case a single listing. A listing describes an address rather than necessarily the firm using it, so tenancy should be confirmed before any of the three is attributed.

6. Stolen credentials: three populations, and a near-empty result

Credential exposure is reported in three separate populations. They describe different people, carry different consequences and are fixed by different parties, so **they are quoted independently and never added into one figure**. The source answered for all 128 reported websites and its three buckets reconciled on every one.

Population	Who it concerns, and who can fix it	Firms	Records
1. Staff accounts	Accounts on the firm's own domain. Fixed by the firm, through reset, revocation and multi-factor sign-in.	0	0
2. Identities elsewhere	The firm's own work identities on somebody else's platform. Fixed by the firm, but through a reset on that platform.	5	5
3. Client accounts	Members of the public holding an account on the site. Cannot be fixed by the firm at all.	0	0
No records at all	Firms with nothing in any of the three populations. A measured zero, not an absent answer.	123	96%

Why this result is unusual, and what it does not prove

In comparable finance estates the staff bucket alone runs to hundreds of records. Here it is empty, and the second bucket holds five single records across five firms. **This is the strongest credential result we have measured in this sector's neighbourhood**, and it should be reported as such.

It is also the least informative good news in the report. These are small organisations: a firm with six staff has six addresses to be harvested, and a firm with no client portal has no client accounts to lose. The measurement is of what circulates publicly, not of how well identity is managed.

And it does not cover the route this sector actually uses. Family-office work frequently passes through personal email accounts, personal devices and family members' own machines, none of which carries the firm's domain and none of which this measurement can see.

One firm's own internal login or administration address also appears in the stolen-password logs. That is a separate observation from the five records above and describes a different thing: not a credential in circulation, but the firm's own sign-in page named in material criminals are trading. It is a reason for that firm to check its exposed administrative routes.

All of this comes from criminal logs rather than from anything the scan observed on the firms' public systems. Counts are not verified unique people, current accounts or working passwords. **Never test a recovered credential.** Named evidence stays in the restricted application and should be reconciled against authorised identity records before anyone acts on it.

7. Forged email: the largest gap in this report

Anyone can put a firm's name on an email. What stops it reaching the inbox is a published instruction telling receiving mail systems what to do with a message that fails the checks. It can say refuse, send to spam, or do nothing.

What the firm publishes	Firms	Share of 128
Refuse the forgery	20	16%
Send it to spam	27	21%
Do nothing, monitoring only	36	28%
No usable policy observed	45	35%

Eighty-one firms, 63%, do not instruct refusal or spam filing at all. Thirty-six publish a policy set to do nothing and **45 have no usable policy whatever**, which is the largest single group in the table. Only 20 firms of 128 instruct outright refusal.

Why this is the most consequential row in the report

In most sectors a forged email is a phishing nuisance. In a family office it is the opening move in a payment-redirection fraud: a message that appears to come from a principal, an adviser or the office itself, about a real transaction, asking for a change to payment details or authorising a transfer before a deadline.

The arrangement being exploited is the one that makes the office work: a small, trusted group acting quickly on written instruction. **The control that stops the message arriving under the office's own name is a published instruction costing nothing to set, and it is the cheapest item in this report with the most direct consequence.**

The work behind it is harder than the result suggests. Publishing the instruction takes minutes; doing it safely does not. A firm has to know every system that sends mail in its name, the accountant, the custodian, the newsletter tool, the booking system, and watch for long enough to be confident, or genuine correspondence starts being refused. **The right sequence is watch, then file to spam, then refuse**, and the 36 firms already publishing a monitoring-only policy are further along that path than the 45 with nothing at all.

The supporting records

Control	Have it	Do not
Record naming which servers may send mail	122	6
Signing record on the names we sampled	80	48
Encryption reporting record	6	122

A missing signing record means none was found under the names we sampled, not that none exists. Published records describe what a firm asks other systems to do; they do not prove a forgery would in fact be refused, because receiving systems apply their own judgement. **The first row is this sector's best result on any control measured**, which makes the gap in the refusal instruction harder to explain rather than easier: most of these firms have already done the preparatory work.

