



1290 WORLD LLC | TWELVE NINETY CONNECTIONS

TNC Communications Notice

Version 1.3

Document ID: TNC-COMMUNICATIONS-2026-08-23-002

Entity: 1290 World LLC, acting through 1290 World Connections and publicly known as Twelve Ninety Connections ("TNC")

Audience: Public-site visitors, participants, account holders, candidates, clients, partners, service customers, and other communication recipients

Effective Date: The date this version is accepted for a new account.

Prior versions: This version applies to new acceptances. Earlier accepted versions, signed copies, decisions, and receipts remain valid and retrievable.

1. SCOPE

This Notice applies to communications initiated, received, prepared, routed, delivered, or recorded through TNC's integrated end-to-end platform, including TNC public websites and pages, T.E.A., accounts, Network Portals, the private governed CRM backend, recruiting, Services, World Connections, Events, relationship programs, support, agreements, billing references, security, privacy, accessibility, and authorized technology-assisted workflows.

T.E.A. is the public-facing identity and interaction layer of the Integrated TNC Platform. The private governed CRM backend is the administrative, record, workflow, permission, audit, and command surface of that same platform. The frontend and backend are two operational faces of one system, not separate senders, controllers, or independent platforms. A communication request or response may begin on a public page and continue through backend routing, review, delivery, logging, suppression, or follow-up. TNC remains the accountable communicating entity, and integration does not create consent, authority, access, or permission that is otherwise absent.

TNC may communicate through T.E.A., authenticated portal messages, Secure Conversations, email, telephone, voicemail, SMS or other text messaging, video or meeting platforms, scheduling tools, in-app or push notifications, mailed or couriered records, and other disclosed and approved channels. A frontend prompt, backend workflow, provider event, or automated draft is not a separate sender and does not independently create send authority.

The applicable Network terms, action instrument, channel consent, Event terms, recording notice, privacy notice, or jurisdiction-specific addendum may impose additional requirements. The more specific instrument controls its stated subject.

2. COMMUNICATION CATEGORIES

TNC communications may include:

- Account and security: authentication, verification, passkey or multi-factor events, recovery, access changes, security alerts, suspected misuse, incident response, and closure.
- Legal and governance: terms, notices, document updates, material-change notices, acceptance, reacceptance, receipts, privacy requests, rights responses, accessibility matters, disputes, and required records.
- Relationship and Network: intake, Questions, verification, activation, status, follow-up, relationship continuity, introductions, Circles, Rooms, Tables, Events, and permitted community activity.
- Recruiting and Talent: jobs, searches, opportunity interest, résumé or identity authorization, submissions, interviews, references, offers, placements, Start Dates, onboarding, guarantees, and follow-up.
- Client and organization: organization verification, authority, account access, job creation, Protected Search, candidate review, billing contacts, administrators, and relationship administration.
- Partner: collaboration, Shared Search, source, submission, split, placement, Client payment, data access, integration, dispute, and closeout.
- Services: inquiry, scope, proposal, scheduling, dependencies, change, delivery, review, acceptance, cancellation, refund or credit, support, and closeout.



- Financial-reference: invoice, payment-status, failed-payment, refund, credit, tax, reconciliation, suspension, default, reinstatement, and enforcement notices. The approved financial system remains the source of truth for financial facts.
- Public and commercial: newsletters, offers, campaigns, programs, Events, thought leadership, market information, announcements, sponsorships, public activity, and other promotional communications permitted by law.
- Safety and emergency: urgent security, fraud, safety, service-interruption, or legally required communications appropriate to the circumstances.

3. COMMUNICATION PURPOSE AND CLASSIFICATION

Each communication should be classified by channel, sender, recipient, purpose, relationship, applicable legal basis or consent, commercial or noncommercial character, confidentiality, urgency, and required evidence.

TNC must not label a promotional message “transactional,” “security,” “relationship,” or “service” merely to avoid an opt-out or consent requirement. When a message combines transactional and promotional content, TNC must classify it according to applicable law and the message’s primary purpose.

