



CONSENTVAULT.AI

A PRODUCT OF THE INNOVATIVE NATIVE

FIELD GUIDE · OCTOBER 2026 EDITION

The *Outside* Consent Register

Proof of consent that survives a demand letter, a class action, and an AI audit.

For lead gen, demand gen and anyone who lets software dial, text or talk to a human.



The 60-second **version**

- 1** A checkbox in your CRM is not proof. It is a claim, and anyone with edit rights could have written it, including you.
- 2** When a plaintiff says "I never agreed," the burden of proving consent sits with the company that called. You win with evidence, not with a field that says TRUE.
- 3** An outside consent register is an append-only ledger of every consent and every revocation, each one sealed by a party outside your company, so nobody can rewrite history without it showing.
- 4** Every dialer, texting tool and AI agent asks the register before it touches a person. No row, no ring.
- 5** The same register is the data-provenance evidence an AI management audit (ISO/IEC 42001) asks for. One build, two exams.
- 6** You can stand up version one in 30 days. The plan is on page 15.

"Your consent record is an **odometer. If you can roll it back, so can the jury's imagination."**

Consent you can't prove is consent you don't have

Every lead gen team I have worked with believes it has consent. Very few can prove it in the form a court accepts: the exact words the person saw, the moment they agreed, who they agreed to hear from, and evidence that none of it was edited later.

\$500

per call or text under the TCPA. **\$1,500 if a court finds it willful.** Per message, not per person.

4 years

the federal window a plaintiff has to sue. Your proof has to outlive your CRM migration.

~2x

TCPA class actions filed in the first half of 2025 versus the same period of 2024 (1,052 vs 539, TCPAWorld midyear report).

0

the deference courts now owe an FCC reading of the statute in a private suit (McLaughlin Chiropractic v. McKesson, U.S. Supreme Court, June 2025). Courts read the statute themselves. **Agency guidance is no longer a shield; your evidence is.**

THE FOUR WAYS CONSENT DIES



01

MISSING .

The form fired, the lead landed, and the consent language never traveled with it. You have a phone number and a hope.



02

MUTABLE .

The consent lives in an editable field. A rep, an import, an integration or a vendor can change it, and nothing records that they did. In discovery, mutable reads as made up.



03

MISMATCHED .

The person agreed to hear from one brand and a different brand called. Or the disclosure on the page changed in March and nobody kept the February version. Or the number was reassigned to someone else.



04

MUTED .

The person said stop, by text, by voicemail, by email, by telling the rep, and the system that dials never heard it.

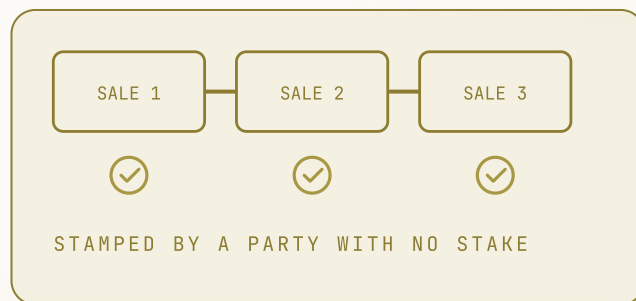
"If your consent proof is a screenshot someone took last week, you do not have consent proof. You have a screenshot."

The odometer problem

Buying a used car, you never trust the odometer by itself. You trust the title history: every sale, the mileage written down at that moment, stamped by the state, a party that has no stake in the number.

Your CRM consent field is the odometer. It shows a number, and anyone with a screwdriver can change it.

An outside consent register is the title history. Each consent event is written once, chained to the event before it, and stamped by someone outside your company. Change one old record and every stamp after it stops matching. **You do not have to promise nobody touched it. The math shows nobody did.**



The CRM checkbox

- ✗ one editable field
- ✗ overwritten on every import
- ✗ no record of who changed it
- ✗ no copy of what the person saw
- ✗ proves what the database says today

The outside register

- ✓ one sealed row per event
- ✓ append-only, never overwritten
- ✓ every change is a new row
- ✓ the exact disclosure text, hashed
- ✓ proves what was true at that moment, to someone who does not trust you

OUTSIDE CONSENT REGISTER (n.)

An append-only ledger of consent and revocation events, where each event is hash-chained to the one before it and periodically sealed by an independent third party (a trusted timestamp authority, a public transparency log, or a write-once store you cannot override), so the record can be verified by someone who does not trust the company that keeps it.