8. Cookies, consent and tracking

This concerns what happens on a visitor's own device, and it sits in a regime that applies to every firm on this list whether or not it is FCA-authorised.

Read this before the number

Our privacy check scored **49.7% of the points it was able to assess**, 1,065 of 2,143. **That is not 50% compliant with anything.** It scores a handful of visible technical settings and nothing about how a firm actually handles personal information.

What we looked for	Yes	No	Could not tell	Why it matters
Insecure requests redirected to the secure site	101	14	13	Anything typed into an insecure page can be read on the way.
No insecure content on a secure page	100	13	15	A padlock is weakened if parts of the page arrive unprotected.
Privacy policy route found	41	61	26	People should be able to find out what happens to their data.
Cookie consent mechanism found	13	100	15	The law governs what may be stored before a person chooses.
Published vulnerability-disclosure policy	1	88	39	Someone who spots a flaw needs a way to tell the firm privately.

One hundred of the 113 websites we could read showed no consent mechanism, 88%, and 61 of 128 have no privacy-policy route we could locate. Fifteen homepages were not readable, so their consent state is unknown rather than assumed clean.

The first row asks whether an insecure request is redirected; section 9 asks the stricter question of whether secure connections are enforced, which 101 also pass but with a different unknown count. This row asks whether a *disclosure policy* is published; sections 9 and 10 ask whether the standard *security contact file* is present. Both are right for the question each asks.

Two rows that would not be acceptable anywhere else

One of the 89 websites we could check publishes a policy saying how it wants a security problem reported. The other 88 do not, and 39 could not be checked either way, so they count as unknown rather than as failing. Someone who finds a weakness at one of the 88 has no obvious way to tell them, which is how problems end up disclosed in public. It is a short page and a single file, and both cost nothing.

Thirteen of 113 readable sites offer a consent mechanism. An absent mechanism on a brochure site that sets no cookies may be lawful, which is why the next paragraph matters more than the number.

What the websites store

Cookie evidence came back for 111 websites. **51 stored something during the first page visit, 108 items in total.** Of those 51, 34 stored an item without the setting limiting it being sent from other websites, 30 without the setting hiding it from page scripts, and 22 without the setting keeping it off insecure connections. Tracking was observed on 26 websites, a tag manager in every case.

Only a response that was the site's real homepage is counted. Collection was skipped for 11 websites and unavailable for 6. This sees only the first page request, so the real numbers are higher, and not every item needs every setting. **A site that genuinely sets no non-essential storage needs no consent banner**, so the 100 is a list to check in a browser rather than 100 breaches.

9. Card payments and transport security

Most firms on this list do not take card payments, so the card industry standard will not apply to all of them. It applies wherever a firm handles card data or runs something connected to a system that does, and that is decided by payment flows rather than by what kind of business it is.

Two things this section is not

Our payment-surface check scored **83.9% of the points it could assess**, 1,836 of 2,189. Controls we could not verify were removed from the calculation rather than counted as passes, which is exactly why that number is high. **It does not mean 84% compliant.** Three controls could not be answered for a single firm in the estate.

And **this is not the scan the card standard requires.** That standard requires quarterly scans by a company specifically approved by the card industry. We are not one, and nothing here can be submitted as evidence of compliance.^[3]

External signal, of 128 reported	Pass	Issue	Could not tell
No Heartbleed weakness	128	0	0
Valid certificate	127	1	0
No software weakness reported	115	13	0
Modern encryption only	113	14	1
No database port answering	110	18	0
Visitors forced onto a secure connection	101	13	14
Browser told never to try the insecure version	53	60	15
Route to report a security problem published	1	87	40
Cloud storage, mail encryption, mail relay	0	0	128

The 18 database-port issues are this check's own result and include the 6 reported separately in section 5, which is why the firm-level database count is 12. **The last row is the honest part of this section:** three controls could not be answered for a single firm, and they were excluded from the calculation rather than recorded as passes, which is precisely why the headline percentage is high. An unknown is not a pass.

Transport is the largest practical job here

Thirteen firms do not force visitors onto a secure connection and **60 do not tell the browser to stop trying the insecure version**, which means the first request of every visit is exposed even where a redirect exists. The two belong in one piece of work, and the second is the single most common correctable gap in this report after email. Fourteen still accept outdated encryption and one has a certificate fault: different jobs, the first invisible and mattering only to an attacker already positioned to use it, the second visible to every client who visits.

