



How UK Wealth and Investment Managers Look to an External Scan

A September 2026 baseline of 193 firm websites drawn from the UK's largest wealth managers and investment managers, written for people who do not work in cyber security

What this report is

We looked at every firm website in our tracked estate from the outside, the way any client could, and recorded what was visible. We did not log in anywhere, try any password, or touch anything inside a firm's systems. This report says what we saw, what it means in plain English, and what is worth doing about it.

Sources	Two separately tracked lists, reported separately: 96 wealth manager websites and 118 investment manager websites .
Combined	21 firms appear on both lists. The 214 rows therefore describe 193 distinct websites , each counted once. 214 is a count of list entries and is never used as a population.
Evidence	One assessment, 26 September 2026, every website scanned the same way, with a single firm rescanned on 28 September and reported at that later scan. Nine produced no usable score and are excluded: seven completed without one, and two are tracked at an address that is not in the internet's address system while the correct one is confirmed. That leaves 184 reported : 150 with an exact score and 34 with a floor score.
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	26 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. Six firms are named on ransomware leak sites.** A listing means a criminal group has published the firm's name. Each needs matching against the right legal entity and date before anyone draws a conclusion, but this is the item to check first.
- 2. Stolen staff passwords are circulating for 35 firms, 953 records.** That is 27 on a typical affected firm: keys to the firm's own systems that it can take back today.
- 3. Fifty-three firms cannot stop email being forged in their name.** Here that message is the opening move in a payment-redirection fraud, and the control costs nothing to publish.
- 4. Twenty firms have a port answering the internet that probably should not be.** Six are on an address used only by the firm, and only two of those have a service we could identify: a database server and a file-transfer server. The other fourteen sit on shared addresses and are reported separately.

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 have a confirmed lowest-band score** and five more sit there on a floor figure only.

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.	6
An identified database server answering the internet	Databases hold client records. Three further database ports are open on a provider's edge with nothing identified behind them.	1
Any risky port answering, on the firm's own address remote access, file transfer or admin tools	Doors that normally face inwards. The 4 database ports sit inside this 6.	6
Software weakness on a public list of those being exploited	Two firms, one entry each, and both the same flaw: it can take a website offline but gives no access.	2
Certificate or encryption problem	Thirteen accept outdated encryption; one has a certificate fault.	14
The same risky ports, on an address shared with others	Nothing identified running. Reported separately because only the provider can confirm or close it.	14
Stolen staff passwords in criminal collections	953 records, 27 on a typical affected firm, harvested by viruses on staff computers.	35
Cannot stop email being forged in the firm's name	Here a forged email is a direct route to a fraudulent payment instruction.	53
Clients' own account details in circulation	75,696 records. Nobody at the firm can reset these; only the client can.	102

Rows overlap and must never be added; the 6 firm-level and 14 shared cases are the 20 observed. Six firms also carry a poor-reputation listing, two on their own address and four on two shared cloud addresses.

Executive summary, continued

Stolen passwords, and what the figure actually describes

What a criminal collection actually is

When a virus infects somebody's computer it copies every username and password saved in the browser, and those get bundled up and traded. If a member of staff ever saved a work login on an infected machine, their firm address and password can end up on a list anyone can buy. We never see or try those passwords, only that records exist against a firm's domain and how many. **We cannot tell whether any still works**, only that the material is out there.

953

staff password records across 35 firms

27

records on a typical affected firm, so this is deep as well as wide

What sits behind those identities is what makes this sector different. These firms hold client mandates and payment instructions, so a working staff login is not simply access to a mailbox. Thirty-five firms also have an internal login or administration page recorded in the same criminal collections, which is the same number as the firms carrying staff records, though the two lists are counted separately and this report does not claim they are the same firms.

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

The change that matters for reading every table in this report

Some firm 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 **34 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	150	71.2
Floor scores, counted at their floor	34	59.0
All published figures	184	69.0

Use 71.2 for the sector's measured position and 69.0 for the most cautious one. Were every unread instruction present and correct, those 34 firms would average 79.5 rather than 59.0. **That is an upper bound on what the evidence permits, not a prediction**, and the gap is the point: the browser-instruction family carries roughly a fifth of the score, so a website that turns the scanner away loses a band on evidence grounds alone. Nine further websites produced no usable score and are excluded throughout.

What is going well

No firm carries a known-breach record and none is flagged as unsafe by browser makers. **131 of 184 firms, 71%, either refuse forged email in their name or send it to spam**, and 96 of those refuse it outright. Certificates are in good order, with a single fault across the whole estate.

Why this matters for these firms in particular

A wealth or investment manager holds two things that make it an unusually attractive target. The first is money, in the direct sense: client mandates, payment instructions and the authority to move funds. The second is trust of a specific and fragile kind. A client who receives a message that appears to come from their adviser, about their own portfolio, referencing a real transaction, is a client who acts.

That is why the email finding in this report matters more here than the raw number suggests. A forged message in a firm's name is not a nuisance. It is the opening move in a payment-redirection fraud, and 53 of the 184 firms reported cannot instruct a receiving mail system to refuse one.

A way of picturing what we did

Somebody walking down your street

They never go inside any building and never try a door. They walk past and notice what is visible from the pavement: a window left open, a side gate unlatched, a spare key under the mat where everyone knows to look.

None of that means the building has been burgled. It means somebody passing by can see opportunities, and most of them take a minute to put right.

That is exactly this assessment. When this report says staff passwords are circulating, that is the spare key under the mat: it does not mean anyone has used it, but somebody else knows where it is. When it says a port is answering that need not be, that is the side gate nobody remembers leaving unlatched. And when a firm's website turns our scanner away, that is a locked gate doing its job, which is why those firms get a floor score rather than a mark against them.

