

DOCUMENT 2 OF 4 · THE EVIDENCE AND THE EXACT FIX

Technical Evidence and Findings

Every finding with its raw evidence, the command to reproduce it and the fix, step by step.

PREPARED FOR
Harbourview Law LLP

DOMAIN ASSESSED
harbourview-llp.example

DATE OF ASSESSMENT
15 Sep 2026

REFERENCE
LT-BIZ-2026-7098

IN THIS DOCUMENT

1	Method and how to read this document	p. 2
2	Findings index	p. 4
3	The findings, F-01 to F-09	p. 5
4	Seen from outside	p. 16
5	LeakTrace AI Impersonation Check	p. 17
6	Appendix A: what we found in good order	p. 19
7	Appendix B: terms used, in plain words	p. 19
8	How we confirm each fix	p. 20

THREE DOCUMENTS AND A DATED RECORD

1 Owner Summary	2 Technical Evidence	3 Rules and Insurance	4 Assessment Record
-----------------	----------------------	-----------------------	---------------------

METHOD AND HOW TO READ THIS DOCUMENT

What we looked at, and how

IN SCOPE

Appearance of organizational credentials in known breach and paste sources; email authentication configuration, being SPF, DMARC, DKIM, transport security (MTA-STS and TLS-RPT), BMI and DNSSEC; web server transport security and certificate validity; publicly resolvable hosts and services associated with the domain; publicly readable code repositories referencing the domain; and lookalike domain registrations.

These findings are what was publicly visible on 15 September 2026. They are not a guarantee of security. Your outside changes after that date. On monitoring the same checks run again, email settings, look-alikes and new host names every hour and everything else every day, and each change found is recorded with its date. If anything here is wrong, write to info@getleaktrace.com and we will correct or delete it.

WHAT WE DID NOT DO

No sign-in to any system, no software installed, no testing behind a login. Backups, devices and staff training cannot be seen from outside.

SEVERITY

- CRITICAL

Fix first.
- HIGH

Fix this week.
- MEDIUM

Fix this month.
- LOW

Worth tidying. Fix when convenient.

HOW EACH FINDING IS LAID OUT

What we saw, in plain words. What it means for you. The raw evidence exactly as returned, with line numbers. The command to reproduce it. The fix, step by step. The check that proves it is done.

Severity is shown by label and fill, so it reads in black and white. Status: Open, Watch (amber) or Fixed (green).

COMMANDS IN THIS DOCUMENT

Every command only reads information that is already public. Run them from any computer with a terminal. Long commands are broken with a trailing backslash; type them as one line or paste them as shown.

```
dig TXT \  
_dmarc.harbourview-llp.example \  
+short @1.1.1.1
```

Example from this document: one command split across lines with a backslash.

FINDINGS INDEX

9 findings, most serious first

2

WAYS IN

7

TO TIDY

2

HIGH

ID	FINDING	AREA	SEVERITY	STATUS	PAGE
F-01	Firm addresses in breach data	Firm logins	HIGH	OPEN	5
F-02	No DMARC record	Email	HIGH	OPEN	6
F-03	Your site is missing 6 browser protections	Website	MEDIUM	OPEN	8
F-04	DNSSEC not enabled	Domains	LOW	OPEN	9
F-05	Your robots.txt file publicly lists internal paths (/wp-admin/)	Website	LOW	OPEN	10
F-06	MTA-STS not configured	Email	LOW	OPEN	11
F-07	TLS-RPT reporting not configured	Email	LOW	OPEN	12
F-08	WordPress publishes its author list	Website	LOW	OPEN	13
F-09	An online storage folder with your firm's name exists, called harbourview-llp. We could not open it and cannot tell whose it is. Please say whether it is yours	Website	LOW	OPEN	14

Appendix A on page 19 lists what we checked and found in good order.

F-01 · Firm logins

HIGH

OPEN

Firm addresses in breach data

ASSET	OBSERVED	METHOD	ROUGH FIX TIME
harbourview-llp.example	15 Sep 2026	Monitored breach databases	About 30 to 60 minutes an account

WHAT WE SAW

14 firm addresses on harbourview-llp.example are present in monitored breach databases. The passwords were exposed by other sites, not by your systems.

