Institutional Media Kit

Reference material for brokers, advisors, counsel, and family office consultants introducing LeakTrace to a client.

Every claim in this document is verifiable through the sources referenced. Every case cited is a real forensic engagement anonymized by vertical and region. Every methodology component is disclosed. If you are considering introducing LeakTrace to a client, this is the document to forward.

PUBLISHED RESEARCH

30 briefings

21 sectors covered

CASE FILES

Public library

Anonymized engagement records

COVERAGE

Canada + US

Data hosted in North America

STANDARD TURNAROUND

72 hours

From engagement to briefing

POSITIONING

What LeakTrace is.

LeakTrace is a threat intelligence firm serving the professional advisors, brokers, insurers, and firms whose clients require independent verification of cyber exposure. We are not a software vendor. We do not sell tooling. We publish findings, not features.

Every engagement produces a briefing that documents a client's external attack surface, credential exposure, vendor relationships, and public-record aggregation surface. The briefing is drawn from monitored breach databases, DNS and certificate transparency records, corporate registry filings, paste-site monitoring, and public-record aggregators. No engagement requires access to a client's internal systems.

The client-facing question we answer is what an operator would see when preparing a targeted approach against the firm and its principals. The advisor-facing question we answer is whether the client's answers on the standard cyber intake are complete.

Operating principles

How we operate.

Discretion by default

We publish institutionally, not personally. Findings are never attributed to named clients. Introduction relationships are never disclosed. Discretion is the standard, not the exception.

Methodology transparency

Sources are disclosed in every briefing. Enumeration order and proprietary technique are not. The distinction matters for reproducibility without disclosing operational capability.

Evidence-backed claims

Every finding is drawn from a verifiable source. No claim is made that cannot be substantiated with the underlying source available to the client on request.

No named threat actors

We do not publish attribution to named criminal groups or state actors. That work is left to firms whose operational posture accommodates the retaliation risk it invites.

Institutional voice

Research and briefings are published under the LeakTrace name. No individual bylines. The firm's word is the collateral, not any single principal's.

Introduction primacy

Most engagements originate through introductions from brokers, wealth advisors, counsel, or existing clients. This is deliberate. Trust is easier to underwrite when the network vouches for the relationship.

Methodology

What every engagement covers.

The LeakTrace forensic audit runs against thirty-six discrete external attack surface categories. The categories below summarize what is examined in every engagement. Additional depth is added when a client's vertical or exposure profile requires it.

Domain	What we examine
Credential	Breach database inclusion, password recovery quality, credential reuse patterns across personal and business accounts
Domain	Registrar posture, DNS configuration, mail infrastructure, certificate transparency observations, visually confusable domain registrations
Public identity	Corporate registry filings, principal disclosure, address aggregation, philanthropic and directorship exposure
Portal	Publicly reachable client portals, authentication baselines, unauthenticated metadata disclosure, session and rate-limit configuration
Vendor	Vendor relationships observable through DNS and public disclosure, vendor-side breach inclusion, vendor policy adherence
Household	For high-value principals, correlation across public records, staff exposure, property management infrastructure, philanthropic vehicle posture

Every finding is delivered with a source citation, a severity assessment, a remediation recommendation, and a monitoring baseline. Remediation is not billed separately from the engagement; the audit and the recommended actions are delivered together.

Regulatory anchors

Regulatory posture per jurisdiction.

Findings are framed against the regulatory obligations that apply to the client's vertical and jurisdiction. This is not a legal opinion. It is a mapping between observed exposure and the applicable regulatory expectations, prepared to support the client's counsel in the remediation and, when required, notification process.

Canada · Federal

Personal Information Protection and Electronic Documents Act

Applies to private-sector organizations collecting, using, or disclosing personal information in the course of commercial activity.

Ontario · Health sector

Personal Health Information Protection Act

Applies to health information custodians. Sets the risk-of-significant-harm assessment obligation that triggers the notification requirement to the Information and Privacy Commissioner of Ontario.