What we could not see, which is most of it

Standing in the street tells you nothing about the alarm, the safe or the locks on the internal doors. Many of these firms will have good protections we simply cannot observe: staff training, monitoring, payment verification procedures, internal access controls, everything inside the building.

So nothing in this report is a verdict on any firm's security. It is an account of what is showing from outside, which is useful precisely because it is what a criminal sees too.

Three cautions that apply to every number here

A finding is not a break-in. Nothing establishes that any firm has been compromised, and every serious item needs the firm to check it privately before it is treated as fact.

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

Nothing here is a compliance judgement. We observe technical settings. We cannot see contracts, retention, training or how client information is actually handled.

1. The words used in this report

This section exists so that nothing later needs a specialist to interpret. Each term is given the way it is used here, not as a formal definition.

Term	What it means in this report
Cyber posture	The condition of a firm's defences at a point in time, as seen from outside. If a stranger looked at the firm from the public internet, what could they learn?
Criminal credential collection	A traded list of usernames and passwords, mostly harvested by viruses from the browsers of infected computers. Also called infostealer data.
Ransomware leak site	A site where a criminal group publishes the names of organisations it claims to have attacked, usually to pressure payment. A listing is a claim, not a verified fact.
Version-inferred weakness	A weakness guessed from the version number a piece of software reports, not confirmed by testing. Suppliers often fix a fault without changing the version, so these overstate.
Known-exploited list	A public catalogue of weaknesses criminals are known to be using in the real world. Far shorter and more serious than a weakness merely being recorded somewhere.
Floor score	A score published as "at least this much" where one part of the check could not be read. Every unread item counts as missing, so the true figure can only be the same or higher.
Forged email, and the setting that stops it	Anyone can put a firm's name on an email. A published instruction called a DMARC policy tells receiving mail systems to refuse those forgeries. It can be set to refuse, to send to spam, or to do nothing.
Secure connection	The padlock. A page served over HTTPS is encrypted in transit; one served over plain HTTP can be read or altered on the way.
Risky port answering	Something responding on the public internet where a service normally faces inwards: a database, a remote-access tool, a file-transfer or admin console.
Shared provider address	One internet address used by a hosting or web-security company for many customers at once. What answers there may be the provider's equipment rather than any one firm's.
Cookie consent mechanism	The banner that asks permission before storing things on a visitor's device. The law governs what may be stored before a choice is made.
Website instructions to the browser	Settings a website sends telling the browser how to treat the page. Their absence is a review point, not a hole. These are the items a floor score counts as missing.

Security is cumulative, which is why there is no single fix

A strong position is rarely one product. It is the combined effect of many ordinary settings done properly: strong sign-in, sensible configuration, secure email, patched software, limited exposure to the internet, knowing what suppliers hold, a route for someone to report a problem, and a plan for when something goes wrong.

2. Where these firms sit in the rules

Unlike some sectors we have measured, wealth and investment managers are firmly inside a regulatory regime that speaks directly to what this report observes.

Operational resilience

Firms sit under the Financial Conduct Authority's operational resilience rules, and where dual-regulated also under the Prudential Regulation Authority's supervisory statement. Both require a firm to identify its **important business services**, set a tolerance for how much disruption each can take, and understand the dependencies that could cause it.^[1]

Why that matters for this report specifically

A client portal, a trustworthy email channel and the staff identities that control both are dependencies of an important business service. They are not IT housekeeping.

Read that way, the findings here are not a separate technical list. A reachable database port, an unenforced email policy or a set of circulating staff credentials is a dependency with a known weakness, and the regime already expects it to be recorded, owned and tolerated or fixed. The same applies to a shared provider address: a platform serving ten firms in this list at once is exactly the kind of dependency the rules expect to be written down.

Data protection applies directly too

Firms are legally responsible for the personal information they hold about clients under the UK GDPR, and separate rules govern what may be stored on a client's device when they visit a website. The Information Commissioner's Office regulates both and publishes the guidance that decides whether an arrangement is lawful.^[2]

What this report can and cannot say about that

We can see whether a website forces a secure connection, whether a privacy policy can be found, whether a cookie banner is present in the page as delivered, and what the website stores. **None of that establishes whether a firm is complying with anything.**

We cannot see the lawful basis for any processing, how long information is kept, what contracts are in place with suppliers, whether information leaves the country, how requests from clients are handled, or any of the training and internal controls that make up most of the regime.

How this differs from the statistics you may have seen

Most sector cyber figures come from surveys, which ask organisations what happened to them and what they have in place. This study asked nobody anything. Every number is an observation taken from outside using the same checks on every website. A survey tells you what a sector believes about itself; this 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.

The overlap between the two lists, stated before anything else

Twenty-one firms appear on both the wealth manager list and the investment manager list, usually because a single group runs both a private-client business and an institutional fund management business. **214 is a count of list entries, not firms.** Adding the two lists would describe a population that does not exist, so every consolidated figure in this report counts each website once and rests on 193 distinct websites.

Coverage	Wealth managers	Investment managers	Consolidated
Tracked entries	96	118	214 entries
Appearing on both lists	21	21	counted once
Distinct websites	96	118	193
Excluded, completed without a score	5	3	7
Excluded, tracked address not in DNS	2	0	2
Exact score	64	98	150
Floor score	25	17	34
Reported	89	115	184

The two source columns add to 204 rather than 184 because of the shared firms: 20 of the 21 produced a score and are counted once here, the 21st being one of the seven excluded without a score. The consolidated unscored figure is 7 rather than 8 for the same reason, one unscored website appearing on both lists.

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 and not observations.