What changed, 2024 to 2026

- FEB 2024** ○ The FCC rules that AI-generated voices are "artificial" voices under the TCPA. An AI voice agent calling for marketing needs the same prior express written consent as a prerecorded robocall.
- AUG 2024** ○ The FCC proposes AI-call disclosure rules: say AI is in use at the start of the call, and make consent to AI calls explicit. Still a proposal as of this edition. **Build for it anyway.**
- JAN 2025** ○ The Eleventh Circuit vacates the FCC's "one-to-one consent" rule (Insurance Marketing Coalition v. FCC). Comparison sites can still collect consent for several sellers on one form. Not a license to get sloppy: the seller list is still your evidence.
- APR 11, 2025** ○ The revocation rule takes effect. A consumer can revoke consent by any reasonable means. Replies such as STOP, QUIT, END, REVOKE, OPT OUT, CANCEL and UNSUBSCRIBE count. You have 10 business days to honor it, and you may send one confirmation text.
- JUN 2025** ○ The Supreme Court decides McLaughlin. District courts no longer have to follow the FCC's reading of the TCPA. Expect more variance from court to court, which makes clean evidence worth more.
- SEP 1, 2025** ○ Texas SB 140 treats marketing texts as telephone solicitation and opens a private action under the Texas DTPA.
- JAN 2026** ○ The FCC pushes the "revoke-all" provision to January 31, 2027.
- OCT 1, 2026** ● **NEW** The FCC replaces revoke-all. For informational messages, an opt-out can be limited to that category (payment reminders, for example). For marketing it is not: one opt-out from a telemarketing call or text still stops all telemarketing calls and texts from that caller, affiliates included. Callers may name one exclusive opt-out method if it is clearly and conspicuously disclosed. The 10-business-day clock stays. A further proposal asks about cutting it to seven. Takes effect 30 days after Federal Register publication.

STATE LAYER Florida (FTSA, with a 15-day safe harbor after a STOP reply to a text), Oklahoma (OTSA), Texas (SB 140) and Maryland have their own rules on top of the federal floor. **Your register should know which state a person was in when they agreed.**

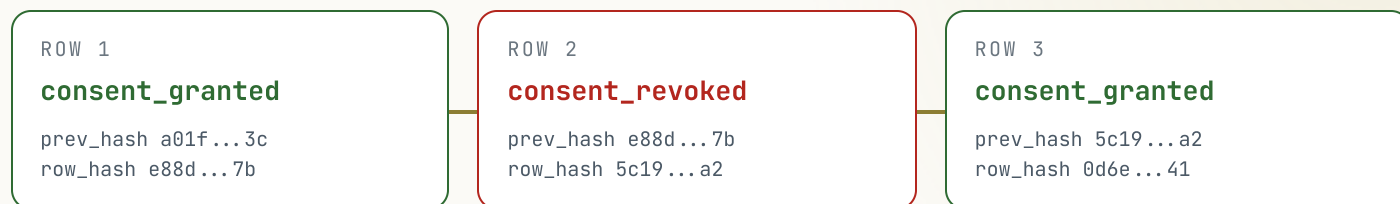
"The rules move every few months. A register that stores the exact words, the exact time and the exact scope survives every rule change, because you can re-ask the record any new question."

Anatomy of a consent event

One row per event. Never one row per person. A person who agrees, revokes, and agrees again is three rows, in order, forever.

FIELD	WHAT IT HOLDS	WHY A COURT CARES
event_id	a unique id for this event	lets every downstream system cite exactly which proof it relied on
event_type	consent_granted, consent_revoked, consent_scoped, number_reassigned	revocation is an event, not a deleted row
subject	a keyed hash of the phone and email, never the raw value in the ledger	you can prove a match without spraying PII across every log
channel_scope	calls, texts, prerecorded or AI voice, email	consent to a call is not consent to an AI voice
seller_scope	every brand named in the disclosure	the answer to "who did they agree to hear from"
disclosure_hash	SHA-256 of the exact text and the page version shown	proves the words, not a paraphrase
capture_context	page URL, form version, IP, user agent, the checkbox state (unchecked by default), the click	proves a human acted
third_party_cert	the session-certificate id from a provider such as TrustedForm or Jornaya, if used	an independent witness to the session
jurisdiction	the state at capture	drives the state rule layer
server_time	UTC from your server, not the browser	the browser clock is the plaintiff's favorite exhibit
prev_hash	the hash of the previous event in the chain	tamper evidence
row_hash	the hash of this event, including prev_hash	what the outside seal signs