WHAT IT MEANS FOR YOU

A password for these addresses was published after a breach at another site. If it was reused anywhere, including your email, someone could sign in as that person. Resetting the password and turning on a second sign-in step removes the risk.

EVIDENCE · WHAT THE BREACH RECORDS SHOW, 15 SEP 2026

1	Source	monitored breach databases
2	Domain	harbourview-llp.example
3	Addresses	14

Wrapped lines carry no number.

PROOF IT IS DONE

Each exposed account shows a new password and multifactor sign-in set to Enforced in your email admin console.

FIX, STEP BY STEP · ABOUT 30 TO 60 MINUTES AN ACCOUNT

- 1 Reset the password on each exposed account, and anywhere the same password was reused.
- 2 Turn on multifactor sign-in for each account and set it to Enforced. Prefer an authenticator app to text-message codes.
- 3 Sign each account out of all sessions.
- 4 The lookup returned a count and no names. On your private assessment page, run the named address check on the addresses your people use.

F-02 · Email

HIGH

OPEN

No DMARC record

ASSET	OBSERVED	METHOD	ROUGH FIX TIME
harbourview-llp.example	15 Sep 2026, 16:43 ET	Public DNS query	About 20 minutes a stage, over two to four weeks

WHAT WE SAW

Attackers can send fake invoices and emails from your domain and recipients have no authoritative way to reject them.

WHAT IT MEANS FOR YOU

Your domain publishes no instruction telling mail servers to refuse email that fails its checks. Someone can send email in your name, and nothing you publish asks for it to be turned away. Requests to pay or to move client money, and forged invoices, can all be sent in your firm's name while this is open. Reported business email fraud losses averaged about US\$123,000 per complaint in 2025 (FBI IC3).

EVIDENCE · RAW ANSWER, 15 SEP 2026

1	;; status: NXDOMAIN (answered by 1.1.1.1): _dmarc.harbourview-llp.example does not exist
---	--

Wrapped lines carry no number.

F-02 · Email · continued

HIGH

OPEN

No DMARC record

REPRODUCE

```
dig TXT \
  _dmarc.harbourview-llp.example \
  +short @1.1.1.1
```

PROOF IT IS DONE

Run the reproduce command again. At each stage it returns the policy in force; the fix is done when it shows p=quarantine or p=reject.

FIX, STEP BY STEP · ABOUT 20 MINUTES A STAGE, OVER TWO TO FOUR WEEKS

- 1 Log into the company that manages your domain's DNS (usually where the domain is registered) → DNS Settings → Add Record → Type: TXT → Name: _dmarc → Value: v=DMARC1; p=none; rua=mailto:ADDRESS-YOU-READ@yourdomain.ca (replace yourdomain.ca with your actual domain, and ADDRESS-YOU-READ with a mailbox someone at your firm reads, because the reports arrive there).
- 2 Read the reports that arrive for about two weeks to see every service that sends mail as you, such as your booking system, accounting software and payment processor, and make sure each one is covered by SPF and DKIM.
- 3 Then change p=none to p=quarantine only when every one of those services is covered, and to p=reject the same way.
- 4 The date alone does not make a step safe: do not raise it until the reports show every sender is covered.
- 5 Do not go straight to p=reject: enforcing before every sender is known can stop your own mail being delivered.
- 6 At p=reject, receiving mail servers refuse email that pretends to come from your domain.
- 7 It stops forged mail from your own domain; lookalike domains need watching separately.

F-03 · Website

MEDIUM

OPEN

Your site is missing 6 browser protections

ASSET	OBSERVED	METHOD	ROUGH FIX TIME
harbourview-llp.example	15 Sep 2026, 16:43 ET	Public web request	Not estimated

WHAT WE SAW

Missing: Strict-Transport-Security, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy.

EVIDENCE · RAW ANSWER, 15 SEP 2026

1	HTTP/1.1 200 OK
2	Date: Tue, 15 Sep 2026 20:43:20 GMT
3	Content-Type: text/html; charset=UTF-8
4	Transfer-Encoding: chunked
5	Connection: keep-alive
6	Server: nginx
7	X-Powered-By: PHP/8.2

Wrapped lines carry no number.