Rows in a table overlap and must never be added. The clearest case: 6 firms have a risky port answering on their own address and 4 have a database port, but the 4 are inside the 6. The total is 6 firms, not 10.

Every percentage names its denominator. Most are shares of the 184 reported websites. Some checks could only answer for fewer, and those tables say so, in the form 67 / 150 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 8 sets them out. They are never combined into one headline number.

4. Source one: the 96 wealth manager websites

The first list is the UK's largest wealth managers, counted by website rather than by legal entity, fund or brand. Of the 96, seven produced no usable score: five completed without one and two did not resolve in the internet's address system. That leaves **89 reported**, 64 with an exact score and 25 with a floor score.

Measure	Exact scores 64 websites	All published 89 websites
Average	70.4	67.0
Median	74	67
Good, 75 and above	20	20
Needs improvement, 50 to 74	37	58
At risk, below 50	7	11
Sum of scores	4,505	5,963

Tracked 96, excluded 7, reported 89. The two columns are two views of the same websites: the right-hand one adds the 25 floor scores at their floor value, and those floors average 58.3 against a ceiling of 77.8.

This list carries every address-not-found case in the study

Two websites are tracked at an address that does not exist in the internet's address system, and both are on the wealth manager list. That is not a security finding and produces no evidence at all. The tracked address is wrong, retired or moved, so the first step is a correction to the list rather than work by the firm; two further addresses in this position were replaced with the firms' current ones before this scan and both then scored. With five that completed without a score, this list has the higher exclusion rate, seven of 96 against three of 118, and those seven firms cannot be described here in any respect.

What this list carries, on its own 89

Observation	Firms	Share of 89
Named on a ransomware leak site	3	3%
Risky ports on an address used only by the firm no service identified on either	2	2%
Risky ports only on a shared provider address	5	6%
Version-inferred software weakness	2	2%
of which on the known-exploited list	1	1%
Certificate, protocol or cipher issue	11	12%
Forged email not instructed to be refused	26	29%

Neither firm-level port case on this list has an identified service. On one, open database and remote-access ports sit on the provider's edge address dedicated to the firm's group; on the other, nothing answered. The two carry 9 port observations and the five shared-provider cases a further 36. Transport is where this list is visibly weaker: **11 firms carry a certificate, protocol or cipher issue and 10 accept legacy encryption**, against 5 on the investment list, and both are configuration fixes rather than findings of consequence.

5. Source two: the 118 investment manager websites

The second list is the UK's largest investment managers, again counted by website. Three produced no usable score, all completing without one rather than failing to resolve. That leaves **115 reported**, 98 with an exact score and 17 with a floor score.

Measure	Exact scores 98 websites	All published 115 websites
Average	72.2	70.5
Median	74	72
Good, 75 and above	30	30
Needs improvement, 50 to 74	62	78
At risk, below 50	6	7
Sum of scores	7,076	8,112

Tracked 118, excluded 3, reported 115. The better covered list: 97% produced a usable score against 93% on the wealth list, every address resolved, and the 17 floors average 60.9 against a ceiling of 83.0.

What this list carries, on its own 115

Observation	Firms	Share of 115
Named on a ransomware leak site	4	3%
Risky ports on an address used only by the firm 2 of the 4 with a service identified	4	3%
Risky ports only on a shared provider address 8 of the 10 on one managed-hosting address	10	9%
Version-inferred software weakness	5	4%
of which on the known-exploited list	1	1%
Certificate, protocol or cipher issue	5	4%
Forged email not instructed to be refused	31	27%

Both identified services in the whole study sit on this list, a database server and a file-transfer server. The other two firm-level cases are open database ports on the provider's edge addresses dedicated to them. The four carry 19 port observations, the ten shared cases 65.

Eight of the ten shared-provider cases sit on one managed-hosting address, which makes most of this list's port exposure a single supplier question rather than ten separate ones.

The 1.9-point gap on exact scores is not a ranking

Twenty-one firms are on both lists and contribute to both averages. The populations differ in size, 118 against 96, and in how much evidence came back, 18 floor scores against 26. A floor score drags an average down by an amount that depends on how many websites turn the scanner away rather than on how well those firms are run.

The honest reading is that the two lists are close on score. What separates firms in this sector is not which list they sit on but whether they carry one of the consequential findings in section 7, and those do not follow the list boundary at all.

Where the two lists meet: what adds, and what does not

Twenty-one firms appear on both lists and twenty of them scored. Every consolidated figure in this report counts each of those firms once. **That makes the two single-list tables above a pair of views rather than two halves**, and it is why almost nothing on this page can be added.

Figure	Wealth list	Investment list	Sum	Consolidated
Reported websites	89	115	204	184
Exact scores	64	98	162	150
Floor scores	25	17	42	34
Sum of published scores	5,963	8,112	14,075	12,691
Named on a ransomware leak site	3	4	7	6
Risky ports, firm's own address	2	4	6	6
Risky ports, shared provider address	5	10	15	14
On the one managed-hosting address	3	8	11	10
Poor-reputation addresses	4	4	8	6
Version-inferred weaknesses	2	5	7	7
Firms with staff records	15	22	37	35
Staff records	531	532	1,063	953

Read the last two columns together and the shape of the overlap becomes visible. Where the sum and the consolidated figure are equal, no dual-listed firm carries that finding: the six firm-level port cases, the seven version-inferred weaknesses and both known-exploited entries fall entirely on one list or the other. Where they differ, the gap is the number of dual-listed firms carrying it.

The four places a reader would get it wrong

Ransomware: 3 plus 4 is 6, not 7. One of the named firms appears on both lists. **Shared-provider ports: 5 plus 10 is 14, not 15,** and the managed-hosting group is 10 rather than 11, because one firm on that address runs both a wealth and an investment business. **Poor-reputation addresses: 4 plus 4 is 6, not 8.** Two of those firms are dual-listed, one on its own address and one on a shared cloud address. **Staff records: 531 plus 532 is 953, not 1,063,** because two dual-listed firms hold 110 records that would otherwise be counted twice.