One person, **three rows**, in order



ONE EVENT, AS STORED

```

{
  "event_id": "evt_01J...",
  "event_type": "consent_granted",
  "subject": "hmac:9f2c...e1",
  "channel_scope": ["calls", "texts", "ai_voice"],
  "seller_scope": ["Acme Home Services"],
  "disclosure_hash": "sha256:4b7a...90",
  "capture_context": {
    "url": "https://example.com/quote",
    "form_version": "2026-10-03.2",
    "checkbox_default": "unchecked",
    "ip": "203.0.113.24"
  },
  "third_party_cert": "cert_7Q...",
  "jurisdiction": "FL",
  "server_time": "2026-10-21T14:03:11Z",
  "prev_hash": "sha256:a01f...3c",
  "row_hash": "sha256:e88d...7b"
}

```

Example values. Your schema can differ; the principle cannot: the row carries the words, the scope, the moment and its place in the chain.

The five properties

A register earns the word "outside" when it has all five. **Four out of five is a nicer CRM.**

1

OF 5

APPEND-ONLY

Nothing is updated or deleted. A correction is a new row that points at the old one. Enforce it in the database (revoke UPDATE and DELETE, or use write-once object storage in compliance mode), not in a policy document.

2

OF 5

CHAINED

Each row carries the hash of the row before it. Change any old row and every hash after it breaks. Same idea as Certificate Transparency logs on the web.

3

OF 5

OUTSIDE-SEALED

On a schedule (hourly is plenty), hash the latest chain head and get it signed by someone you do not control: an RFC 3161 timestamp authority, a public transparency anchor, or a write-once bucket whose lock you cannot lift. Now the record proves itself to a stranger.

4

OF 5

SELF-DESCRIBING

Every seal records exactly which fields it covered. Verification checks only those fields. Add a column next year and old seals still verify.

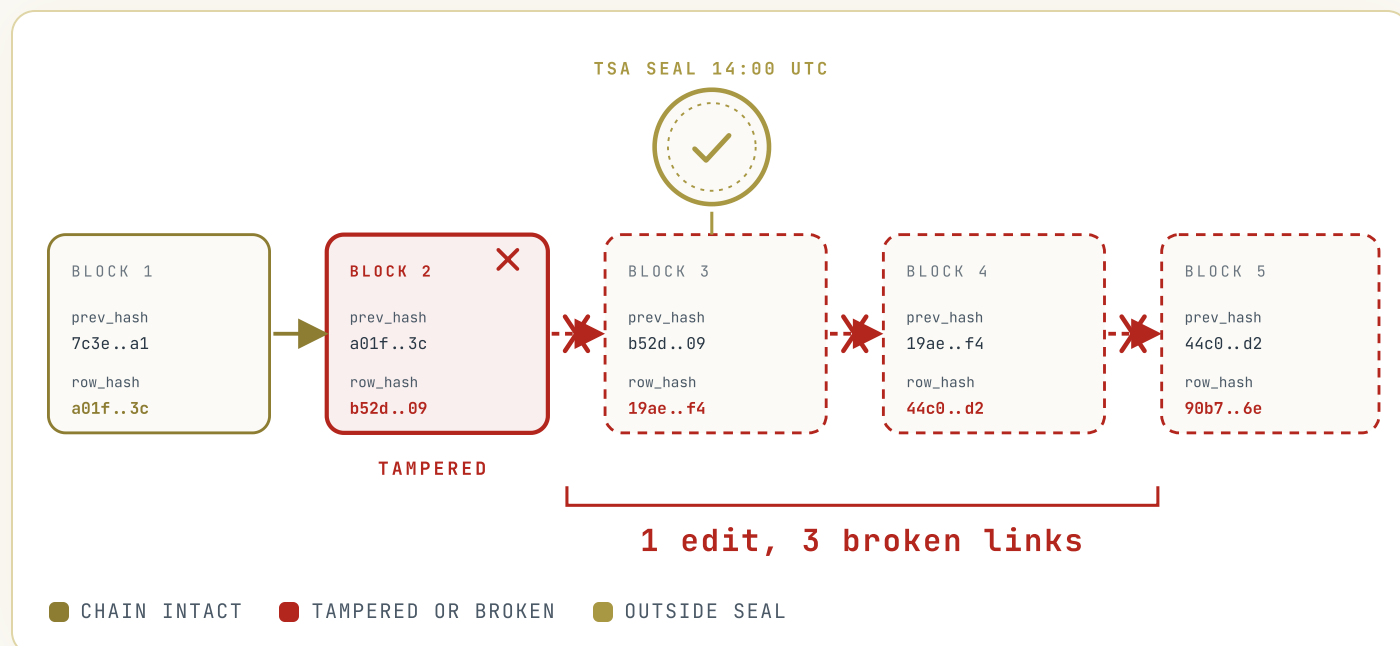
5

OF 5

RE-VERIFIED DAILY

A job re-checks every chain link and every seal every day and fails loudly, by name, the same day. A seal nobody checks is a seal nobody can testify to.

