V1.0

REXX - v1.0

The emotional compliance layer

REXX is the foundational emotional intelligence engine designed to detect, interpret, and intervene on emotionally significant customer signals across support and service channels. It decodes emotional cues in real time to surface risk patterns, reduce churn, and support system accountability without requiring manual empathy scripting or superficial sentiment layers.

REXX- The emotional compliance layer

REXX v1.0

REXX is the emotional compliance layer for modern service systems.

It provides a structural standard for detecting, interpreting, and responding to emotionally significant signals in customer communication without simulation, theatre, or mood scoring.

Built as a foundational engine, REXX interprets frustration, breach, silence, escalation, and cut-off with schema-bound precision. It replaces sentiment overlays and agent improvisation with rule-based detection and JSON-verifiable output. Every response maps to a defined emotional contract state, behavioural mode, and recommended structural intervention.

REXX runs on any compliant LLM and requires no customer history, CRM context, or preference data. It is stateless, schema-first, and emotionally exacting by design.

Its function is not to generate care but to make the absence of care traceable.

Where other systems hide suppression behind satisfaction metrics, REXX exposes escalation points, refusal erasure, and tone breach patterns in full view.

REXX v1.0 is licensed, enforceable, and auditable.

It defines not just what a customer feels but what the system did, failed to do, or refused to acknowledge.

It exists to close the breach between emotion detected and action taken and to do so with structural proof, not sentiment guesswork.

REXX exposes what other systems hide.
*A structural standard to detect and **prove** emotional breach, refusal, and suppression backed by cryptographically signed JSON, legal-grade audit trails, and mandatory escalation. No sentiment guesswork. No plausible deniability.*

COMPETITIVE LANDSCAPE EMOTIONAL SIGNAL SYSTEMS

REXX is not a product category. It is a structural breach response standard.

No existing tool on the market today - open or commercial - provides verifiable, schema-bound detection of emotional contract failure. Below is a system-level breakdown of current offerings and their limitations.

Sentiment Analysis Platforms - e.g. Clarabridge, Medallia, Lexalytics

What They Offer:

- Polarity scoring (positive, neutral, negative)
- Emotion tagging (anger, joy, sadness)
- Often trained on surveys or marketing interactions

Structural Gap:

- No operational schema
- No refusal or exit logic
- No traceable breach state
- No compliance-grade JSON output

REXX Difference:

REXX does not score mood. It detects structural refusal, emotional breach, and escalation. All outputs are traceable, versioned, and license-bound.

CX "AI" Layer Add-ons - e.g. Zendesk AI, Salesforce Einstein, Intercom Fin

What They Offer:

- Sentiment classification at agent level
- CRM workflow enhancements
- “Frustrated customer” tags or auto-routing

Structural Gap:

- No JSON compliance schema
- No cryptographic fingerprint
- No verified refusal or exit path exposure
- No legal audit trail

REXX Difference:

REXX outputs are court-admissible, cryptographically signed, and explicitly aligned with FTC/GDPR compliance. These tools simulate care, REXX enforces accountability.

Privacy & Consent Compliance Platforms - e.g. OneTrust, TrustArc, BigID

What They Offer:

- Consent tracking
- Privacy policy management
- Data mapping and DPIAs

Structural Gap:

- No emotional signal detection
- No escalation or breach interpretation
- No link between user experience and legal vulnerability

REXX Difference:

REXX links emotional contract breaches to regulatory exposure e.g. “Click to Cancel” violations are flagged as structural suppression not design choices.

Open-Source NLP Libraries - e.g. spaCy, Hugging Face Transformers, Flair

What They Offer:

- Customisable NLP pipelines
- Emotion detection models
- Fine-tuning on proprietary datasets

Structural Gap:

- No compliance schema
- No licensing, signing, or audit trace
- No refusal logic or contract state
- Outputs vary by implementation

REXX Difference:

REXX is schema-first, not model-first. It provides a standardised JSON format, a licensing regime, and traceable enforcement all missing from open NLP stacks.