None of this is a correction to the single-list figures, which are right for their own population. It is what happens when 21 firms run two businesses and appear on two lists.

The floors behave differently on each list, which is most of why the two averages differ: 25 of the 89 wealth websites are floors, averaging 58.3 against a ceiling of 77.8, against 17 of 115 on the investment list at 60.9 against 83.0. The same arithmetic holds for every control measured in this report. Each of the email, transport, DNS and privacy tables reconciles to exactly 20 dual-listed scored firms when the two single-list figures are set against the consolidated one, which is how the consolidation was checked rather than assumed.

6. The consolidated view: 184 reported websites

From here on every figure describes the 184 distinct reported websites, with each shared firm counted once.

Band	On exact scores 150 websites	Including floor scores 184 websites
Good, 75 and above	42 (28%)	42 (23%)
Needs improvement, 50 to 74	97 (65%)	126 (68%)
At risk, below 50	11 (7%)	16 (9%)

Exact average **71.2**, median **74**. Counting the 34 floor scores at their floor gives **69.0**, median **71**. Those floors average 59.0 and would average 79.5 if every unread instruction turned out to be in place. **The five extra at-risk results in the right-hand column are floor figures and may all sit higher.**

Fewer than three in ten are in good order, and that is the headline on hygiene

Forty-two of 150 exactly scored firms reach the top band. Ninety-seven sit in the middle, where the gaps are real but routine. Eleven are confirmed in the lowest band.

The gap is not in any single control. It is the accumulation of email authentication, disclosure routes, transport settings and browser instructions, none of which is individually serious and all of which the score counts.

Where the two source lists sit inside this

Measure	Wealth managers	Investment managers	Consolidated
Reported websites	89	115	184
Exact scores	64	98	150
Floor scores	25	17	34
Exact-score average	70.4	72.2	71.2
Score sum, all published	5,963	8,112	12,691

The two source sums add to 14,075 rather than 12,691 because the shared firms contribute to both. The consolidated average is calculated from the 184 underlying scores, not by averaging the two list averages.

7. The findings that carry real consequence

These are the items that would matter on a Monday morning. They are small in number and 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	6 / 184	3%
Risky ports on an address used only by the firm	6 / 184	3%
of which a database port 1 identified server; 3 open ports on a provider edge	4 / 184	2%
Risky ports only on a shared provider address, nothing identified	14 / 184	8%
Software weakness read from a version number	7 / 184	4%
of which on the known-exploited list both the same denial-of-service flaw	2 / 184	1%
Poor public reputation, address used only by the firm	2 / 184	1%
Poor public reputation, shared cloud address	4 / 184	2%
Certificate, protocol or encryption problem	14 / 184	8%
Known breach records or browser-safety warnings	0 / 184	0%

Six ransomware leak-site references, and how to handle them

Six firms appear on ransomware leak sites: on this evidence 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 a similarly named entity elsewhere. The right response is restricted matching of entity, date and incident record with the firm's incident response team, and **it must not be published against a named firm without that validation.**

The software weaknesses, and what the two exploited entries actually are

Seven firms show software weaknesses on a reachable service, across 88 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 seven firms, not 88 observations.

Two entries are on the exploited list, and both are the same kind of flaw

Two of the 88 observations, on two different firms, are on the public list of weaknesses criminals are known to be using. **Both are the same one: a way of overloading a web server so the website goes offline.** It does not give an attacker access to systems or data, and it applies only where a particular web protocol is switched on, which this scan did not establish. **It belongs with the version-checking work, not alongside the ransomware references.** The remaining 86 observations are a validation exercise rather than an alarm.

Poor-reputation addresses, split the same way

Six firms carry an elevated public reputation finding, in every case a single listing on one threat feed. **Two sit on an address used only by that firm** among those we have scanned, which is not proof nobody else uses it. **Four sit on two shared cloud addresses:** such a listing describes the address, not any one tenant. Confirm tenancy before attributing any of the six.

7 continued: whose address the port sits on

Ports answering: 20 cases, and how little is confirmed

Twenty cases were observed. **Six sit on an address used only by the firm** and fourteen on an address shared with unrelated organisations, reported separately. Of the six, **only two have a service we could identify**: a database server and a file-transfer server. Three are open database ports on a security provider's edge addresses dedicated to those firms, with nothing behind them but the provider's own proxy software, and on the sixth nothing answered at all.

A port answering is not the same as a vulnerability. A service may be deliberately published, access-controlled, or run by a supplier. It does mean the door is visible and somebody should confirm what is behind it. Each case was checked individually on two questions: did a named product, version or protocol answer on the flagged port, and do unrelated organisations resolve to the same address?

Where the flagged port answers	Firms	Anything identified?	Treatment
One managed-hosting platform address at least 22 unrelated organisations resolve to it	10	Nothing	Reported separately
Shared web-hosting servers	3	Nothing	Reported separately
A shared edge address of one web-security provider	1	Nothing	Reported separately
The same provider, addresses dedicated to one firm only the firm's own group names resolve there	3	Nothing on most ports; on one or two, the provider's own proxy software	Firm-level: 3 open database ports on the provider's edge
Hosting where a service was identified	2	A database server, and a file-transfer server	Firm-level: an identified service counts whatever else shares the address
Hosting used only by the firm	1	Nothing answered	Firm-level
All cases observed	20	2 with a service identified	6 firm-level, 14 separate

Rows are exclusive and sum to the total. An identified service is counted at firm level whatever else shares the address, which is why the file-transfer case stays firm-level despite sharing. The 6 firm-level cases carry 28 port observations between them and the 14 separated cases a further 94. "Used only by the firm" means only that firm among the organisations we have scanned.