An opt-out from promotional communications does not necessarily prevent lawful account, security, legal, billing, active recruiting, service, support, Event, or relationship communications required to administer an existing request, agreement, or relationship. A recipient may need to close or narrow the underlying relationship to stop communications essential to that relationship, subject to surviving legal and contractual obligations.

4. SENDER IDENTITY AND AUTHORITY

A communication must truthfully identify TNC or the responsible sender and, where applicable, the organization or person on whose behalf it is sent. Header, routing, caller-identification, reply, subject, domain, and display-name information must not be false, misleading, spoofed, or designed to conceal the sender.

A Participant, organization administrator, employee, contractor, Partner, vendor, or service provider may send on TNC’s behalf only within documented authority. Delegation does not eliminate TNC’s responsibility for its instructions, and a vendor’s involvement does not eliminate the sender’s or beneficiary’s legal obligations.

A message from one organization contact does not prove authority for every matter. High-consequence communications require the identity, organization, role, and authority specified by the applicable agreement or action instrument.

5. TRANSACTIONAL AND RELATIONSHIP COMMUNICATIONS

TNC may send communications reasonably necessary to authenticate or secure an Account, respond to a request, operate an active relationship, provide a requested service, administer an agreement, preserve evidence, deliver a legally required notice, or protect affected persons, as permitted by law.

Transactional and relationship communications should remain limited to the relevant purpose. TNC must not add unrelated marketing in a manner that changes the primary purpose or defeats an opt-out.

Where a recipient has no active or requested relationship, TNC must not treat a historical contact, public profile, referral, or general business affiliation as unlimited permission for repeated outreach.

6. COMMERCIAL EMAIL

Commercial email must use accurate header and routing information, a nondeceptive subject line, clear sender identification, and the disclosures required for the message and jurisdiction.

Each covered commercial email must include a clear and conspicuous opportunity to opt out and a valid current physical postal address for the sender. Before commercial email is activated, TNC must designate the address that will appear in released templates. This Notice alone does not satisfy the message-level address requirement.

The opt-out mechanism must be clear, operational, and capable of receiving requests for at least the period required by law. For U.S. CAN-SPAM-covered email, the mechanism must remain operational for at least 30 days after the message is sent, and a valid request must be honored no later than 10 business days after receipt.



TNC may not charge a fee, require information beyond the email address and opt-out preferences, or require more than a reply email or a single web page to submit or honor a CAN-SPAM opt-out.

After a recipient opts out, TNC and persons acting on its behalf must not send commercial email within the scope of the request. The opted-out address must not be sold, leased, exchanged, or transferred except as permitted for legal compliance. A later affirmative request or consent may create a new documented subscription.

TNC must maintain suppression across employees, campaigns, affiliates, and service providers that send for the same responsible sender. Hiring a vendor does not transfer away TNC's compliance responsibility.

7. EMAIL SUBSCRIPTION AND PREFERENCE RECORDS

An email subscription or commercial-email authority record should preserve:

- recipient email address and verified person or organization relationship where known;
- sender or designated sender;
- message categories selected;
- source and method of subscription or other lawful authority;
- disclosure or form version;
- date, time, session, IP or device evidence appropriate to risk;
- affirmative consent where relied upon;
- unsubscribe, suppression, correction, and resubscription history; and
- provider and campaign identifiers needed for audit.

A purchased, scraped, harvested, guessed, or transferred address list must not be used unless TNC has verified the source, legal authority, restrictions, and required notices. Public availability of an email address does not establish consent to recurring commercial email.

8. SMS, TEXTS, AND AUTOMATED COMMUNICATIONS

TNC may use SMS or other texts for verification, security, scheduling, relationship updates, recruiting coordination, service administration, Event information, billing notices, and promotional purposes only when permitted by the applicable relationship, consent, law, provider rules, and message program.

When prior express consent, prior express written consent, or another channel-specific authorization is required for an automated, prerecorded, artificial-voice, or telemarketing call or text, TNC must obtain and preserve that authorization before sending. Consent to receive promotional automated calls or texts must not be a condition of purchasing a service or establishing a relationship unless applicable law permits the condition and it is clearly disclosed.