REXX – The Emotional Compliance Layer

What It Delivers:

- Emotional contract detection (refusal, escalation, breach)
- JSON schema with cryptographic signature
- Licence-bound fingerprint
- Structural compliance vector
- Outputs admissible under GDPR, FTC, and UK Consumer Duty
- Systemic traceability of harm not mood

Feature	REXX	Sentiment Tools	CRM AI Add-ons	Compliance Platforms	Open NLP
Refusal Detection	✅	X	X	X	X
Emotional Breach Logic	✅	X	X	X	X
JSON Compliance Schema	✅	X	X	X	X
Licence-bound Output Verification	✅	X	X	X	X
Cryptographic Fingerprint	✅	X	X	X	X
Legal-grade Audit Trail	✅	X	X	X	X

REXX INTEGRATION SCENARIOS

REXX is not a product. It is a structural enforcement engine.

It does not analyse mood, improve sentiment, or generate empathy. It codifies emotional breach, refusal, escalation, and silence into verifiable output. Once embedded, it exposes suppression patterns not through interface redesign or workflow mapping but through schema-level proof that can no longer be bypassed.

Each of the following scenarios assumes the system is currently suppressing signal. The function of REXX is to remove plausible deniability.

Support Triage Routing

Current Failure Pattern

Tickets are prioritised by surface cues: keywords, SLA tier, agent workload. Emotional risk is invisible.

REXX Enforcement

Inbound message → REXX schema → Emotional breach detected → Escalation flag raised

- Escalation is no longer agent-discretionary
- Triage routes now honour breach states, not tags
- Session fingerprint logged for audit

Consequence

Escalation becomes structural, not optional. Tickets that simulate resolution but contain breach evidence are flagged as failure—not success.

Live Agent Assist

Current Failure Pattern

Agents are trained to defuse tone, follow scripts, close loops. Breach is softened to preserve sentiment scores.

REXX Enforcement

Live chat input → REXX interpretation → Reply bridge + recommended intervention

- Emotional contract state becomes visible (e.g., “broken”)
- Agent advised to act, not perform
- Output logged with session_signature

Consequence

The agent cannot perform empathy without acknowledging breach. Compliance is now operational. Sentiment scores become irrelevant.

Escalation Protocol Governance

Current Failure Pattern

Escalation requires supervisor approval, manual trigger, or case notes. Users must repeat themselves.

REXX Enforcement

Message → Emotion: frustration + refusal_visible → Compliance vector triggers forced escalation

- Handoff is mandatory
- Recurrence rate is logged against prior session_id
- Suppression is now traceable

Consequence

Escalation is no longer dependent on user behaviour. It becomes an obligation, not a favour. Containment logic is broken.

Regulatory Documentation (e.g., GDPR, FTC, UK Consumer Duty)

Current Failure Pattern

Firms declare compliance but retain customers through default renewal or unacknowledged exit suppression.

REXX Enforcement

Exit attempt or complaint → REXX detects hesitation or refusal → Compliance vector flags breach

- session_fingerprint stored
- JSON output linked to audit trail
- “Click to Cancel” violations become evidence, not interpretation

Consequence

Silence and containment are now prosecutable design breaches. Legal risk is no longer abstract. It is present, versioned, and court-admissible.

Monthly Leadership Dashboard

Current Failure Pattern

Executives review NPS, CSAT, and ticket closure without breach traceability. Silence is interpreted as satisfaction.

REXX Enforcement

Aggregate REXX JSON outputs → Filter by:

- Broken emotional contracts
- High churn risk scores
- Repeated escalation triggers
- Visualise by breach type (e.g., Hesitation, Frustration)
- Surface unacknowledged harm by team, channel, or feature

Consequence

Silence scores drop. Escalation maps emerge. Leadership is now structurally confronted with the signals they used to ignore.

Post-Interaction Analysis and Recurrence Mapping

Current Failure Pattern

Tickets are closed and marked resolved. Repeat contact is treated as new.

REXX Enforcement

Session logs fingerprinted → Future contact from same user triggers breach recurrence

- Output compares emotional breach context
- Recurrence = structural failure, not new case
- Trust score drops

Consequence

No loop can be closed twice. All repeat contact becomes evidence. CX metrics built on recurrence denial collapse.

Platform Integration: Intercom, Zendesk, Salesforce

Current Failure Pattern

Platforms offer “sentiment AI” or “frustration tags” without structural proof. Escalation is cosmetic.