10. Domain controls and the dependency nobody records

Control	Have it	Do not	What it does
Mail server record	122	6	Names which servers may send mail for the firm.
Mail signing record	80	48	Signs outgoing mail so it can be verified. Sampled, so absence is not conclusive.
Signed domain records	7	121	Stops someone forging the answer to 'where is this firm's website'.
Encryption reporting record	6	122	Asks other systems to report failures in protecting mail in transit.
Certificate authority record	2	126	Names which companies may issue certificates for the domain, so a rogue one is refused.
Security contact route	1	87	A published file telling a researcher where to report a problem privately.

Four of these six controls sit below 6% adoption. A gap shared by more than nine firms in ten is a sector fact rather than 120 individual failures, and it is a natural candidate for a coordinated push through an industry body or a shared supplier rather than 128 separate projects. Certificate authority records at 2 firms and signed domain records at 7 are the two that most directly protect the firm's own identity on the internet, and they are the two least adopted.

The dependency that is on nobody's risk register

Observation	Firms	Rate
Mail transport policy finding	125 / 128	98%
All address records with one provider	111 / 128	87%
Some form of network concentration	85 / 128	66%
Risky port on a shared provider address	12 / 128	9%
Internet address with a poor public reputation	3 / 128	2%

These overlap and must not be added. A flagged address can belong to another organisation sharing the same infrastructure, so ownership needs confirming first.

111 firms, 87%, depend entirely on one company to answer the question 'where is this firm's website'. That is not a fault. Concentration is usually the better-resourced choice for an office with no technology staff, and splitting the job across providers brings its own problems. **The question is whether anyone has written it down.** For most firms here the same supplier holds the website, the hosting, the domain records and frequently the mail, so a single supplier failure reaches every one of those at once. The shared-hosting concentration in section 5 is the sharpest instance of the same point.

Domain expiry and transfer-lock observations are deliberately excluded from this report. The public evidence does not show whether automatic renewal is switched on and is not reliable enough to support a finding either way.

11. What we could not read

Two different limits apply, and they are not the same thing. Keeping them apart is what stops a gap in evidence being reported as a finding.

Situation	Websites	What it means
Floor score	15	The site turned our scanner away with a protection page. Everything else was read. The score is published as a floor and can only be higher.
Excluded, completed without a score	4	Core evidence was missing: on three the certificate and browser instructions could not be assessed, on one no internet-exposure evidence came back. Excluded from every figure on the owner's instruction. No scan failed.

A protection page is a locked gate, not a hole in the fence

A site that refuses an unknown automated visitor is exercising a security control and doing something sensible. The consequence for us is simply that we cannot read the instructions that site sends to a browser, and those are one of the things the score is built from.

This cannot be fixed from our side. No amount of rescanning will change it without the firm or its provider choosing to let the scanner through. It is not evidence of a problem and should never be reported as one. At 12% of this list it is also the smallest such gap we have had to report on a finance estate, so very little of this picture is provisional.

What else we could not see

Evidence type, of 128 reported	Got it	Partly	Could not
Website instructions to the browser	113	0	15
Homepage content, for consent and tracking	113	0	15
What the website stores on a device	111	0	17
Other systems on the same infrastructure	121	7	0
Direct mail server test	5	0	123
Mail resilience	4	124	0
Cloud storage discovery	0	128	0

These limits apply to scored websites too, so a score does not mean complete evidence and this report never treats it as if it did. Cloud storage could only be partly checked everywhere, which is why that control appears as unknown throughout rather than as a pass. Direct mail server testing ran on five websites and still produced no definitive answer on mail encryption or relay status, and registration data was unavailable for six.

The remedy is diagnosis, not repetition. Running the same blocked request again establishes nothing, and no score is invented in the meantime.

11 continued: the review of what else sits on these names

Separately from the scan, a review looks at the other host names that appear in each firm's certificate history and infrastructure. It is the one check in this report that came back close to complete.