United States · Federal

Federal Trade Commission Act, section 5

The primary federal enforcement authority for cyber posture and data security representations made to consumers.

United States · Health sector

Health Insurance Portability and Accountability Act

Applies to covered entities and business associates handling protected health information. Sets the notification framework under the Breach Notification Rule.

United States · Financial sector

Gramm-Leach-Bliley Act and Safeguards Rule

Applies to financial institutions holding non-public personal information. Updated Safeguards Rule sets specific administrative, technical, and physical safeguard expectations.

Canada · Investment industry

Canadian Investment Regulatory Organization guidance

Sector-specific cyber posture expectations for investment firms and registered representatives. Applies during examinations and enhanced due diligence reviews.

Case reference

Anonymized engagement records.

Case files in the LeakTrace library document the pattern of engagements LeakTrace conducts in each vertical: audit scope, categories of findings, client actions, and outcomes. Presented as anonymized engagement patterns rather than attributions to specific client engagements. Anonymization is by vertical and region only. Full-detail engagement records are available under nondisclosure for referrals from qualified introduction relationships once the underlying engagement has been completed and the client has authorized disclosure.

Current public library covers dental practice (Ontario, insurance renewal), law firm (United States, wire-fraud precursor), medical clinic (Ontario, provincial reporting threshold), wealth advisory firm (Canada, enhanced due diligence), single-family office (Canada, principal correlation graph), and sports agency (United States, athlete and business manager coordination).

Read the case files at getleaktrace.com/case-studies/.

Published research

Sector visibility across the North American attack surface.

The LeakTrace research library covers twenty-one sectors of the North American small-business and mid-market attack surface. Briefings are published under the LeakTrace name, without individual bylines, and address structural exposure patterns rather than individual incidents.

The library serves two purposes. For clients and advisors, it provides sector-specific context that informs the interpretation of an individual client's findings. For the industry, it establishes LeakTrace's position on the exposure patterns that matter in each vertical.

Read the library at getleaktrace.com/research/.

How introductions work.

Most LeakTrace engagements originate through introductions from insurance brokers, wealth advisors, health-law counsel, or family office consultants. The introduction path preserves the advisor's judgment as the primary trust vehicle. LeakTrace serves as the technical execution behind the introduction, not as a competing relationship with the advisor's client.

For insurance brokers. LeakTrace conducts pre-binding forensic audits when an underwriter requires independent verification of a client's cyber posture. The broker retains the primary relationship. LeakTrace delivers findings, and the broker's cyber counsel or the underwriter uses those findings to complete the binding process.

For wealth advisors. LeakTrace conducts advisor-level and household-level exposure audits when a custodian's enhanced due diligence requirements exceed what the firm's internal compliance program can independently verify. Findings are formatted for regulatory filing use in coordination with the firm's counsel.

For counsel. LeakTrace conducts forensic audits as part of the file when a client's compliance review or governance intake indicates exposure that has not been quantified. Findings are reviewed with counsel before any regulatory notification is drafted or filed.

For family office consultants. LeakTrace conducts principal-focused exposure audits covering the principal, household, and philanthropic vehicle surfaces. Consultants use the findings as the anchor for household security baseline work with the family office.

Firm details

Contact and firm information.

Canada · Headquarters

Toronto

1200 Bay Street, Suite 1201
Toronto, Ontario M5R 2A5
Canada

General inquiries · Account support · Legal correspondence

United States · Office

New York

228 Park Avenue South
New York, New York 10003
United States

US business development · Partnership inquiries

Publication rules for this document. Every claim above is verifiable through the sources referenced. Numerical statistics that appear in this document are drawn from public sources or from LeakTrace's own operating record. Absolute counts of LeakTrace's engagement volume are not disclosed. Client identities, engagement dates, and geographic detail below province or state are not disclosed under any circumstance in a public document. Introduction relationships are not disclosed. This document is provided as reference material for advisors and brokers considering an introduction to LeakTrace on behalf of a client.