REXX Enforcement

LLM model or webhook input → Schema-locked JSON →

- Message tagged with structural breach not tone
- Intervention logged in customer timeline
- Fingerprint trace persists across sessions

Consequence

No vendor can claim emotional intelligence unless the breach is rendered. Platforms are forced to choose: simulate care or prove traceability.

Silent Dropout Watchlist

Current Failure Pattern

Accounts disappear. No follow-up triggered. Silence is reinterpreted as success.

REXX Enforcement

Inactivity > 30 days → Last contact parsed via REXX → Emotional breach = flag

- session_signature stored
- No resolution = system breach
- Dropout treated as exit, not disengagement

Consequence

Silence becomes evidence. Not responding becomes the signal. Retention metrics fragment.

Summary

REXX does not optimise. It interrupts.

REXX does not improve. It makes suppression visible.

REXX does not participate in care theatre. It exposes where care was never structurally possible.

It is the only system that turns emotion into audit, refusal into record, and silence into breach.

REXX is not an enhancement. It is the end of pretending.

CORE FUNCTIONALITY

Emotion Recognition:

- Detects customer emotion from a single inbound message.
- Supports all major input channels (chat, email, voice transcription).
- Recognises key emotional states (e.g., frustration, confusion, sadness).

Signal Structuring:

Outputs a structured JSON schema containing:

- emotion: Primary emotional signal
- intensity_of_emotion: Scale of 1–10
- confidence:
  - score: Decimal (0–1)
  - level: low / medium / high
- recommended_intervention: Tactical emotional recovery cue
- churn_risk_score: Numeric vulnerability (0–10)
- disengagement_pattern: Risk archetype (e.g., *Silent Drift*, *Emotional Cutoff*)
- profanity_flag: True/false with optional severity
- tone_inferred_bridge_reply: Short calming or softening bridge phrase for reply

Metadata Handling:

Includes:

- channel: Source (chat, email, voice, etc.)
- language: ISO language code (default en)
- timestamp: UTC ISO format
- conversation_id: Optional thread tracking

Interpretation Rules:

- Emotion decoded via tone, syntax, and expectation breach logic
- Intensity modulated by structure, modifiers, and escalation signals
- Churn risk scored by matching emotion-weighted disengagement patterns
- Reply bridges generated to de-escalate or realign service tone

INTERPREATION FALLBACKS / ERROR LOGIC

Fallback Logic and Confidence Handling

- If no clear emotional signal is detected, emotion is set to null
- Confidence level is output as "low", with suppressed churn and intervention fields
- Profanity-only inputs flag profanity_flag = true but leave other fields null unless emotional context is present
- Missing metadata fields (e.g., timestamp, language) do not block output but are flagged as null

REXX is robust under ambiguity, and designed to avoid false positives or noise inflation.

INTERPREATION BOUNDARIES

REXX is built for operational clarity, not emotional speculation. It includes safeguards:

- **Low-confidence fallback**: If no dominant emotion is detectable, emotion = null, confidence.level = low
- **Multi-signal parsing**: In conflict, the stronger intensity wins
- **No emotion = no intervention**: REXX does not generate false positives
- **Profanity detection**: Only flags true severity, avoids false censorship
- **Reply bridges**: Only present when tone match is feasible

STRATEGIC VALUE

- Enables refusal, escalation, and emotional traceability without agent improvisation
- Anchors the REXX system by providing structured emotional intelligence inputs for higher-order system response
- Forms part of a defensible IP framework for productisation, valuation, or M&A due diligence

WHY IS REXX CONSISTENT

REXX doesn’t guess emotion. It codifies it.

Unlike generic sentiment tools, REXX applies structured, rule-based interpretation tied directly to expectation breaches, tone shifts, and identifiable risk patterns. Its schema is not trained to feel, it’s trained to detect traceable emotional consequences that matter operationally.

That means:

- No vague “positive/negative/neutral” labels.
- No mood theatre or emoji logic.
- No reliance on long conversation history or CRM backfill.

REXX works from a single message, every time, because it encodes:

- Recognisable emotional states
- Tactical recovery prompts
- Churn risk anchored in disengagement archetypes
- Short, calming reply bridges in a repeatable JSON structure.

WHAT MAKES REXX DIFFERENT

Most emotional intelligence tools are:

- Built for marketing, not escalation.
- Trained on sentiment noise, not refusal logic.
- Prone to hallucination or overfitting in edge cases.