Message frequency varies. Message and data rates may apply. Carriers and providers may delay, filter, or fail to deliver messages. Delivery is not guaranteed.

Each recurring text program should identify TNC or the responsible program, state material message-frequency information, provide HELP or another support method, and provide a clear opt-out method.

9. TEXT REVOCATION, STOP, AND CONFIRMATION

A recipient may revoke consent to covered calls or texts by any reasonable method that clearly expresses a desire not to receive further calls or texts from the sender. TNC must not require one exclusive method when applicable law permits reasonable alternatives.

For reply-capable text programs, TNC must recognize STOP, QUIT, END, REVOKE, OPT OUT, CANCEL, UNSUBSCRIBE, and other language that a reasonable person would understand as revocation. If a protocol does not accept replies, each message must clearly provide a reasonable alternative method.

A valid revocation must be honored within the period required by law and, for communications subject to the current federal rule, within a reasonable time not exceeding 10 business days.



TNC may send one nonpromotional confirmation text where permitted. The confirmation must merely confirm the request or, where multiple message categories exist, request limited clarification. Until clarification, TNC must stop consent-required messages within the reasonably understood scope. A confirmation sent promptly after the request is preferred; it must not include advertising or restart the conversation.

HELP, STOP, revocation, clarification, confirmation, suppression, and subsequent affirmative consent must each create source-tagged records.

10. TELEPHONE, VOICEMAIL, AND TELEMARKETING

TNC may call a number supplied or otherwise lawfully available for an appropriate relationship purpose. A person must not provide a number the person is not authorized to use.

Automated, prerecorded, artificial-voice, or telemarketing calls require the notice and consent applicable to the number, purpose, technology, recipient, and jurisdiction. A live business call is not automatically exempt from every federal, state, contract, privacy, or platform requirement.

For covered telephone solicitations, TNC must maintain written do-not-call procedures, train relevant personnel and vendors, keep an entity-specific suppression list, use current National Do Not Call Registry data no more than 31 days old where required, and use that Registry data only for lawful compliance purposes.

Covered residential telephone solicitations must not be initiated before 8:00 a.m. or after 9:00 p.m. at the called party's location. TNC must apply any stricter state, local, contractual, or program-specific quiet hours.

Telemarketing calls must use truthful caller identification, avoid harassment and repeated calling, comply with abandonment and connection rules where applicable, and provide the required identity and opt-out information. A prerecorded message must identify the responsible entity and provide an appropriate callback or opt-out method where required.

A do-not-call request communicated during a call, voicemail, text, email, portal message, or other reasonable method must be routed to the applicable suppression process. TNC must not continue calling merely because the request was delivered through a different supported channel.

11. REASSIGNED, WRONG, OR SHARED CONTACT INFORMATION

TNC should use reasonable processes to identify reassigned, disconnected, invalid, wrong-recipient, or shared telephone numbers and email addresses before repeated or automated communication.

A recipient who reports that a message was intended for another person must not be asked to disclose unnecessary information. TNC should correct, restrict, or remove the contact method from the affected Relationship Chapter and preserve enough suppression evidence to avoid renewed misdirection.

A wrong-recipient response does not authorize disclosure of the intended person, organization, Client account, Candidate, search, document, or relationship.

12. NATIONAL AND ENTITY-SPECIFIC DO-NOT-CALL CONTROLS

Where the National Do Not Call Registry or a state registry applies, TNC must subscribe, scrub, document, and maintain access as required before covered telemarketing activity. An established business relationship or inquiry exception does not override an entity-specific do-not-call request.

Entity-specific do-not-call and text suppression records must be accessible to relevant sending systems and providers and retained for the period required by applicable law and TNC's retention schedule.

Suppression data may not be used to create marketing audiences, infer interest, enrich profiles, or disclose that a person exercised a communications right.

13. SECURE CONVERSATIONS AND PORTAL NOTICES

Authenticated portal messages and Secure Conversations may be used for confidential relationship, recruiting, service, billing-reference, legal, privacy, security, or support communications.