Why these are reported separately

The fourteen reported separately are not discarded. They are reported that way because nothing was identified on the flagged ports and the addresses serve unrelated organisations, so the ports may be the provider's equipment rather than the firm's. **A weakness in a shared platform would reach every organisation on it at the same moment.**

The practical consequence is concentration. One provider's control failure could reach ten firms in this list at once, and those ten have no visibility of each other: a supplier dependency behind a client-facing service, exactly what the resilience rules expect a firm to have written down.

A firm's own servers behind the provider were not examined by this scan.

8. Stolen credentials: three different problems

This is the largest body of evidence in the report and the most misunderstood. The source returns three separate populations, they concern different people, they are fixed by different parties, and **they must never be added into one number**. Counts were returned and reconciled for all 184 reported websites.

Population	Who it concerns, and who can act	Firms	Rate	Records
1. Staff	Accounts on the firm's own domain. The firm can fix these today by resetting the password, ending active sessions and enforcing phishing-resistant multi-factor sign-in.	35 / 184	19%	953
2. Identities elsewhere	Firm email addresses used to sign in to other companies' platforms. The firm can act, but the reset happens on the other system. For 46 of the 82, the criminal logs name the service involved: identity, payroll, email.	82 / 184	45%	2,643
3. Clients	Members of the public with an account on a firm service, whose own device was infected. Nobody at the firm can reset these . Only the client can.	102 / 184	56%	75,696
1 or 2	Deduplicated. Not 35 plus 82.	86 / 184	47%	n/a

Ninety-eight firms, 53%, have nothing in either of the two actionable populations. That is a measured result and a good one.

Why the order matters more than the size

The staff population is the one that matters and it is the smallest. It is a key to the firm's own systems, the firm issued it, and the firm can take it back this afternoon.

The identities-elsewhere population follows closely, because a work address reused across several platforms is how one compromise becomes several. It is also the larger of the two actionable populations here, reaching 45% of firms.

The client population is nearly eighty times larger and ranks last. It is not access to anything the firm runs. It is a client's own laptop that caught a virus. It carries no weight in the score and nobody at the firm can reset it. It is a duty-of-care and communication question, not a security hole.

What 'identities elsewhere' does not mean

It counts **the firm's own email addresses appearing on somebody else's platform**. It is **not** a count of suppliers holding access into the firm, which is close to the opposite. Described that way it would claim something this study has not measured, so we never call it a supplier figure.

8 continued: the depth of the staff exposure

27 staff records on a typical affected firm, so this is deep as well as wide	35 firms whose own internal login addresses appear in the same criminal logs	46 of the 82 outside-service firms where the logs name the service involved
--	--	---

This sector's staff credential problem is deep as well as wide. Nine hundred and fifty-three records across 35 firms is 27 on a typical affected firm rather than the handful a broad, shallow pattern would produce. Concentration of that kind normally means one of two things: a single large firm with many staff whose devices have been infected over time, or an organisation whose people sign in to a great many systems with the same work address.

Two further measures from the same logs, describing different groups

Thirty-five firms have their own internal login or administration addresses captured in the criminal logs. Separately, for **46 of the 82 firms** with identities on outside platforms, the logs name the outside service involved: identity, payroll, email. Both come from the criminal logs, not from anything this scan observed on the firms' public systems.

Why it matters is that a credential on its own has limited value to a stranger who does not know where it fits, while a credential recorded beside the address of the page it opens removes the step that normally slows an attacker down. Sequence the response accordingly: reset, revoke live sessions, then enforce phishing-resistant multi-factor sign-in, starting with identity providers, email, finance systems, client records and remote access.

The 35 firms whose internal login addresses appear in the logs are a separate triage group from the 35 carrying staff records. The two counts are equal, but this report does not claim they describe the same firms: establishing that is a question for the restricted evidence, not for a published figure.

What these records establish, and what they do not

They are public-source records tied to a firm's domain, mostly harvested by viruses on individual computers. **We cannot see whether any password still works, whether the account still exists, or when the infection happened.** The source does not tell us how completely it has collected, so we make no claim that this is fresh or complete.

None of it is evidence that a firm has been broken into. It is a reason for each firm to check its own accounts privately against its own records, and never by trying a recovered password.

9. Forged email: the sector's weakest common control

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 184
Refuse the forgery	96	52%
Send it to spam	35	19%
Do nothing, monitoring only	40	22%
No usable policy observed	13	7%

Fifty-three firms, 29%, do not instruct refusal or spam filing at all. Forty publish a policy set to do nothing and 13 have no usable policy. A further 35 ask only for spam filing, so 86 of 184 do not ask for outright refusal.

Why this control matters more here than almost anywhere

In most sectors a forged email is a phishing nuisance. In wealth and investment management it is the opening move in a payment-redirection fraud: a message that appears to come from an adviser, about a real client's real portfolio, asking for a change to payment details.

The control that stops it is a published instruction costing nothing to set. **It is the cheapest item in this report and the one with the most direct client 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 client portal, the reporting system, the custodian, the marketing tool, the recruitment platform, and watch for long enough to be confident, or genuine client correspondence starts being refused. The right sequence is watch, then file to spam, then refuse.

The supporting records

Control	Have it	Do not
Record naming which servers may send mail	174	10
Signing record on the names we sampled	123	61
Encryption reporting record	13	170

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. One website's encryption reporting record could not be read either way.

10. Cookies, consent and tracking

This concerns what happens on a client's own device, and it sits in the regime that applies to these firms directly.