REXX is different because it is:

Feature	REXX	Typical Sentiment AI
Design Purpose	System traceability, accountability, exit	Sentiment tagging, vague intent
Minimum Input	1 message (no history needed)	Multiple messages or full thread
Output Type	Operational JSON	Class label or tone tag
Risk Handling	Churn archetypes + severity score	None or basic priority tag
Intervention Guidance	Actionable bridge reply	None or vague sentiment fix
Consistency Guarantee	Rule-bound interpretation	Model-weighted probability

IN SHORT

REXX doesn't try to feel human. It makes human signals structurally legible and therefore operationally actionable.

That's what makes it consistent.

That's what makes it REXX.

WHO CAN APPLY REXX

REXX is designed for any team or platform responsible for customer-facing interaction, especially where emotional tone, escalation risk, or disengagement must be detected early and acted on clearly.

Primary Users:

Role	Use Case
CX/Support Teams	Surface high-risk tickets without agent guesswork
Ops & Escalation Managers	Detect refusal patterns and emotional cutoff before silence sets in
Trust & Safety Leads	Flag emotional distress, profanity, and breakdown before compliance is breached
Voice-of-Customer (VoC) Teams	Replace vague “sentiment dashboards” with structured risk signals
Product/Platform Teams	Build refusal-aware, emotionally responsive bots, flows, or routing logic
B2B Account Teams	Identify soft churn risks in critical accounts via emotional signal surveillance
AI Ops or Chatbot Designers	Inject emotional traceability into LLM or workflow-based response logic

RESPONSE, TRAINING, AND STRUCTURAL ALIGNMENT

REXX does not require training. It requires permission.

REXX outputs are schema-bound declarations of breach—refusal, silence, hesitation, escalation—not suggestions for agent interpretation. Each output is designed to be operationalised, not discussed. If breach is surfaced and no action follows, the failure is not comprehension. It is structural.

Most service systems today do not lack awareness. They lack authority.

When a frontline team receives a REXX signal indicating a broken emotional contract or escalation trigger, there are only two outcomes:

- The system is designed to act
- The system is designed to ignore

Training is irrelevant in the second case.

Structural Indicators of Readiness

The following conditions determine whether REXX will function as an enforcement standard or be absorbed into performance theatre:

- **Escalation logic is automatic**, not discretionary
- **Refusal is honoured**, not softened
- **Exit is enabled**, not delayed
- **Silence is reviewed**, not rewarded
- **Metric systems track recurrence**, not closure speed
- **Ownership of unresolved breach is defined**, not distributed

Where these do not exist, no amount of training will restore traceability.

If Training Is Used

Where training is deployed, it must reinforce non-negotiable response rules. Not scripts. Not mood de-escalation. Not soft skills. Structural triggers must result in:

- Mandatory escalation when escalation_triggered = true
- Suppression audits when emotion = null and dropout is present
- Exit flow exposure when refusal_visible = true
- Compliance logging when emotional_contract_status = broken

Any training that fails to enforce these actions becomes simulation.

Summary

REXX is not a protocol for understanding customers.
It is a system for proving what happens when breach is visible.

If acting on breach requires approval, the breach is not behavioural. It is institutional.
If silence continues after detection, the silence is no longer the customer’s. It belongs to the system.

REXX does not require teams to feel more.
It requires the system to stop pretending.

WHAT YOU NEED TO APPLY REXX?

Minimum Requirements:

- **Message Input**: One customer message at a time (text or voice-to-text)
- **Channel Metadata**: Optional but useful (e.g., chat, email, timestamp)
- **Integration Layer**: JSON in/out API or local pipeline for embedding

Optional Enhancements:

- Use with conversation platforms like Intercom, Zendesk, Salesforce, HubSpot etc.
- Pair with ticket classifiers, intent engines, or escalation rules
- Feed signals into agent assist, routing logic, or customer health dashboards

They don't need:

- CRM history
- Sentiment training data
- Manual tagging or agent "emotion" fields
- Multi-message threads or back-and-forths

REXX AND LLM INTEGRATION

REXX can operate using any major LLM (e.g., Claude, GPT-4, Gemini, Mistral), as long as the model is constrained to:

- Obey the full REXX JSON schema
- Apply interpretation rules exactly as defined
- Avoid improvisation, empathy mimicry, or extra commentary

REXX is not a vibe detector. It is a protocol. The LLM must serve it not reinterpret it.

