Tips on Vetting Lead Vendors for TCPA and CMS Compliance

This bulletin provides best practices for evaluating lead vendors to ensure compliance with the Telephone Consumer Protection Act (TCPA) and Centers for Medicare & Medicaid Services (CMS) marketing rules. The information provided is for general guidance only and is not all-encompassing. For specific situations or questions, please consult a qualified expert or seek legal advice as needed.

Lead Vendor Due Diligence

Before onboarding a lead vendor:

1. Perform a compliance review:

- Obtain copies of the vendor's consent language, sample landing pages, and data flow diagrams.
- Confirm use of Jornaya or TrustedForm on all consent pages and verify that certificates are accessible to you upon request.
- Request the vendor's written policies on TCPA compliance, consent capture, revocation processing, and do-not-call (DNC) suppression.
- Verify processes for honoring consent revocation and managing opt-out requests within required timeframes.

2. Validate technical controls:
    - Confirm certificate pass-through (LeadID/TrustedForm URL or token) with each record.
    - Test certificate URLs to ensure they are valid, match the consumer data fields, and display timestamp, originating URL, IP address, and user agent.
    - Ensure calls are recorded, stored, and accessible.
    - Confirm that storage and retention periods for consent artifacts meet CMS' ten- year (10) requirement.
3. Assess vendor credentials:

- Obtain and review any relevant certifications or audits (e.g., TCPA compliance audits, SOC reports, internal QA attestations).
- Request references from similarly regulated clients.
- Confirm vendor maintains documented training for staff handling lead generation.

Lead Intake and Verification

For every batch or individual lead received:

1. Confirm certificate presence:
    - Ensure a valid Jornaya LeadID or TrustedForm certificate link/token is included with the lead data.
    - Open the certificate and verify: consumer name and contact, capture date/time, originating URL, IP address, device/browser, and explicit consent language.
    - Confirm certificate authenticity status is valid and untampered.
2. Match data elements:
    - Validate that certificate data matches the lead record (name, phone, email, ZIP).
    - Investigate and resolve any discrepancies before contact.
3. Evaluate consent scope:

- Confirm the consent language authorizes the intended contact method and references your agency or a clearly identified partner list that includes your agency.

4. Confirm time sensitivity:
    - Ensure contact is initiated within thirty (30) days of consent capture unless otherwise permitted.
    - Do not contact leads older than the approved threshold without reconfirming consent.
5. DNC, Known Litigator and Reassigned Number and opt-out checks:
    - Ensure vendor scrubs its leads against federal/state DNC, known litigator, reassigned number, and internal DNC lists before dialing or texting.
    - Verify no prior opt-out or revocation exists in your systems or vendor's feed.

Proof of Permission to Contact

All leads must be supported by verifiable proof of prior express consent that is traceable to the consumer's submission. Agents must obtain and retain one of the following for every lead sourced from a third party:

Jornaya (Jornya) LeadID certificate evidencing the consumer's consent event; or

TrustedForm certificate of authenticity capturing the consent event.

If neither certificate is available, do not contact the lead until compliant proof of consent is obtained and validated.

- Consent must be clear, conspicuous, and specific to the type of outreach (e.g., call, text, etc.).
- Consent must be obtained by the party generating the lead and be transferable to your agency.
- Ensure all activities align with applicable CMS marketing, permission-to-contact, and documentation rules, including CMS 1:1 consent requirement.

Ongoing Monitoring

- Conduct periodic audits of a statistically valid sample of leads from each vendor, reviewing certificates and consent pages.
- Require quarterly attestations from vendors regarding compliance with TCPA and CMS requirements and any material changes in consent collection methods.
- Monitor complaint rates, opt-out rates, and bad data signals; trigger corrective action or suspension if vendor exceeds thresholds.
- Re-approve vendors annually, including a refresh of creative reviews, landing pages, and data security controls.

Watch Out for Red Flags!

- Missing or invalid Jornaya/TrustedForm certificates.

- Certificates that do not match consumer data or show vague/non-specific consent language.
- Jornaya/TrustedForm playbacks that are lengthy where the consumer data is only entered at the very end of the playback.
- Offshore IP addresses on the certificates.
- Traffic surges inconsistent with historical patterns.
- Incentivized or co-reg leads without prior approval.
- High complaint or opt-out rates.
- Vendor refusal to provide documentation or permit audits.

Recordkeeping

- Retain copies of all certificates, screenshots of the consent page as rendered, vendor contracts, training materials, audits, and communications for at least ten (10) years.
- Maintain an audit trail linking each contacted consumer to the corresponding certificate and consent language.
- Log and retain evidence of DNC scrubs, opt-outs, and revocations.

Agent & Agency Responsibilities

- Do not contact any lead lacking valid proof of consent.
- Use only approved dialing and messaging systems configured for DNC and opt-out compliance.

- Honor opt-outs immediately and document revocations.
- Immediately report any suspected vendor issue or known or suspected privacy breach, data loss, system failure, or misuse to your upline.
- Submit subcontracted lead vendor relationships to carriers according to carrier requirements.

CHECK OUT MORE BULLETINS ON LEAD VENDOR BEST PRACTICES AT Compliance - YourFMO!

Please be sure to distribute this compliance bulletin to all agents in your hierarchy.

IMPORTANT NOTICE: This compliance bulletin is intended strictly for licensed agent use only. Do not distribute to clients, prospects, or any unauthorized individuals.