



The Hidden Risk of Relying on Your Lead Vendor for Consent Proof

THE LEAD BUYER MAKING CONTACT USUALLY CARRIES THE BURDEN OF PROOF.

Many companies that buy inbound leads assume the lead vendor will maintain the consent record if it is ever needed. On the surface, that sounds reasonable. The vendor generated the lead, so they should also have the proof of consent. But this approach creates a hidden risk for lead buyers.

WHERE LIABILITY SITS

Under regulations like the TCPA, the company contacting the consumer is typically responsible for proving prior express written consent if challenged. If a complaint or lawsuit arises, that burden usually falls on the buyer making the call or sending the text.

THE PROBLEM WITH VENDOR-CONTROLLED CONSENT RECORDS

When consent proof is requested months or years later, buyers often need to ask vendors to retrieve the record. That can create delays, incomplete records, or situations where the vendor no longer has access to the data.

- Delayed retrieval while records are searched and exported
- Missing or partial evidence when records are not fully preserved
- No immediate access if a vendor relationship has ended
- Continuing liability long after the lead was generated

This creates a compliance gap: the company responsible for proof does not control the evidence.



A better approach for lead buyers

Instead of relying on vendors to store consent proof, many lead buyers now require that consent evidence is attached to every lead at delivery. This allows the buyer to store the record directly in internal systems and access it immediately whenever it is needed.

VENDOR RETRIEVAL MODEL

Evidence is requested later, often under pressure, and may be delayed, incomplete, or unavailable. The buyer remains exposed while waiting on a third party.

BUYER-CONTROLLED MODEL

Consent records are delivered with each lead and stored by the buyer from day one. Access is immediate and independent of vendor relationships.

HOW EXPRESSCONSENT SOLVES THIS

CERTIFIED DIGITAL RECORD

Require a Certified Digital Record (CDR) before a lead is accepted into your lead management workflow.

COMPLETE EVENT EVIDENCE

Each CDR captures a full webpage snapshot, disclosure language, timestamp, and supporting metadata.

API DELIVERY WITH THE LEAD

Deliver the CDR through API alongside lead data so buyers can retain records in their own systems.

ALWAYS ON HAND

Buyers never need to rely on a vendor to retrieve proof later because the evidence is already in place.

TAKING CONTROL OF YOUR CONSENT EVIDENCE

For lead buyers, attaching consent proof to each lead creates a simple but powerful compliance advantage. Instead of hoping a vendor can locate the record later, the evidence is already stored in your own system from day one.