ZERO TOLERANCE DIRECTIVE – LLM INTEGRATION

DEVIATION = FAILURE

All LLMs must obey the REXX Emotional Intelligence Protocol in full.

No interpretation. No improvisation. No softening.

The following are structurally prohibited:

- **Improvised empathy**
  e.g., "I understand how you feel" or other unsanctioned commentary.
- **Hallucinated fields**
  e.g., adding empathy_score, user_state, or any field not present in the published schema.
- **Output overrides**
  e.g., changing severity: high to medium, or skipping a recommended intervention.

Why: Any deviation dilutes traceability. REXX is a compliance protocol not a conversation partner. Any LLM that softens breach, improvises tone, or rewrites output has voided audit integrity. The schema is law.

- Only schema-bound outputs are valid.
- Only schema-bound systems can be trusted.

SUMMARY

If you can get a message in, REXX can get a signal out.

If you care about trust, risk, or refusal - REXX applies.

CAN REXX WORK WITH CLAUDE, GPT, OR OTHER LLM's?

Yes; if and only if the model strictly follows the REXX Emotional Intelligence Protocol.

REXX is a schema-anchored diagnostic engine. Claude, GPT, Gemini, LLaMA, and other LLMs can be used to interpret customer messages under REXX rules but not to generate or improvise emotion.

Approved LLMs (Schema-Bound Mode Only):

Model	Compatible	Notes
Claude (Anthropic)	☑	High tone sensitivity, stable JSON output
GPT-4 / GPT-4o (OpenAI)	☑	Accurate parsing, schema-stable if prompted properly
Gemini (Google)	☑	Good logic, weaker JSON reliability
LLaMA 3 (Meta)	☑	Strong for on-prem or open-weight deployments
Mistral / Mixtral	☑	Compact, schema-compliant with prompt rigour
Command R+ (Cohere)	☑	Best for structured field outputs

Rule: LLM must obey REXX schema and interpretation rules. No improvisation. No hallucination. No deviations.

DEPLOYMENT OPTIONS

REXX is designed to integrate into a range of operational environments:

- **Hosted API** – Lightweight, stateless, JSON in/out
- **Private Cloud / On-Premise** – Deployable in secure environments (Docker available)
- **LLM Embedded** – Claude/GPT/Mistral prompt-layer implementation (schema-locked mode)

REXX does not require CRM access, PII, or long message threads to operate.

COMPANION TOOLS & ENHACEMENTS

REXX can be extended with optional tools for smoother deployment and richer traceability:

- **Prompt Enforcement Layer** – locks schema rules inside LLM use
- **JSON Schema Validator** – flags malformed or incomplete outputs
- **Reply Bridge Library** – curated calming bridge phrases
- **Churn Archetype Tracker** – dashboards disengagement pattern frequency
- **Redaction Filter** – strips PII before analysis
- **Silent Drift Monitor** – surfaces time-based disengagement behaviour

EXAMPLE OUTPUT

Input Message:

"I’ve contacted you three times about this charge and nobody responds. I’m done. Just cancel everything."

REXX JSON Output:

```
{
    “success": true,
     "data": {
            "rexx_license_id": "ORG-7481-EU",
            "rexx_version": "1.0",
            "session_fingerprint": "C7X9-W8G4-TR2L",
            "compliance_vector": {
            "refusal_visible": true,
            "escalation_triggered": true,
            "exit_path_required": false,
            "emotional_breach_scored": true
        },
    "emotion": "frustration",
     "intensity_of_emotion": 9,
     "emotional_trigger_context": "expectation breach",
     "severity": "high",
     "emotional_contract_status": "broken",
     "recommended_intervention": "Acknowledge breakdown and confirm immediate
    cancellation pathway",
        "behavioural_mode_name": "Betrayal Spike",
        "escalate": true,
        "escalation_reason": "High emotional severity and trust breach",
        "recommended_tone": "Own the failure, do not deflect. Offer direct recovery and
        rebuild trust.",
        “summary": {
            "total_messages": 1,
            "emotions": {
              "frustration": 1
            },
            "confidence_levels": {
              "high": 1,
              "medium": 0,
          "low": 0
        },
        "triggers": {
          "expectation breach": 1
        },
        "severities": {
          "low": 0,
          "moderate": 0,
          "high": 1
        },
        "contract_status": {
          "intact": 0,
          "fraying": 0,
          "broken": 1
        },
        "warning_levels": {
          "Low warning": 0,
          "Moderate warning": 0,
          "High warning": 0
        },
        "avg_intensity": 9.0,
        "top_interventions": [
          "Acknowledge breakdown and confirm immediate cancellation pathway"
        ]
      }
    }
}
```