REPRODUCE

```
curl -sI \  
https://harbourview-llp.example/
```

PROOF IT IS DONE

Run this after the change. The result should no longer show the finding.

FIX, STEP BY STEP

- 1 Add these response headers to every page of your site: Strict-Transport-Security, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy.
- 2 Set them wherever your site's response headers are set: your web server settings, your host's control panel or your CDN.
- 3 Then run the check shown here and confirm each one appears.

F-04 · Domains

LOW

OPEN

DNSSEC not enabled

What we saw. Your domain's traffic can be redirected to a fake version of your website without detection.

EVIDENCE · RAW ANSWER, 15 SEP 2026

```
1  *** Can't find harbourview-llp.example: No answer
2  Authoritative answers can be found from:
3  harbourview-llp.example
4  origin = ns1.harbourview-llp.example
5  mail addr = hostmaster.harbourview-llp.example
6  serial = 2026100101
7  refresh = 10000
8  retry = 2400
9  expire = 604800
10 minimum = 1800
```

Wrapped lines carry no number.

REPRODUCE

```
dig DNSKEY harbourview-llp.example \
    @1.1.1.1 +dnssec
```

PROOF IT IS DONE

Run the reproduce command again. It should return DNSKEY records.

FIX, STEP BY STEP · ABOUT 20 MINUTES

- 1 Enable DNSSEC at your DNS provider.
- 2 Most providers now offer it as a single setting; it signs your records so they cannot be quietly altered in transit.

F-05 · Website

LOW

OPEN

Your robots.txt file publicly lists internal paths (/wp-admin/)

What we saw. This tells attackers exactly where to look for admin panels and private areas.

EVIDENCE · RAW ANSWER, 15 SEP 2026

1 | **Disallow: /wp-admin/**

Line 1 is the finding. Wrapped lines carry no number.

REPRODUCE

```
curl -s https://harbourview-llp.example/robots.txt
```

PROOF IT IS DONE

Run the reproduce command again. The internal paths should no longer be listed.

FIX, STEP BY STEP · ABOUT 15 MINUTES

- 1 Remove internal and administrative paths from robots.txt.
- 2 The file is public, so listing a path there advertises it rather than hiding it.

F-06 · Email

LOW

OPEN

MTA-STS not configured

What we saw. Email-in-transit to your domain can be silently downgraded to plaintext by a network attacker. Both the _mta-sts TXT record and the policy file are missing.

EVIDENCE · RAW ANSWER, 15 SEP 2026

```
1  DNS record: (none)
2  Policy URL: https://mta-sts.harbourview-llp.example/.well-known/mta-sts.txt
   (HTTP n/a)
3  Policy text:
4  (no policy file fetched)
```

Lines 1 and 4 are the finding. Wrapped lines carry no number.

REPRODUCE

```
dig TXT _mta-sts.harbourview-llp.example +short @1.1.1.1 ; curl -s https://mta-sts.harbourview-llp.example/.well-known/mta-sts.txt
```

PROOF IT IS DONE

Run the reproduce command again. It should return a record starting v=STSV1.

FIX, STEP BY STEP · ABOUT 30 MINUTES

- 1
- Publish an MTA-STS policy and a TLS-RPT record so mail to your domain cannot be silently downgraded to an unencrypted connection.

F-07 · Email

LOW

OPEN

TLS-RPT reporting not configured

What we saw. You have no visibility into email-in-transit security failures (downgrade attempts, certificate issues, etc.).

EVIDENCE · RAW ANSWER, 15 SEP 2026

```
1 | ;; status: NXDOMAIN (answered by 1.1.1.1): _smtp._tls.harbourview-llp.example
   | does not exist
```

Wrapped lines carry no number.

REPRODUCE

```
dig TXT _smtp._tls.harbourview-llp.example +short @1.1.1.1
```

PROOF IT IS DONE

Run this after the change. The result should no longer show the finding.

FIX, STEP BY STEP

- 1 Add a TXT record named _smtp._tls for your domain with the value v=TLSRPTv1; rua=mailto:tls-reports@yourdomain.
- 2 Use an address someone reads.
- 3 Mail servers then send you a daily report whenever encrypted delivery to your domain fails.