Portal and message access remains limited by identity, Relationship Chapter, organization role, matter scope, audience, confidentiality, and current authorization. A portal message must not expose a private Client account, Candidate, search, document, or organization relationship to an unauthorized person.

A notification badge, email alert, or visual “sent” state is not proof that the underlying message was delivered, read, accepted, paid, activated, or completed. A legal document or consequential action requires the exact evidence and durable receipt specified by the controlling instrument.

14. WORLD CONNECTIONS MESSAGING

World Connections is not a cold bulk-outreach channel. A Participant may not send mass or substantially identical unsolicited messages, use automation to evade limits, scrape contact information, sell access, pressure another Participant, or continue after a decline or stop request.

Direct communication may require an existing relationship, accepted request, mutual introduction, shared Circle or Room, Event, organization relationship, or another valid bridge.

Payment, membership, Investor Relationship, Enterprise Diamond, 1290 Circle, title, influence, or organization status does not purchase another person’s attention or override messaging, privacy, confidentiality, moderation, or consent controls.

15. VIDEO, MEETINGS, SCHEDULING, AND EVENTS

TNC may use approved video, meeting, scheduling, calendar, and Event providers. Inviting, registering, scheduling, joining, or attending does not automatically authorize recording, transcription, publicity, marketing, or later unrelated contact.

Recording and transcription are governed by the TNC Recording & Transcription Notice and any required just-in-time notice or consent. Public or commercial use of a person’s identity, image, voice, quote, story, organization, or Event participation requires the applicable authorization.

Calendar invitations and reminders must identify the purpose, organizer, time zone, location or access method, and material confidentiality or recording information appropriate to the Event.

16. COMMUNICATION PREFERENCES AND QUIET HOURS

TNC may maintain preferences by channel, topic, Network, relationship, sender, purpose, urgency, and legal basis. A preference change applies prospectively and may require a reasonable processing period, but TNC should apply it promptly.

A preference change must not be misrepresented as closing every relationship or revoking every distinct consent. Conversely, TNC must not treat a narrow preference screen as limiting a broader revocation that the recipient reasonably communicated.

TNC should respect local time zones, Event schedules, accessibility needs, and reasonable quiet hours even when a specific legal time limit does not apply. Emergency and security communications should be limited to genuine urgent purposes.

17. T.E.A. AND TECHNOLOGY-ASSISTED COMMUNICATIONS

T.E.A. is the public-facing interface of the integrated platform. T.E.A. and other technology-assisted functions operating through the platform may help classify a communication, identify a permitted audience, prepare a draft, summarize context, recommend a channel, detect missing consent or authority, route a response, and record delivery or suppression evidence in the private CRM backend.

T.E.A. may not independently impersonate a Participant, accept an agreement, create consent, grant Account or Client access, make a final employment or investment decision, initiate an external consequential communication without the required authority, or override a stop, block, privacy choice, organization approval, or human-review requirement.

TNC remains accountable for the final recipient, content, channel, purpose, timing, confidentiality, and send authorization. The responsible human or specifically authorized system must complete any required approval. The existence of an end-to-end platform does not allow the frontend or backend to bypass a stop request, consent requirement, role boundary, organization authority, or human-review gate.



18. ACCESSIBILITY AND LANGUAGE

TNC should provide communication methods and content that support keyboard access, screen readers, zoom, readable contrast, captions or transcripts where appropriate, plain-language explanations, and reasonable alternative formats within TNC-controlled surfaces.

A recipient may request a reasonable communication accommodation or alternative channel. An accommodation request must not be treated as a promotional consent, waiver, adverse signal, or reason for retaliation.

Translated or interpreted content should identify the controlling language or resolve material ambiguity before a consequential acceptance or action.

19. PHISHING, SPOOFING, AND PAYMENT SAFETY

TNC will not ask a recipient to disclose a password, secret key, full payment-card number, or other credential through an ordinary message.

A recipient should verify unexpected payment, credential, urgent-access, document-signing, or confidential-information requests through an established TNC contact method. Suspected phishing, spoofing, impersonation, account compromise, or fraudulent messaging should be reported promptly.