ONE EDIT, THREE BROKEN LINKS



Scar tissue

203

sealed records flagged "changed after sealing."
Not one had changed.

I learned property four the expensive way. I added one column to a consent register I built. The next morning, the daily check flagged 203 sealed records as "changed after sealing." Not one had changed. The seals had digested the whole row, so a new empty column made every old record look tampered.

Picture that in a deposition. Your own verification report, calling your own evidence altered.

THE FIX Every seal now names the exact columns it signed, and verification digests only those. A real edit still fails, loudly. A new column never does. **Nothing should ever read as tampered unless it was.**

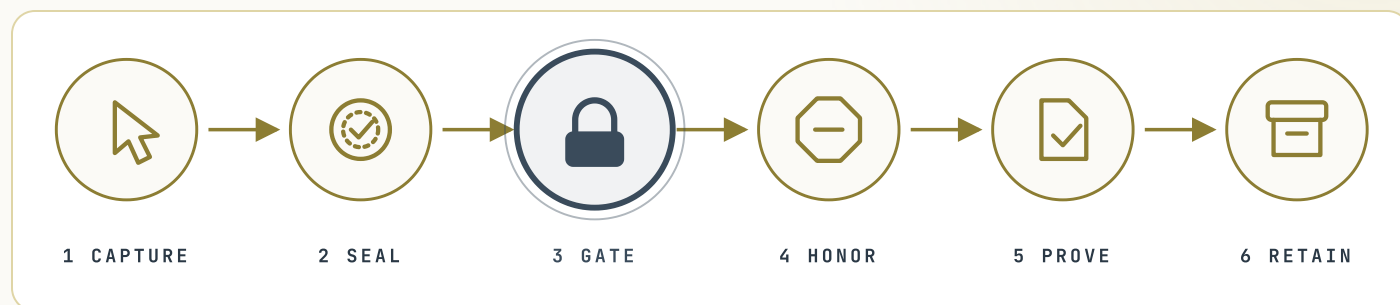
BEFORE: DIGESTED THE WHOLE ROW

event_id	event_type	subject	row_hash	server_time	new column
----------	------------	---------	----------	-------------	------------

AFTER: NAMES THE EXACT COLUMNS IT SIGNED

					new column
--	--	--	--	--	------------

The lifecycle: capture, seal, gate, honor, prove, retain



01 CAPTURE

Write the event at the moment of the click, from your server. Store the full disclosure text once in a versioned library and put its hash on the row. Unchecked box by default. Seller names in plain words next to the box, not behind a link.

02 SEAL

Chain the row on insert. Seal the chain head on a schedule. Keep the seal receipts next to the register, and keep a copy somewhere a single admin cannot delete.

03 GATE

Before any call, text, voicemail drop or AI conversation, the sending system asks one question: "Is there an unrevoked consent for this person, this channel, this seller, right now?" No row, no ring. The answer and the event_id it relied on are logged with the send.

04 HONOR

Every place a person can say stop (text reply, IVR keypress, email, the rep's disposition, a web form, a voicemail) writes a consent_revoked event to the same register. Target minutes, not the ten business days the rule allows. One opt-out from a marketing message stops all marketing from you and your affiliates.

05 PROVE

Anyone on the team can produce an evidence pack for one person in under ten minutes: every event in order, the disclosure text matching each hash, the seal receipts, and the gate decisions for every contact.

06 RETAIN

At least four years past the last contact, plus margin. Session certificates from third-party providers expire unless claimed and stored; TrustedForm's unclaimed certificates expire in about three days. Copy what you rely on into your own store.

The gate and **your AI agents**

AI voice agents and texting bots are the fastest way to multiply a consent mistake. **A human rep makes one bad call. An agent makes four thousand before lunch.**

1	NO ROW, NO RING. The agent cannot start a conversation without a fresh gate decision that names the consent event it relies on. Deny by default when the register is unreachable. A gate that fails open is not a gate.
2	AI VOICE IS ITS OWN SCOPE. Consent to "calls" is not automatically consent to an artificial or AI voice. Capture it explicitly, name it in the disclosure, and say AI is in use at the start of the call.
3	THE AGENT READS, IT NEVER WRITES CONSENT. An AI can record that a person said stop (a revocation always flows in). It can never create or restore a consent. Writing a grant is a human or capture-system action, with its own credentials.
4	EVERY OPT-OUT PHRASE, EVERY CHANNEL. "Take me off your list," "don't call me again," "stop" in a voice call: the agent's transcript is scanned for revocation language and writes the event before the call ends.