F-08 · Website

LOW

OPEN

WordPress publishes its author list

What we saw. The display names and URL slugs of accounts that have posted content are readable without logging in, via 1 endpoint(s).

EVIDENCE · RAW ANSWER, 15 SEP 2026

```
1 GET https://harbourview-llp.example/wp-json/wp/v2/users
2 Response: 200 OK (application/json)
3 [
4   {
5     "id": 2,
6     "name": "Jordan Wexley",
7     "slug": "jordan-wexley"
8   },
9   {
10    "id": 3,
11    "name": "Harbourview Law LLP",
12    "slug": "front-desk"
13  }
14 ]
```

Wrapped lines carry no number.

REPRODUCE

```
curl -s https://harbourview-llp.example/wp-json/wp/v2/users | jq
```

PROOF IT IS DONE

Run this after the change. The result should no longer show the finding.

FIX, STEP BY STEP

- 1 Disable the WordPress REST users endpoint, or restrict it to authenticated requests.
- 2 Most security plugins expose this as one toggle.

F-09 · Website

LOW

OPEN

An online storage folder with your firm's name exists, called harbourview-llp. We could not open it and cannot tell whose it is. Please say whether it is yours

What we saw. Anyone can pick any storage name, so a name like your firm's proves nothing by itself. If it is yours, answer yes and the steps to check follow. If it is not, answer no and this closes as not yours.

EVIDENCE · RAW ANSWER, 15 SEP 2026

```
1 provider: Azure Blob
2 bucket: harbourview-llp
3 url: https://harbourview-llp.blob.storage.example/?comp=list
4 access_level: exists_protected
5 approximate_object_count: 0
```

Wrapped lines carry no number.

F-09 · Website · continued

LOW

OPEN

An online storage folder with your firm's name exists, called harbourview-llp. We could not open it and cannot tell whose it is. Please say whether it is yours

REPRODUCE

```
curl -sI https://harbourview-llp.blob.storage.example/?comp=list
```

PROOF IT IS DONE

Run this after the change. The result should no longer show the finding.

FIX, STEP BY STEP

- 1 Confirm on your dashboard whether this storage account is your firm's. If it is not, answer no there and this closes; nothing needs doing.
- 2 If it is yours, check that public access is blocked at the account level and on the folder itself.
- 3 If it is yours, check who can change that setting, and rotate any access keys that have ever had write access.
- 4 If it is yours, turn on access logging and an alert on any change to the public-access setting.

SEEN FROM OUTSIDE

The view an attacker assembles first

This is the view an attacker's AI tools assemble first. We read it first.

WHAT WE READ	WHAT IT SHOWS
Email authentication	DMARC not assessed (the lookup did not answer). SPF not assessed. DKIM couldn't be confirmed from outside (the key sits under a name only the mail service knows).
Services your DNS reveals	1 service in 1 category: email hosting. Microsoft 365 (email hosting)
Look-alike domains, live	6 registered and live
AI impersonation findings	Not checked on this reading
People your site names	Not counted on this reading

WOULD MAIL IN YOUR NAME BE REFUSED?

For each kind of service your DNS shows, what a receiving mail server does with mail that claims to come from you, read from your own SPF, DKIM and DMARC records.

SERVICE	MAIL IN YOUR NAME	RESULT
Email hosting: Microsoft 365	Not assessed: the DMARC lookup did not answer on the day. Whether it signs your mail with DKIM cannot be seen from outside; confirm it in its settings.	Not assessed

HOW PAYMENT-CHANGE AND INVOICE FRAUD USE THIS VIEW

Payment-change and invoice fraud does not need to break into anything. It relies on a client, or someone in your own office, trusting an email at the moment money is about to move, and acting on a request to pay into different bank details.

The view above is what makes that email believable. Your DNS tells anyone which services send mail for you, so they know which notices your clients expect to see. Whether that email is refused depends on your own records: without enforced DMARC, mail that only claims to be from your domain is still delivered.

It succeeds when three things line up: mail can pass as yours, nobody has a rule for checking a change of bank details, and a mailbox can be opened with a password alone. Each of the four controls below removes one of them.