A message or payment link does not itself prove an invoice, balance, payment status, or authority. The approved financial system and the applicable agreement remain controlling for financial facts.

20. THIRD-PARTY COMMUNICATION PROVIDERS

TNC may use providers for email, telephone, SMS, video, calendar, support, delivery, authentication, routing, analytics, suppression, accessibility, security, and archiving.

Providers may process sender, recipient, routing, device, delivery, failure, reply, consent, preference, and suppression information only within the approved purpose and contract. A provider connection is not proof that every capability, sender identity, campaign, number, short code, or template is approved or active.

TNC must configure and test provider-level suppression, sender authentication, access controls, retention, export, deletion, and incident handling before production use. Provider failures must not silently erase or reverse a recipient's opt-out.

21. COMMUNICATION RECORDS AND EVIDENCE

The integrated platform and private CRM backend may preserve a source-tagged communication record that includes:

- sender, responsible entity, recipient, and represented organization;
- channel, purpose, message category, and legal basis or consent;
- Network, Relationship Chapter, account, job, search, service, invoice, Event, or matter;
- template, document, disclosure, or content version;
- date, time, time zone, provider, campaign, sender address or number, and trace identifier;
- delivery, bounce, failure, filter, read, acknowledgment, reply, opt-out, revocation, complaint, or consent status;
- authority, audience, confidentiality, and human approval where required;
- suppression and resubscription history; and
- source-system, frontend entry point, backend workflow, provider, and durable receipt references.

Sent is not delivered. Delivered is not read. Read is not accepted. Accepted is not paid. Paid is not activated beyond the exact scope. Each state must remain separately recorded.

22. COMPLAINTS, DISPUTES, AND ENFORCEMENT

A recipient may report unwanted, deceptive, inaccessible, misdirected, threatening, harassing, or otherwise improper communications through the message method, the applicable portal, or TNC contact information.



TNC may investigate, restrict, suspend, preserve, or disclose communications as permitted by law and contract for security, abuse, fraud, privacy, safety, audit, dispute, legal hold, or enforcement purposes.

TNC should preserve relevant sender, consent, suppression, template, provider, and delivery records when a complaint or legal hold exists. A complaint must not be deleted merely to reduce evidence.

23. CHILDREN AND MINORS

TNC's general-audience communications are not directed to children under 13. TNC must not knowingly send marketing to or create independent messaging programs for a child under 13 outside an approved process that satisfies applicable parental-notice and consent requirements.

Communications with a permitted minor may require a parent, guardian, or legally authorized representative and must be limited to an age-appropriate, lawful purpose.

24. CHANGES, NOTICE, AND RECONSENT

TNC may update this Notice. Material changes must be versioned and presented through the notice, acknowledgment, consent, or reacceptance process required by law, contract, risk, or TNC policy.

A new Notice does not silently rewrite an earlier channel consent, opt-out, do-not-call request, communication preference, authorization, or receipt. Prior versions and evidence remain preserved.

Where a change materially affects the sender, channel, purpose, automation, recipient class, frequency, commercial content, consent requirement, or opt-out method, the affected program must remain blocked or limited until required notice or consent is complete.

25. CONTACT AND COMMUNICATION CHOICES

Communication preferences, revocations, complaints, and questions may be submitted through the applicable authenticated portal, by using the method stated in the message, or to tsullivan@1290worldconnections.com. Office: (316) 365-5546. Direct: (316) 374-4159.

For promotional email, use the unsubscribe method in the message or released preference center. For a reply-capable SMS program, reply STOP or another recognized revocation term. For telephone communications, state the do-not-call request clearly to the caller or through the designated contact method.

Before covered commercial email, telephone, or SMS activity is activated, TNC must designate and test the required physical postal address, sender identities, reply paths, HELP paths, SMS terms, short-code or number configuration, do-not-call process, preference center, and provider suppression integration.

26. SUPERSESSION AND RECORD PRESERVATION

CONTACT

Questions may be submitted through the applicable authenticated portal or to tsullivan@1290worldconnections.com. Office: (316) 365-5546. Direct: (316) 374-4159.