Small estates, and a clean result on the thing that usually goes wrong

The review ran on all 132 tracked websites and reviewed certificate history for every one. It is complete for 125 and partial for 7, because 14 individual discovered hosts could not be assessed. Across the 128 reported websites it found **506 related host names, a median of two per firm and at most 28**, so no firm came near the 50-host review limit.

No firm published an address pointing at a service that does not exist, or at an unconfigured hosted service. That is the finding this check exists to catch, and on this estate it is empty.

261 host names, across 56 firms, appear only in expired certificates. Those are names that once had a certificate and may since have been abandoned: an old staging site, a campaign microsite, a service that was retired without anyone removing the name. None of that is a security finding on its own, and the right response is an inventory question rather than remediation. A name nobody remembers owning is a name nobody is watching.

Two honest limits on that result. The review is **a bounded check of the addresses each host publishes; it did not test who controls any resource**, so it cannot say that nothing is dangling, only that nothing it could see was. And hosts that only ever appeared in a wildcard certificate, or that never had a certificate at all, will not appear in it. **A clean result here is reassuring and is not proof.**

The small estate sizes are themselves consistent with the rest of the report: a median of two related host names per firm describes an organisation with one website and very little else, which is what most of this sector is.

12. What to do, in order

Ordered by consequence, not ease. These groups overlap and are not a count of separate firms. Almost every item here is a conversation with an existing supplier rather than a project.

1	Validate the one ransomware leak-site reference Match entity, date and incident record privately. The firm is named in posts by three different groups, which makes duplication across sites more likely rather than less. Never publish it against a named firm.
2	Move towards refusing forged email, starting with the 45 The largest and cheapest win in the report. Begin with the 45 firms publishing no usable instruction at all, then the 36 set to do nothing. Inventory every legitimate sender first, then watch, then file to spam, then refuse. Investigate the 48 sampled signing-record gaps and 6 missing mail server records alongside.
3	Check the Apache entry, then the other three known-exploited cases Four of the 420 version-read observations are on the public exploited list. The Apache flaw can expose files and in some configurations allow code to run, so confirm the software actually running on that firm first. The two Rapid Reset entries can only take a site offline; the jQuery entry concerns visitors' browsers.
4	Write to the hosting providers about the 27 port cases Start with the five where a database product was identified. Ask which services are meant to be reachable, whether file transfer can be closed or encryption enforced on it, and what the contract says about breach notification. One letter covers most of these firms because they share a handful of hosts.
5	Fix transport, then the browser instructions Thirteen firms not forcing a secure connection, 60 without the instruction that stops the browser trying the insecure version, 14 accepting outdated encryption and one certificate fault. Confirm the 3 poor-reputation addresses against tenancy.
6	Open the 100 websites in a browser and watch what happens The consent question cannot be settled from outside. Ten minutes per site, no specialist needed. A brochure site that genuinely stores nothing needs no banner, so this exercise will clear many of the 100 rather than add to the work.
7	Reset the five outside-service records, and check the one named login page Five records across five firms is the smallest credential task in any report we have produced. The reset happens on the other company's system. Separately, one firm has its own internal sign-in address named in criminal logs and should review what is reachable there.
8	Publish a privacy route, a disclosure route and the domain records Sixty-one firms have no locatable privacy policy, 88 of the 89 we could check publish no disclosure policy, 87 of 88 no security contact file, 126 no certificate authority record and 121 no signed domain records. Each is a one-off publication, and at these adoption rates they are better done once across the sector than 128 times separately.
9	Tidy the 261 abandoned names, and close the evidence gaps Fifty-six firms carry host names that appear only in expired certificates. Confirm each is genuinely retired and remove it. The four unscored websites need a completed run and the 15 floor scores a decision on whether the scanner may read them.

Conclusion

This sector's problem is not a small number of bad firms. It is that the middle sits low. An exact-score average of 60.7 with 11 of 113 firms in the top band and 84 in the middle describes an estate where ordinary settings have gone unreviewed almost everywhere, rather than one with a dangerous tail. Eighteen firms are confirmed in the lowest band and seven more may be, which is a real group but not the shape of the problem.