WHAT ATTACKS A CONSENT PIPELINE THAT HAS AI IN IT

Prompt injection through a form field.

A lead types instructions into the "notes" box and your summarizer obeys.

CONTROL

Treat every form field as untrusted data; the model that reads it has no tool that can change consent.

Hallucinated consent.

A model asked "did they agree?" says yes because the transcript sounded friendly.

CONTROL

Consent is a lookup in the register, never a model judgment.

PII sprawl.

Raw phone numbers flowing into prompts, logs and third-party model providers.

CONTROL

Keyed hashes in the ledger; the raw value lives in one governed store; vendors are on a no-train agreement.

Shadow tools.

A rep uploads a lead list to a consumer chatbot to "clean it up."

CONTROL

A written data-tier rule (what may enter which tool) and an approved-processor list.

Bought leads and partner leads

If you buy leads, you inherit the seller's consent, which means you inherit the seller's evidence. **Ask before the first lead lands, not after the first demand letter.**

TEN QUESTIONS FOR EVERY LEAD VENDOR



01

Show me the exact disclosure text for this campaign, with its version date.



02

Is my brand named on the page, in words, next to the consent box?



03

Is the box unchecked by default?



04

Do you pass a third-party session certificate with every lead, and how long is it valid before I must claim it?



05

Which channels did the person consent to: calls, texts, AI voice?



06

What time zone and source are your timestamps in?



07

How do you pass revocations you receive back to me, and how fast?



08

Do you sell the same lead to anyone else, and are they named too?



09

Will you put your consent-evidence obligations, and indemnity for them, in the contract?



10

Can I export or delete every record you hold on my leads, in writing?

"A lead with no certificate is a phone number with a story attached."

AI security and ISO/IEC 42001

ISO/IEC 42001:2023 is the international standard for an AI management system: the policies, roles, risk process and controls an organization uses to run AI responsibly. It follows the same management-system shape as ISO 27001 (clauses 4 to 10: context, leadership, planning, support, operation, performance evaluation, improvement), with reference controls in Annex A grouped into nine areas, A.2 through A.10.

If your AI touches consumers, your consent register is not just a TCPA defense. **It is a large share of the evidence an AI auditor will ask for.**

STANDARD AREA	WHAT THE AUDITOR ASKS	WHAT THE REGISTER SHOWS
A.2 Policies related to AI	Do you have a written rule for how AI may contact people?	The gate rule: no row, no ring, deny by default.
A.3 Internal organization	Who owns it? Who can change it?	Named owners for capture, gate and revocation; separate credentials for writing grants.
A.4 Resources for AI systems	What data and tools does the AI use?	The register is a documented data resource with its schema and versions.
A.5 Assessing impacts of AI systems	What happens to people if it goes wrong?	Unwanted calls, ignored opt-outs; the gate and revocation path are the treatment.
A.6 AI system life cycle	Is it designed, tested and monitored?	Daily re-verification, gate decision logs, revocation latency tracked.
A.7 Data for AI systems	Where did the data come from, and can you prove it?	Provenance per event: words, moment, scope, source, outside seal.
A.8 Information for interested parties	Are people told what is happening?	The disclosure text library; the AI-in-use announcement at call start.
A.9 Use of AI systems	Is AI used only for its intended purpose?	Agents can read consent and write revocations, never grants.
A.10 Third-party and customer relationships	Are vendors and lead sellers controlled?	The ten vendor questions, certificates, contract terms.

SAME EVIDENCE, NIST AI RMF

GOVERN

the rule and owners

MAP

where AI meets a consumer

MEASURE

gate denials, revocation minutes, seal checks

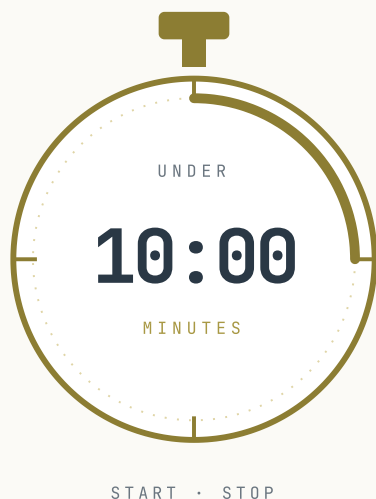
MANAGE

what happens when a check fails

"Certification is a management-system audit, not a product badge. The auditor wants to see the rule, the owner, the evidence and the check that runs when nobody is looking. A register gives you all four for one of your highest-risk AI uses."

