Legal Terminology Quick Reference

Key legal rules, technical terms, and FileSworn concepts explained in plain language.

1. Federal Rules of Evidence and Civil Procedure

FRE 901: Requirement for Authenticating Evidence

Requires the proponent to produce sufficient evidence to support a finding that the item is what the proponent claims. FileSworn's SHA-256 hashing and access audit trail provide this foundation.

FRE 902(13): Self-Authenticating Certified Records (Electronic Process)

Records generated by an electronic process that produces an accurate result, shown by certification of a qualified person, are self-authenticating. FileSworn's provenance certificates satisfy this rule.

FRE 902(14): Self-Authenticating Certified Data Copied from Electronic Device

Data copied from an electronic device, authenticated by digital identification (e.g., hash value), shown by certification of a qualified person. Supports using FileSworn's SHA-256 hash as authentication.

FRCP 37(e): Failure to Preserve Electronically Stored Information

If ESI that should have been preserved is lost because a party failed to take reasonable steps, the court may order curative measures or, upon finding intent to deprive, may presume the information was unfavorable, instruct the jury, or dismiss. FileSworn's preserved evidence mode with litigation hold helps parties meet preservation obligations.

2. Technical Terms in Plain English

SHA-256 Hash

A cryptographic function that produces a unique 64-character fingerprint for any digital file. If even one bit changes, the hash changes completely. Used to prove a file has not been altered. NIST FIPS 180-4 standard.

Access Audit Trail

A chronological record of who accessed evidence and when, including viewer email, timestamp, IP address, and browser information. FileSworn generates this automatically for every shared file.

Litigation Hold

A directive to preserve all relevant documents when litigation is reasonably anticipated. In FileSworn, enabling litigation hold on a preserved evidence file prevents it from being deleted.

Viewer Identity Watermark

A visible overlay applied to shared content that identifies the viewer by email address. Applied in real time during viewing. Used to attribute unauthorized distribution to a specific recipient.

Temporary Access

A FileSworn storage mode where files auto-expire after a set period. Designed for temporary evidence sharing where permanent third-party storage is undesirable.

Preserved Evidence

A FileSworn storage mode where files are retained permanently. Supports litigation hold for evidence preservation compliance.

Provenance Certificate

A document certifying the origin, integrity, and access history of a digital file. FileSworn certificates include file identification, SHA-256 hash, access audit trail, viewer attribution methodology, independent verification instructions, and a declaration under 28 U.S.C. Section 1746.

Self-Authentication

Under FRE 902, certain evidence is considered authentic without requiring extrinsic evidence or live witness testimony.

28 U.S.C. Section 1746

A federal statute allowing unsworn written declarations under penalty of perjury to substitute for sworn affidavits.

Bates Numbering

A sequential numbering system for identifying documents in legal proceedings. FileSworn assigns Bates numbers automatically per case, locked once assigned.

Discovery Production

A formal transfer of documents to opposing counsel in response to discovery requests. FileSworn tracks productions with Bates-numbered logs and delivery confirmation.

Recipient Verification

Email-based identity verification required before viewing shared evidence. Ensures the intended recipient is the actual viewer.

Viewer Attribution Methodology

The four-step process (verification, rendering, persistence, log correlation) linking a viewer's verified identity to their watermarked session. Documented in Section 5 of provenance certificates. All timestamps use NTP (Network Time Protocol) synchronization.