Read this before the number

Our privacy check scored **66.3% of the points it was able to assess**, 1,971 of 2,972. **That is not 67% 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	143	10	31	Anything typed into an insecure page can be read on the way.
No insecure content on a secure page	141	9	34	A padlock is weakened if parts of the page arrive unprotected.
Privacy policy route found	96	43	45	People should be able to find out what happens to their data.
Cookie consent mechanism found	83	67	34	The law governs what may be stored before a person chooses.
Published vulnerability-disclosure policy	7	147	30	A stated policy telling a researcher how the firm wants a problem reported.

Sixty-seven of the 150 websites we could read showed no consent mechanism, 45%. Thirty-four homepages were not readable by the scanner at all, and their consent state is unknown rather than assumed clean.

Two rows here resemble rows in section 11 and are not the same check. This table asks whether an insecure request is redirected (143); section 11 asks whether secure connections are enforced, a stricter test, which 141 pass. This table asks whether a *disclosure policy* is published, which 7 firms do; sections 11 and 12 ask whether the standard *security contact file* is present, which 17 publish. Both figures are right for the question each asks.

The last row is the one nobody expects

Only seven firms of 184 publish a policy saying how they want a security problem reported, and 147 do not. **That is the lowest adoption of any control in this report.** The related contact file fares a little better at 17 firms, and the two together still leave most of the sector unreachable.

Someone who finds a weakness at one of those firms has no obvious way to tell them, which is how problems end up disclosed in public instead. It is a short page and a single file, and both cost nothing.

What the websites store

Cookie evidence came back for 146 websites. **83 stored something during the first page visit, 218 items in total.** Of those 83, 49 stored at least one item without the setting that limits it being sent from other websites, 39 without the setting that hides it from page scripts, and 27 without the setting that keeps it off insecure connections.

Only a response that was the site's real homepage is counted; a protection or error page answering in its place is not. Collection was skipped for 24 websites and unavailable for 14. This sees only what the first page request returns, so the real numbers are higher, and not every item needs every setting, so this is a review list rather than a defect list.

10 continued: tracking, and the regulator's position

Tracking technology on 101 of 150 readable websites

Tracking technology was present on **101 of the 150 websites we could read, 67%**. A tag manager accounts for nearly all of it, appearing on 100 of the 101. Beyond that the picture is sparse: a session-replay tool on 6, analytics on 3, a heat-mapping tool on 2, and an advertising tag, a marketing-automation tag and a customer-data platform on one each. These overlap on a single website.

The presence of tracking code proves nothing on its own. It does not show that personal data was sent, that permission was needed, that permission was missing, or what legal role the vendor plays. A tag manager is a container: what it loads and when has to be watched, not assumed.

The six session-replay deployments are worth separate attention. Session replay records what a visitor does on the page rather than counting visits, which raises sharper questions about what is captured and whether form fields are masked. In a sector whose web forms carry client and financial detail, that is a question worth answering deliberately.

The regulator is actively testing this

In December 2025 the Information Commissioner's Office reported the result of testing the **top 1,000 websites used in the UK**. It checked three things: whether advertising cookies were stored before consent, whether refusing was as easy as accepting, and whether cookies were placed without permission at all.

564 of the 1,000 only became compliant after the ICO contacted them	17 received preliminary enforcement notices	21 were still non-compliant when the ICO reported
---	---	---

The ICO said it will keep testing the top 1,000 periodically.^[3] Two things follow. An absent consent mechanism is not unusual, since more than half of the UK's most-visited websites needed prompting. And more importantly, **the regulator tests precisely the behaviours this scan cannot see**, so our signal is a prompt to look rather than an answer.

What a browser check should establish, in order

1. What is stored on the device before any choice is made, and is any of it not strictly necessary.
2. Is there a refuse option, is it on the first screen, and does it take no more effort than accepting.
3. Does refusing actually stop the storage, or just record a preference.
4. Does the same hold on client-facing forms, not just the homepage.
5. What does each piece of tracking code load, and what leaves the browser when it does.

11. Card payments and transport security

Many firms in this sector do not take card payments directly, 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 report is not

Our payment-surface check scored **89.6% of the points it could assess**, 2,765 of 3,087. 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 90% 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.^[4]

External signal, of 184 reported	Pass	Issue	Could not tell
No Heartbleed weakness	184	0	0
Valid certificate	183	1	0
No software weakness reported	177	7	0
No database port answering	170	14	0
Modern encryption only	163	13	8
Visitors forced onto a secure connection	141	8	35
Browser told never to try the insecure version	115	35	34
Route to report a security problem published	17	139	28
Cloud storage, mail encryption, mail relay	0	0	184

The 14 database-port issues are this check's own result and include the 10 reported separately in section 7, which is why the firm-level database count is 4. **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

Eight firms do not force visitors onto a secure connection and 35 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. Thirteen 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.

12. Domain controls and the dependency nobody records

Control	Have it	Do not	What it does
Mail server record	174	10	Names which servers may send mail for the firm.
Mail signing record	123	61	Signs outgoing mail so it can be verified. Sampled, so absence is not conclusive.
Certificate authority record	23	161	Names which companies may issue certificates for the domain, so a rogue one is refused.
Signed domain records	21	163	Stops someone forging the answer to 'where is this firm's website'.
Security contact route	17	139	A published file telling a researcher where to report a problem privately.
Encryption reporting record	13	170	Asks other systems to report failures in protecting mail in transit.

Four of these six controls sit below 15% adoption. A gap shared by more than eight firms in ten is a sector fact rather than 160 or so individual failures, and it is a natural candidate for a coordinated push through an industry body rather than 184 separate projects. Signed domain records at 21 firms and certificate authority records at 23 are the two that most directly protect the firm's own identity on the internet.