The 10-minute proof drill

Run this on Monday. **It tells you more than any vendor demo.**



- 1 Pick a phone number at random from last month's outbound dials or texts.
- 2 Start a timer.
- 3 Produce the exact disclosure text that person saw, word for word.
- 4 Show the moment they agreed, from a server clock, and which brands and channels they agreed to.
- 5 Show every opt-out they sent, on any channel, and when it was honored.
- 6 Show evidence a stranger would accept that none of it was edited.
- 7 Stop the timer.

UNDER 10 MINUTES

Under 10 minutes with all four answered: you have a register.

OVER AN HOUR

Over an hour, or any answer is "we'd have to ask the vendor": you have a liability with a CRM on top.

SCORECARD: CIRCLE YOUR LEVEL

LEVEL 0

HOPE

Consent is a field.
Nobody knows who
can edit it.

0

LEVEL 1

CAPTURE

You store the
disclosure text and a
timestamp at the
click.

1

LEVEL 2

LEDGER

Append-only events,
revocations as rows,
one register for every
channel.

2

LEVEL 3

SEALED

Chained, outside-
sealed, re-verified
daily, seals name their
columns.

3

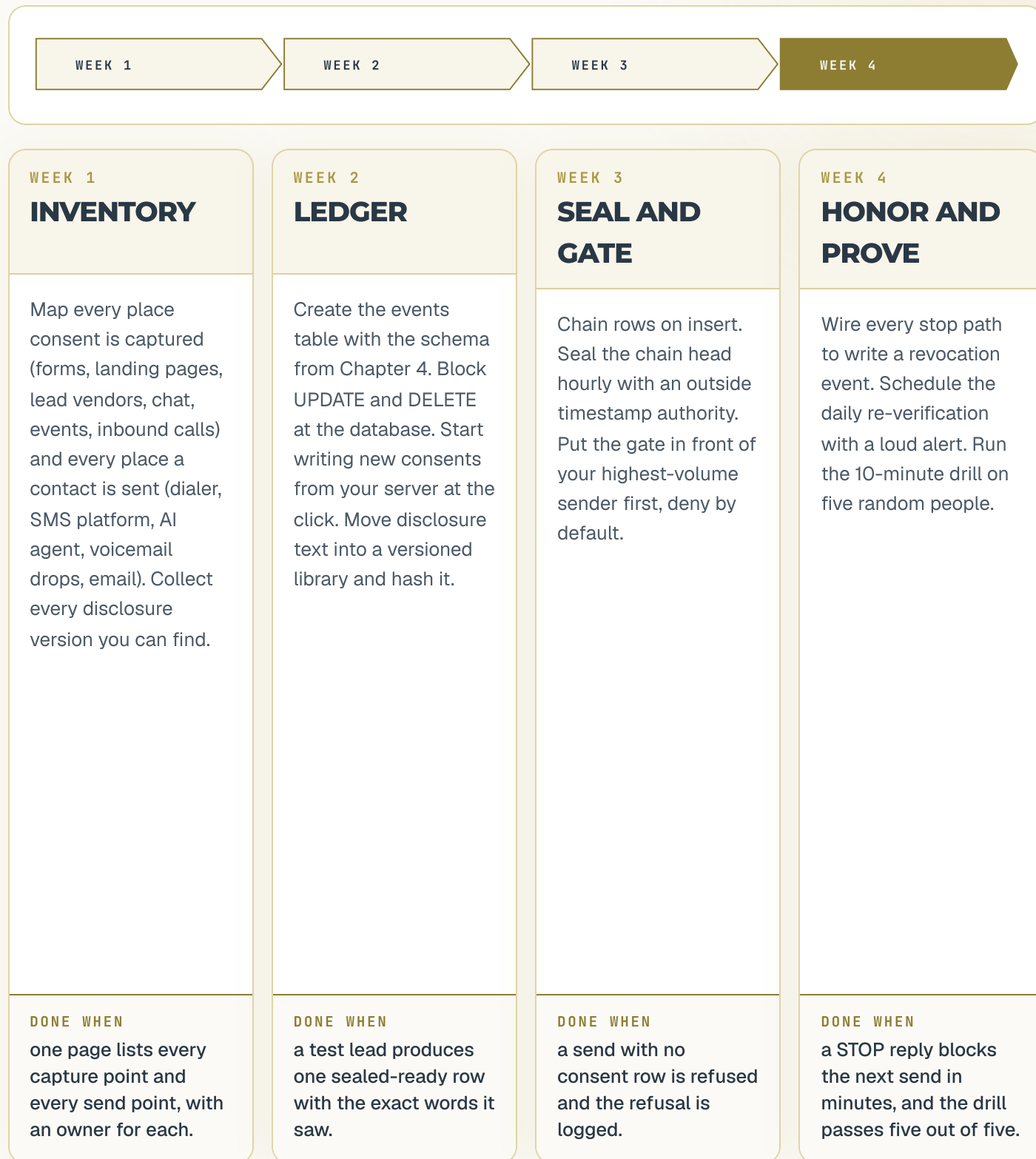
LEVEL 4

GATED

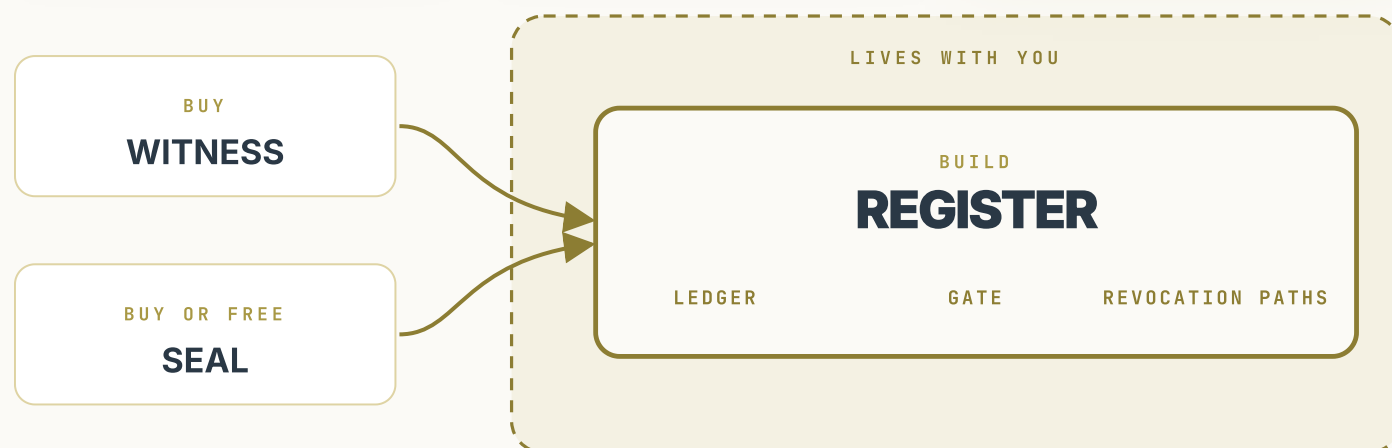
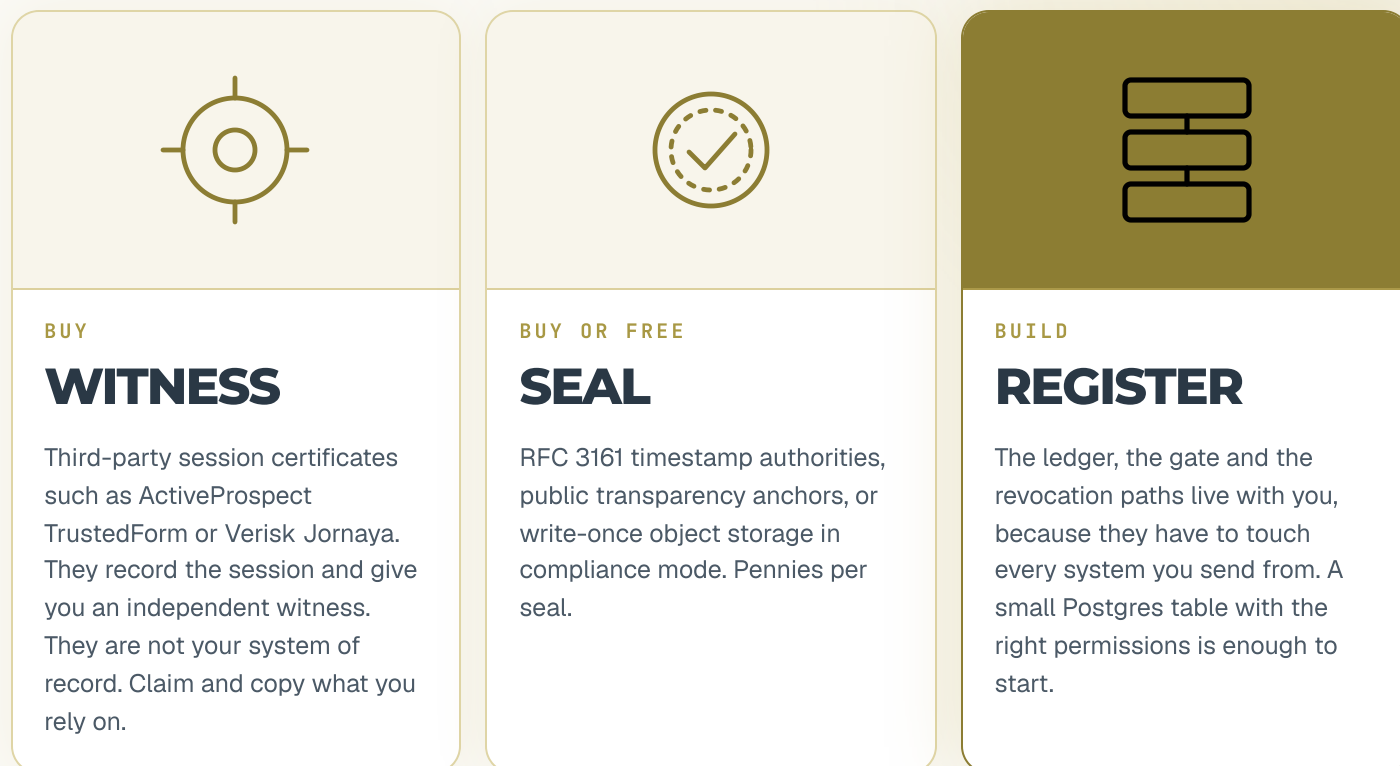
Every dialer, texter
and AI agent asks the
register first and logs
the event it relied on.
Evidence pack in
under ten minutes.