The consequential findings are few and they do not follow the score bands. One firm named on ransomware leak sites, five with a database product answering the internet, four carrying a weakness on the public exploited list. A firm can sit comfortably in the top band and carry any of these, which is why the bands and the consequential findings are reported separately here and should be governed separately too.

The three things that distinguish this sector

Forged email is the defining exposure, not a hygiene item. Eighty-one firms of 128 cannot instruct refusal of a message sent in their name, and 45 publish nothing usable at all, in a business whose core activity is acting on written instruction to move family money.

The exposed services are a hosting story. Twenty-six of the 27 port cases include a file-transfer login, every identified database sits on a shared hosting server, and a handful of commodity configurations account for almost the whole surface. That makes it correctable by supplier rather than by firm.

The credential result is genuinely clean and genuinely uninformative. No staff records, no client records, five single records on outside platforms. It reflects organisations with few staff and no public accounts, and it says nothing about the personal devices and personal email this sector's work runs through.

And one structural point. Most of these offices depend on a single supplier for the website, the hosting, the domain records and often the mail. 111 of 128 have all their address records with one provider. That concentration is usually the right choice for an organisation with no technology staff, but it means one supplier's failure reaches everything at once, and nobody appears to have written it down.

Three things this report does not claim. It does not say any firm has been broken into: we could not see inside one and did not try. It does not know which firms are FCA-authorized, and makes no compliance judgement about any of them. And where it compares this estate with the published wealth and investment management assessment, it compares rates between two independent populations and never ranks a firm across them.

One thing it does claim. The distance between this sector and a good score is made up almost entirely of cheap, externally verifiable, low-risk work: a published email instruction, a browser instruction, a word with the host about file transfer, and four published records. None of it requires a security programme and most of it requires one supplier conversation.

About this report

Produced with MyDomainRisk, a tool developed by Huro Data Technologies Ltd, which has a commercial interest in this analysis and declares it here so readers can weigh it. Every observation was made from outside using public websites, domain records, certificates, cookies and public threat intelligence. Nothing was logged into, no password was tried and nothing was exploited. It is not certification, an audit, legal advice or regulatory advice.

How to read the figures

No website on this list appears on any other finance list we track, so no figure needs an adjustment for double counting. **Every figure describes 128 distinct family-office websites.** The single comparison in section 4 continued sets this estate and the published wealth and investment management population side by side as rates; the two are never combined and no firm is ranked across them.

Bands, and what a score is

Good is 75 and above, **needs improvement** 50 to 74, **at risk** below 50. One serious finding can hold a website below a band however much else is right, and a top-band firm can carry a consequential finding from section 5. **A score is a floor, not a verdict:** it records what was visible from outside on one day, not internal controls, patching, training, payment verification or incident readiness.

Exact scores and floor scores

113 websites have an exact score and 15 a floor score, published as "at least this much" where the browser instructions could not be read. **Floor scores count every unread item as missing**, so the true figure can only be the same or higher, and they are never compared with exact scores. Two averages are given: **60.7** on exact scores alone and **59.5** counting floors at their floor.

Counting, and whose server a port sits on

Every figure counts **websites, not problems**. One unpatched service can produce dozens of observations, which is why firms are counted and observations given only as context: thirteen firms, not 420 observations. Rows overlap and must never be added: the 12 database ports sit inside the 15 cases counted against firms, and the 12 on shared addresses are counted once, on their own line.

Exposure is reported by owner, case by case. A case counts against the firm where a service was identified on the flagged port, or where the address serves only that firm, whoever operates it; separately where nothing was identified and unrelated organisations share the address. **Separate keeps its full weight.** Of 27 observed, **15 count against firms and 12 are reported separately.**

The two percentage scores are not compliance rates

The privacy check scored 49.7%, 1,065 of 2,143, and the payment-surface check 83.9%, 1,836 of 2,189, **of the points each was able to assess.** Controls that could not be verified were removed from the calculation rather than counted as passes, which is why the payment figure is the higher. Neither is an audit or a legal conclusion.