The dependency that is on nobody's risk register

Observation	Firms	Rate
Mail transport policy finding	175 / 184	95%
Some form of network concentration	148 / 184	80%
All address records with one provider	116 / 184	63%
Risky port on a shared provider address	14 / 184	8%
Internet address with a poor public reputation	6 / 184	3%

These overlap and must not be added. A flagged address can belong to another organisation sharing the same infrastructure, so ownership needs confirming first. A reputation listing on a recognised shared hosting address is not attributed to each firm on it, because it describes that platform's tenants collectively.

116 firms, 63%, 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, and splitting the job across providers brings its own problems. **The question is whether anyone has written it down.** Under the operational resilience rules a single provider behind a client-facing service is exactly the kind of dependency a firm is expected to have identified, with a failure mode and a recovery route attached. The ten firms sharing one hosting platform address in section 7 are 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.

13. What we could not read

Three 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	34	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	7	A second piece of core evidence was missing too, so no score could be published. Excluded from every figure on the owner's instruction.
Excluded, address did not resolve	2	The scanner could not find the website at all. Not a security finding: it usually means a tracked address is wrong or retired, and the correct one is being confirmed. Two further domains in this position were replaced with the firms' current addresses before this scan and are now scored.

What else we could not see

Evidence type, of 184 reported	Got it	Partly	Could not
Website instructions to the browser	150	0	34
Homepage content, for consent and tracking	150	0	34
What the website stores on a device	146	0	38
Direct mail server test	19	0	165
Mail resilience	9	175	0
Other systems on the same infrastructure	69	115	0
Cloud storage discovery	0	183	1

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 19 websites and still produced no definitive answer on mail encryption or relay status.

13 continued: the evidence that ran but did not finish

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.

The related-host review ran everywhere and finished nowhere near everywhere

The review of other names sharing a firm's certificates and infrastructure ran on all 184 websites, but it is complete on only 69 of them. It found **66,667 related host names**. Ninety-two websites exceeded the 50-host review limit, so **6,062 hosts were examined individually and 60,605 were not**, and 145 of those examined could not be assessed. **No absence claim can rest on this evidence.**

Two things in it are worth a firm's attention rather than alarm. **35,623 host names, across 168 websites, appear only in expired certificates:** names that once had a certificate and may since have been abandoned, which is a tidying exercise and an inventory question. And on six websites the review found seven published addresses pointing at a target that does not exist. That is a loose end to close, not evidence that anyone else controls it, and the review did not test who controls any resource.

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

14. What to do, in order

Ordered by consequence, not ease. These groups overlap and are not a count of separate firms.

1	Validate the six ransomware leak-site references Match entity, date and incident record privately with the incident response team. A listing can be historical, duplicated, or a similar entity elsewhere. Never publish it against a named firm.
2	Check the two known-exploited entries, then the other five Two of the 88 version-read observations, on two different firms, are on the public list of weaknesses being exploited. Confirm the software actually running first. The other five firms carry version-read weaknesses not on that list: a validation exercise, not an alarm.
3	Check the six ports answering on firms' own addresses Four are database ports: one an identified database server, three open ports on provider edge addresses dedicated to the firm. A port answering is not the same as a vulnerability, but the database cases hold client records. Two of the six have a service actually identified, a file-transfer server and a database server; start there, then the one case where nothing answered.
4	Take the fourteen shared-provider cases to the provider Ten sit on one managed-hosting address serving at least 22 unrelated organisations, three on shared web hosting and one on a shared edge address. Ask which services are meant to be reachable, how the platform is protected, and what the contract says about breach notice.
5	Reset the staff passwords 35 firms, 953 records, 27 on a typical affected firm. Reset, revoke live sessions, then enforce phishing-resistant multi-factor sign-in, starting with identity providers, email and finance. Never test a recovered password.
6	Move the 53 firms towards refusing forged email Inventory every legitimate sender first, then watch, then file to spam, then refuse. The 35 already filing to spam should finish. Investigate the 61 sampled signing-record gaps and 10 missing mail server records alongside.
7	Work the 82 firms with identities on other platforms 2,643 records, the largest actionable population. For 46 of the 82 the logs name the outside service involved, so start there. The reset happens on the other company's system; the harder half is establishing which outside services staff used a work address on.
8	Fix transport, then the browser instructions Eight firms not forcing a secure connection, 35 without the instruction that stops the browser trying the insecure version, 13 accepting outdated encryption and one certificate fault. Confirm the 2 firm-level poor-reputation addresses against tenancy.
9	Open the 67 websites in a browser and watch what happens The consent question cannot be settled from outside. Ten minutes per site, no specialist needed, and it answers the cookie review for the 48 sites with attribute gaps too.
10	Publish a security contact route, and close the evidence gaps Only 17 firms publish the contact file and seven a disclosure policy, which is why findings here surface publicly. The two unresolvable addresses need confirming, the seven unscored a completed run, and the 34 floor scores a decision on the scanner.

Conclusion

This sector's problem is not its average. It is the concentration of consequence in a small number of firms. An exact-score average of 71.2 with 42 of 150 firms in the top band is a middling hygiene picture, and on its own it would justify a routine improvement programme. What changes the conversation is that six firms are named on ransomware leak sites, two are running software with a weakness on the public list of those being exploited, and one has an identified database server answering the internet.

Those findings do not follow the score bands. A firm can sit comfortably in the top band and carry any of these findings, 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

Staff credential exposure is deep, not just wide. Nine hundred and fifty-three records across 35 firms, 27 on a typical affected firm, and 35 firms also have an internal login page recorded in the same collections.