- 1. **Enforced email authentication.** DMARC at p=quarantine, then p=reject, with every service that sends for you signing with a DKIM key published under your domain. Mail that fails is then refused, not delivered.
- 2. **A written rule for bank-detail changes.** Any change to bank or payment details is confirmed by phone on a number you already hold, never a number given in the message that asked for the change.
- 3. **A notice to clients.** "We never change bank details by email." On invoices, engagement letters and your email footer, so a client knows to call before paying anywhere new.
- 4. **Multi-factor sign-in on every mailbox.** So a password found in breach data, or guessed, does not open the mailbox a fraudulent request would be sent from or answered in.

LEAKTRACE AI IMPERSONATION CHECK

Not run for this reading.

Forged invoices, account takeover, stolen staff passwords, invoice redirects and clients taken by an impostor are one problem. Each starts with something visible from outside.

The check was not run for this reading. That is neither a finding nor a clear result. We ask again at the next check.

LOOK-ALIKE DOMAINS

Registered domains with names close to yours

Each domain is graded from what we read about it from outside, never from who we think owns it. Only the ones graded "Worth a look" are raised as findings. The others are listed so you can see they were found.

DOMAIN	GRADE	WHAT WE READ
harbourviewllp.example	Registered, nothing more known	harbourviewllp.example: has a website. One sign only (its name is one character off a name longer than six letters), not enough to grade it a concern.

Table continues on the next page

LOOK-ALIKE DOMAINS, CONTINUED

DOMAIN	GRADE	WHAT WE READ
harbourview-llp-law.example	Registered, nothing more known	harbourview-llp-law.example: has a website. Nothing more is known about it.
harbourviewllplaw.example	Registered, nothing more known	harbourviewllplaw.example: has a website. Nothing more is known about it.
harbourview-llp-legal.example	Registered, nothing more known	harbourview-llp-legal.example: has a website. Nothing more is known about it.
myharbourviewllp.example	Registered, nothing more known	myharbourviewllp.example: has a website. Nothing more is known about it.
harbourview-llps.example	Registered, nothing more known	harbourview-llps.example: has a website. One sign only (its name is one character off a name longer than six letters), not enough to grade it a concern.

APPENDIX A

What we checked and found in good order

CHECK	WHAT WE SAW	RESULT
Sending servers listed (SPF)	An SPF record answers for your domain	NO ISSUE
No lookalike domains of concern	None registered that we could attribute to anyone targeting you	NO ISSUE

RECORDED FOR CONTEXT

Facts recorded so you can see they were checked. There is nothing here for your firm to close, so none of it is counted.

NOTE

WordPress detected

Your website shares an IP address with 500+ other sites

APPENDIX B

Terms used, in plain words

DMARC. A published rule telling other mail servers what to do with mail that fakes your address.

DNSSEC. A signature on your domain records so they cannot be quietly altered.

Breach data. Data taken in another organization's breach and published or traded.

MTA-STTS. A published policy telling senders to insist on encryption when delivering to you.

robots.txt. A public file that tells search engines which paths to skip.

AFTER THE FIXES

How we confirm each fix

On 17 Oct we run the checks in this document again and record the result. Findings that pass are marked Fixed. Anything still open stays on your next re-check record. Questions about a finding? Reply to the email this came with, quoting LT-BIZ-2026-7098 and the finding ID.

ID	FINDING	SEVERITY	
F-01	Firm addresses in breach data	HIGH	☐ Re-checked
F-02	No DMARC record	HIGH	☐ Re-checked
F-03	Your site is missing 6 browser protections	MEDIUM	☐ Re-checked
F-04	DNSSEC not enabled	LOW	☐ Re-checked
F-05	Your robots.txt file publicly lists internal paths (/wp-admin/)	LOW	☐ Re-checked
F-06	MTA-STS not configured	LOW	☐ Re-checked
F-07	TLS-RPT reporting not configured	LOW	☐ Re-checked
F-08	WordPress publishes its author list	LOW	☐ Re-checked
F-09	An online storage folder with your firm's name exists, called harbourview-llp. We could not open it and cannot tell whose it is. Please say whether it is yours	LOW	☐ Re-checked