Notes

- Every figure describes the assessment of 28 September 2026. No trend is reported. The comparator figures in section 4 continued describe the published UK wealth and investment management assessment of 26 September 2026, 184 scored websites, under the same scan method.
- The three credential populations are quoted independently and never summed. A zero means a check ran and found nothing, never an absent answer.
- This report does not know which firms are FCA-authorised and makes no claim about the regulatory status of any of them.
- Four websites completed without a published main score and are excluded throughout. The population is tracked websites, not legal entities or brands, and we publish counts and distributions, never a league table.

Sources and notes

[1] Operational resilience: FCA PS21/3

Requires authorised firms to identify important business services, set impact tolerances and understand the dependencies that could cause disruption. Trustworthy communications and client-facing services are dependencies of those services. Whether a particular family office is authorised is a question of its permissions and its activities, which this report did not examine. [FCA PS21/3](#)

[2] Information Commissioner's Office

Guide to PECR: cookies and similar technologies, governing what may be stored on a person's device and the permission needed, and *A guide to data security* under the UK GDPR. These apply to every firm on this list regardless of financial regulation, and they decide whether an arrangement is lawful; the signals in section 8 are technical observations and are not such an assessment. [ICO cookie guidance](#) and [ICO data security guidance](#)

[3] PCI Security Standards Council

The PCI DSS standard and the Council's applicability guidance determine actual scope; payment flows, redirection arrangements and supplier relationships cannot be scoped from an external scan. Requirement 11.3.2 requires passing external scans by an Approved Scanning Vendor at least every three months. An Approved Scanning Vendor is one specifically qualified by the Council, and this assessment is not one. [PCI DSS standard](#) and [applicability guidance](#)

[4] National Cyber Security Centre

Email security and anti-spoofing, including the staged move from monitoring, through spam filing, to refusal, which is the sequence recommended in section 7; *External attack surface management*; *Vulnerability disclosure toolkit*. Free plain-English guidance requiring no specialist team, which matters on a list where most firms have none. [NCSC email security](#), [external attack surface management](#) and [vulnerability disclosure toolkit](#)

[5] MyDomainRisk / Huro Data Technologies Ltd, family offices estate baseline, extraction 28 September 2026

132 tracked websites, 128 reported (113 exact, 15 floor), 4 excluded without a published score. Exact sum 6,860 and average 60.7; published sum 7,616 and average 59.5; floors average 50.4 against a ceiling of 73.1. Bands on exact scores 11 / 84 / 18; including floors at their floor 11 / 92 / 25. Each sum is stated beside the average computed from it, and no website here appears on any other finance list we track.

Provenance and handling

The source is one read-only production snapshot of the latest owner-matched security scan for every currently tracked website on the family offices list, all dated **28 September 2026 and queued as a single run at 11:24 UTC**, under one scan method. Every reported website's latest attempt carries that date. Websites without a published main score are excluded on the owner's instruction and counted in section 11. The analysis refuses to report where an evidence path is absent rather than reading it as zero, and the per-case provider split in section 5 was read from the stored evidence before it was quoted.

Each case of a port answering was classified one at a time from the same scans: the service evidence for each flagged port, and the other websites in the scan data sharing each address. "Used only by the firm" means only that firm among the organisations we have scanned, which is not proof nobody else uses the address. Known-exploited counts only entries found on the public list, never those merely checked against it.

No firm is named in this report. The findings are aggregate by design: a named firm beside its weakness is a document that cannot safely be circulated, and the value here is the sector pattern. Per-firm detail exists and is available privately to the firm concerned, or to anyone it authorises.

Publication rule

Do not describe an individual firm as 'at risk', as non-compliant, or as ransomware-affected on this evidence alone. Everything serious needs the firm to check it privately first. A leak-site listing is a criminal group's claim, not a verified fact, a website that refuses an automated scanner is exercising a security control, and a hosting provider's shared infrastructure is not attributable to a single firm.

For information: Our scans use bounded, external, non-intrusive checks. They do not attempt exploitation, credential testing or intentional modification of target systems.

Every named finding should be rechecked immediately before responsible disclosure, because public-facing settings change constantly. Aggregate figures may be used with the cautions in this report. This document contains counts only: no passwords, no personal records, no raw provider data, no exploit instructions and no named firm detail. A finding is not evidence that any firm has been compromised or is in breach of any obligation.