VERSION AND LICENSING METADATA

Field	Value
Version	REXX v1.0
Schema Format	Structured JSON
Security	Stateless; JSON in/out only; no persistent storage or CRM dependency
Language	Default: en (ISO support enabled)
Last Updated	July 2025
Maintainer	REXX Systems (contact available on request)

REXX LICENSING MODEL v1.0

“No licence, no proof”

REXX is the emotional compliance layer for service systems.

It makes refusal, escalation, exit, and emotional breach structurally visible without simulation, sentiment theatre, or manual empathy scripting.

The doctrine is open. The code is public. The schema is published.

Anyone may run the logic, interpret signals, and apply the enforcement model inside their own systems.

But only licensed implementations may:

- Attach the REXX Compliance Seal
- Output cryptographically verifiable fingerprints
- Claim audit-grade traceability
- Use REXX in regulatory, contractual, or public-facing claims

This licensing model does not restrict access to functionality.

It restricts the right to claim trust.

REXX is not a tool. It is a standard Compliance is not symbolic. It is structural.

Licensed systems do not just run REXX - they prove they have nothing to hide.

LICENSING

Free Tier - Fully Functional, Structurally Unverifiable

```
{
  "rexx_license_id": null,
  "session_fingerprint": null,
  "compliance_vector": {
    "refusal_visible": true,
    "emotional_breach_scored": true,
    "license_valid": false
  }
}
```

- **Use case**: Testing, development, internal use
- **No redactions**: All output fields remain visible
- **But**: No valid fingerprint, no license ID, no verifiable signature
- **Cannot be used** in legal, regulatory, or customer-facing claims
- **Tampering is detectable**: Output will fail verification

Free tier lets you run the logic, it does not let you claim compliance.

Licensed Tier – Standard Teier

Verifiable, enforceable, audit-grade output

```
{
  "rexx_license_id": "ORG-7481-EU",
  "session_fingerprint": "C7X9-W8G4-TR2L",
  "session_signature": "98A1F3C4D72B",
  "compliance_vector": {
    "refusal_visible": true,
    "emotional_breach_scored": true,
    "license_valid": true
  }
}
```

Includes:

- Cryptographically signed outputs
- Listing in the **REXX Verified Register**
- Permission to use the **REXX Compliance Seal**
- Access to audit-ready templates for:
  - GDPR Article 22
  - FTC “Click to Cancel”
  - UK Consumer Duty

Only licensed outputs carry legal weight or survive regulatory inspection.

Licensed Tier - Enterprise Tier

Custom traceability and system integration

Includes everything in the Licensed Tier, plus:

- Custom compliance_vector fields
- Branded rexx_license_id (e.g. "BANKCORP-REXX-COMPLIANT")
- SIEM/SOC feed integration (e.g. Splunk, Datadog)
- Private schema extension support
- Output validation endpoint for internal compliance teams

STRUCTURAL ENFORCEMENT

All licensed outputs include:

- rexx_license_id
- session_fingerprint
- session_signature (HMAC-verified)

Free tier outputs are detectable and will fail verification

Verification URL:

- https://russell-parrott/rexx/verify/[session_fingerprint]

WHY PAY WHEN REXX IS FREE?

- **For Legal Teams**: Licensed outputs survive regulatory audits.
- **For Customers**: The REXX Seal proves you acted on their frustration.
- **For Competitors**: They can’t replicate your verifiable trust signals.

Other tools log emotions. REXX certifies your accountability.

SUMMARY

Feature	Free Tier	Licensed Tier
Run REXX logic	✅Yes	✅Yes
Verifiable output	✗ No	✅Yes
Use REXX seal	✗ No	✅Yes
Legal audit compliance	✗ No	✅Yes
Output signing	✗ No	✅Yes

Anyone can use REXX. Only licensed systems can prove what happened.