Email authentication is the weakest common control. Fifty-three firms cannot instruct refusal of a message forged in their name, in a sector where that message is the opening move in a payment fraud.

Almost nobody can be told about a problem. Seven firms of 184 publish a route for reporting one. That is the lowest adoption of any control measured.

And one structural point. Of the 20 ports answering that should not be, fourteen sit on addresses shared with unrelated organisations, ten of them on a single managed-hosting platform, and are reported separately from the six on firms' own addresses. They are reported separately because only the provider can confirm or close them, and they are a concentration: one provider's control failure would reach ten of these firms at the same moment, and none of the ten can see the other nine.

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 rank the two source lists, which are close on score and share 21 firms. And it makes no compliance judgement, because we observe settings, not lawfulness.

One thing it does claim. Under the operational resilience rules these are not IT findings. An identified database server answering, an unenforced email policy, a shared platform behind ten firms and a set of circulating staff credentials are dependencies of important business services, and the regime already expects each to be identified, owned, and either tolerated or fixed.

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

The overlap, before anything else

Twenty-one firms appear on both source lists. **214 is a count of list entries and is never a population.** Every consolidated figure rests on 193 distinct websites, of which 184 are reported.

Bands, and what a score is

Good is 75 and above, **needs improvement** is 50 to 74, **at risk** is 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 7. **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

150 websites have an exact score and 34 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. They are never compared with exact scores or used to rank a firm. Two averages are given: **71.2** on exact scores alone and **69.0** counting floors at their floor.

Counting, and whose address 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: seven firms, not 88 observations. Rows overlap and must never be added: the 4 database ports sit inside the 6 ports answering on firms' own addresses, and the 14 shared-provider cases are counted once, on their own line.

Exposure is reported by owner, decided 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 20 observed, **6 are firm-level and 14 shared.**

The two percentage scores are not compliance rates

The privacy check scored 66.3%, 1,971 of 2,972, and the payment-surface check 89.6%, 2,765 of 3,087, **of the points each was able to assess.** Controls that could not be verified from outside were removed from the calculation rather than counted as passes, which is why the payment figure is high. Neither is an audit or a legal conclusion.

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 do not attribute a provider's shared infrastructure to a single firm.

Notes

- Every figure describes the assessment of 26 September 2026. No trend is reported and none should be inferred. Client account records are unscored and concern the public, not firm systems. The population is tracked websites, not legal entities, funds or brands; a zero means a check ran and found nothing. We publish counts and distributions, never a league table.

Sources and notes

[1] Operational resilience: FCA PS21/3 and PRA SS1/21

Both require firms to identify important business services, set impact tolerances and understand the dependencies that could cause disruption. Client-facing portals, trustworthy communications, shared platform providers and the staff identity controls behind all three are dependencies of those services. [FCA PS21/3](#) and [PRA SS1/21](#)

[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 decide whether an arrangement is lawful; the signals in section 10 of this report are technical observations and are not such an assessment. [ICO cookie guidance](#) and [ICO data security guidance](#)

[3] Information Commissioner's Office, *ICO action secures increased cookie compliance, December 2025*

The ICO tested the top 1,000 websites used in the UK against three requirements: no non-essential advertising cookies before consent, refusing as easy as accepting, and no cookies placed without permission. 415 passed without intervention, 564 improved after ICO engagement, 17 received preliminary enforcement notices and 21 remained non-compliant at the point of reporting. [ico.org.uk](#)

[4] 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](#)

[5] National Cyber Security Centre

Email security and anti-spoofing, including the staged move from monitoring, through spam filing, to refusal; *External attack surface management*; *Multi-factor authentication for corporate online services*; *Vulnerability disclosure toolkit*. Free plain-English guidance requiring no specialist team. [NCSC email security](#), [MFA guidance](#) and [vulnerability disclosure toolkit](#)

[6] MyDomainRisk / Huro Data Technologies Ltd, *two source estate baselines and one consolidated baseline, extraction 26 September 2026*

Wealth managers 96 tracked, 89 reported (64 exact, 25 floor), 5 unscored and 2 tracked domains not in DNS; exact sum 4,505 and average 70.4, published sum 5,963 and average 67.0. Investment managers 118 tracked, 115 reported (98 exact, 17 floor), 3 unscored; exact sum 7,076 and average 72.2, published sum 8,112 and average 70.5. Twenty-one websites appear on both lists, so 214 entries describe 193 distinct websites and 184 reported; 20 of the 21 scored and are counted once, the 21st being one of the seven excluded without a score. Consolidated: 150 exact and 34 floor scores, published sum 12,691 and average 69.0, exact average 71.2. The two published list sums total 14,075 because the 20 shared scored firms contribute to both; the consolidated average is calculated from the 184 underlying scores rather than by averaging the two list averages. Each sum is stated beside the average computed from it.

Provenance and handling

The source is one read-only, repeatable-read production snapshot of the latest owner-matched security attempt for every currently tracked website across both lists, taken on 26 September 2026, with a website tracked on both counted once. The scan window, in UTC by time queued, was 17:13 to 18:15 for the 177 websites in the wealth and investment rescan; 20:52 for the 14 websites that also sit on the bank lists, whose latest scan is the banks and building societies rescan, so each firm carries one set of findings across both finance reports; and 21:34 for the 2 replacement addresses.

One firm, which appears on both lists, was rescanned on 28 September at 16:35 and is reported at that later scan, which replaces its 26 September result. Every completed scan used the same method. Websites without a published main score are excluded on the owner's instruction and counted in section 13. The analysis refuses to report where an evidence path is absent rather than reading it as zero.

Each case of a port answering was classified one at a time from the same scans: the service evidence recorded for each flagged port, and the other websites in the scan data and the provider's own hostname records that share each address.

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.

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.