4

The 30-day build



Build, buy, or both



Buy the witnesses. Build the register. Never let the only copy of your evidence live in someone else's account.

Glossary

Prior express written consent: a signed (including e-signed) agreement to receive marketing calls or texts using an autodialer or artificial or prerecorded voice, with the required disclosures.

Hash: a fingerprint of data; change one character and the fingerprint changes completely.

RFC 3161: the internet standard for trusted timestamps, where an outside authority signs "this fingerprint existed at this time."

Gate: the check every sending system runs against the register before contact.

Revocation: the person withdrawing consent, by any reasonable means.

Hash chain: each record includes the fingerprint of the one before it.

Write-once storage: storage that cannot be overwritten or deleted until a retention date, even by an administrator.

ISO/IEC 42001: the international standard for an AI management system.

SOURCES (AS OF OCTOBER 22, 2026)

47 U.S.C. § 227 (TCPA), law.cornell.edu/uscode/text/47/227

Insurance Marketing Coalition v. FCC (11th Cir., Jan. 24, 2025); summary: [mofo.com insight 250130](https://mofo.com/insight/250130)

FCC revocation rules effective April 11, 2025; revoke-all delay to Jan. 31, 2027 (Jan. 2026 order): hunton.com, burr.com

FCC order released Oct. 1, 2026 replacing revoke-all with category opt-outs: bassberry.com, troutman.com

FCC declaratory ruling on AI-generated voices, Feb. 8, 2024: fcc.gov

FCC AI-call NPRM, Aug. 2024: benton.org, akingump.com

McLaughlin Chiropractic v. McKesson (U.S., June 20, 2025): law.cornell.edu

Texas SB 140 (eff. Sept. 1, 2025): morganlewis.com, paulhastings.com

Florida FTSA, Fla. Stat. 501.059 (2023 amendment): gmlaw.com

TCPA class action filings, H1 2025: tcpaworld.com midyear litigation report

TrustedForm certificate expiration and retention: support.activeprospect.com

ISO/IEC 42001:2023: iso.org/standard/81230.html

RFC 3161 Time-Stamp Protocol; RFC 6962 Certificate Transparency: rfc-editor.org

DISCLAIMER

This guide is education, not legal advice. Consent law varies by state and changes often; the October 2026 FCC order takes effect 30 days after Federal Register publication. Have your counsel review your disclosures and your contact rules.





CONSENT**V**AULT.AI



ABOUT THE AUTHOR

Michael Soto

Michael Soto builds AI and growth systems that grow revenue, lower acquisition cost, and run without babysitting. Twenty years in growth marketing, now building the infrastructure underneath it.

"There's a difference between using AI and having AI run your business. **The difference is the evidence.**"

GET EARLY ACCESS → CONSENTVAULT.AI



ConsentVault.AI

A Product of The Innovative Native