Dispute Evidence Pack Checklist

Dispute Evidence Pack Checklist

Carriers weaponize fake disputes to delay payments and bleed suppliers dry. This checklist ensures you deliver a bulletproof evidence pack to crush baseless claims and protect your cash flow. Compile and send within 48–72 hours to maintain leverage. All data must be accurate, time-synced, and tamper-proof.

1. **Call Detail Records (CDRs)**

   - Extract CDRs matching disputed invoice line-items.
   - Include UTC timestamps for call start and end.
   - Specify origination (ANI), termination (DNIS), and carrier details.
   - Provide SHA256 hash of CDR file with generation timestamp for tamper-proofing.

2. **Call Samples**

   - Include audio samples (WAV format, minimum 30 seconds) for disputed calls.
   - Provide metadata: Call-ID, UTC timestamp, and call direction (inbound/outbound).
   - Store samples proactively for 30–90 days for rapid retrieval.

3. **SIP/SS7 Signaling Headers**

   - Capture full SIP headers: P-Asserted-Identity, From, To, Call-ID.
   - Include SS7/MTP segments or gateway identifiers, if available.
   - Ensure headers are NTP-synced and stored in immutable format (e.g., WORM storage).

4. **Termination Carrier Information**

   - List carrier name, ASN, and peer IP for disputed calls.
   - Provide proof of delivery (e.g., termination confirmation or gateway logs).

5. **Invoice Details**

   - Include full invoice with disputed line-items clearly highlighted.
   - Reference contract clauses defining dispute scope and timelines (e.g., 7-day SLA).

6. **Additional Evidence (if applicable)**

   - Routing configuration logs to prove path integrity.

   - Third-party verification reports from neutral labs or monitoring vendors.

   - Time-synced system logs showing no anomalies during disputed call periods.

Best Practices for Dispute Defense

- **Automate Evidence Collection**: Use scripts to generate packs quickly and consistently.

- **Secure Storage**: Store logs and samples in write-once (WORM) systems to prevent tampering.

- **NTP Time-Sync**: Sync all systems to Network Time Protocol for consistent timestamps.

- **Rapid Response**: Deliver evidence within 48–72 hours to shut down delay tactics.

- **Escalate Smart**: If buyers demand impossible data, escalate to commercial or legal teams, citing contract deadlines.

How to Use This Checklist

1. Apply this checklist to every dispute for consistent, professional responses.

2. Package evidence in a single, secure file (e.g., encrypted ZIP) named `[DisputeID]_[InvoiceID]_[`

3. Cite relevant contract clauses in your response to limit dispute scope.

4. Retain copies of all evidence for audits, escalations, or regulatory filings.

Disclaimer: This checklist is for illustrative purposes only. Consult legal counsel to ensure compliance with your contracts and local regulations.

Visit telecom.wtf for more tools to fight telecom scams.