Reliable Context

RELIABLE CONTEXT / RESEARCH & PRACTICAL GUIDANCE

Business Records as Evidence: FRE 803(6), 901, 902 and AI

> Reliable Context is a kernel of truth: a system of record for organizations that fuse private and public information and must defend every value they act on. One canonical record per real thing, a cited source and an observation date behind every value, unknowns declared rather than left blank, and any past state of the record reproducible.

Published by Reliable Context · 2026-10-29 · fre 803(6) business records · rule 902(13) 902(14) · authenticating electronic records · database records as evidence · ai generated evidence admissibility

Original article: https://reliablecontext.com/articles/business-records-as-evidence-fre-803-902-databases-and-ai-output



In this article

1. Two hurdles, not one
2. Rule 803(6): the business-records exception
3. Rule 901: authentication
4. Self-authentication: 902(11), 902(13) and 902(14)
5. Hash values and the 902(14) process
6. Machine-generated output versus human statements
7. AI output: proposed Rule 707 and draft Rule 901(c), status at 28 October 2026
8. Foundation checklist
9. Worked example: Halden Therapeutics AG (fictional)
10. Limits and jurisdictions

Two hurdles, not one

A database export, a sensor log or the output of a language model can fail in a US federal courtroom for two separate reasons. It may not be shown to be what its proponent says it is, which is a question of **authentication** under Federal Rule of Evidence (FRE) 901. Or its content may be an out-of-court statement offered for its truth, which is a question of **hearsay** under FRE 801 to 807, and the most common way through for corporate data is the business-records exception in FRE 803(6). Clearing one hurdle does not clear the other. The original Advisory Committee note to Rule 901 says that meeting the authentication requirement "by no means assures admission" because other bars, "hearsay for example, may remain" (FRE 901, Advisory Committee note).

This article covers the federal rules only. State evidence codes often track the federal text but differ in detail, and courts apply them case by case. It is an educational reading of public texts, not legal advice.

Each rule rewards a property of the system that produced the record: regular practice, contemporaneous recording, a process shown to be accurate, and copies identifiable by hash value. A system either captures these at the time or cannot reconstruct them later.

Rule 803(6): the business-records exception

Rule 803(6) admits "a record of an act, event, condition, opinion, or diagnosis" if five conditions hold (FRE 803(6)):

- **(A)** made at or near the time by, or from information transmitted by, someone with knowledge;
- **(B)** kept in the course of a regularly conducted activity of a business or other organization, whether or not for profit;
- **(C)** making the record was a regular practice of that activity;
- **(D)** these conditions are shown by a custodian or other qualified witness, or by a certification under Rule 902(11) or (12) or a statute;

- **(E)** the opponent does not show that the source, method or circumstances of preparation indicate a lack of trustworthiness.

Three points from the committee history matter for databases. First, the 1972 Advisory Committee note says a "data compilation" includes "electronic computer storage" (FRE 803, Advisory Committee note). Second, the Senate Judiciary Committee report states that the proponent need not identify the individual whose knowledge underlies an entry; a regular practice of recording from a person with knowledge suffices, and for a computer printout the foundation can come from someone "who has knowledge of the particular record system" (FRE 803, Senate Report No. 93-1277). Third, the 2014 amendment placed the burden of showing untrustworthiness on the opponent once (A) to (D) are met, and its note gives as an example the argument that a record "was prepared in anticipation of litigation" (FRE 803, 2014 Committee note). The 1972 note traces that concern to *Palmer v. Hoffman* (1943), where an accident report was excluded because it was prepared "for use in litigating, not railroading" (FRE 803, Advisory Committee note).

Rule 803(7) is the companion for missing entries. Evidence that a matter is not in a record described in 803(6) may be admitted to prove that the matter did not occur or exist, if a record was regularly kept for matters of that kind and the opponent does not show untrustworthiness (FRE 803(7)). An empty query result proves something only if the system was where every such event was regularly recorded.

Rule 901: authentication

Rule 901(a) sets a low threshold: the proponent must produce "evidence sufficient to support a finding that the item is what the proponent claims it is" (FRE 901(a)). Rule 901(b) lists examples, not a closed set. Three fit electronic records:

- **901(b)(1)**: testimony of a witness with knowledge.
- **901(b)(4)**: distinctive characteristics such as contents and internal patterns, taken with all the circumstances; metadata and record identifiers usually do this work.
- **901(b)(9), process or system**: evidence describing a process or system and showing that it produces an accurate result. The 1972 note says this example is designed for results whose accuracy depends on the process that produces them, naming X-rays and "the computer" (FRE 901, Advisory Committee note).

Self-authentication: 902(11), 902(13) and 902(14)

Rule 902 lists items that "require no extrinsic evidence of authenticity in order to be admitted" (FRE 902). Three paragraphs replace a live foundation witness with a written certification.

902(11), certified domestic records of a regularly conducted activity. The original or a copy of a domestic record that meets 803(6)(A) to (C), shown by a certification of the custodian or another qualified person that complies with a federal statute or Supreme Court rule. The proponent must give the adverse party reasonable written notice before trial and make the record and certification available for inspection (FRE 902(11)). The

2000 Committee note says a declaration that satisfies 28 U.S.C. 1746 meets the declaration requirement (FRE 902, 2000 Committee note). Rule 902(12) covers foreign records in civil cases, with a certification whose falsity would be a crime where it is signed.

902(13), certified records generated by an electronic process or system. A record generated by a process or system that produces an accurate result, shown by a certification of a qualified person that complies with the certification requirements of 902(11) or (12), plus the 902(11) notice (FRE 902(13)). The 2017 Committee note explains that the rule "specifically allows the authenticity foundation that satisfies Rule 901(b)(9)" to be laid by certification (FRE 902, 2017 Committee note, paragraph (13)).

902(14), certified data copied from an electronic device, storage medium or file. Data copied from such a source, if authenticated by "a process of digital identification", shown by a qualified person's certification and with the same notice (FRE 902(14)).

The 2017 notes draw two limits. 902(13) and 902(14) are "solely limited to authentication": a certification under them cannot be used to prove the 803(6) elements, and "any attempt to satisfy a hearsay exception must be made independently." And authentication is not reliability. In the note's words, a certification authenticating a computer output such as a spreadsheet "does not preclude an objection that the information produced is unreliable—the authentication establishes only that the output came from the computer" (FRE 902, 2017 Committee notes). A database extract offered under 902(13) or (14) therefore usually also needs a 902(11) certification for the 803(6) elements of its entries.

Hash values and the 902(14) process

A **hash value** (or digest) is a fixed-length value computed from a file's bytes. NIST's Secure Hash Standard, FIPS 180-4, specifies such algorithms (including SHA-256) and states that digests "are used to detect whether messages have been changed since the digests were generated" (FIPS 180-4).

The 902(14) Committee note explains the logic in evidentiary terms: if the hash values of original and copy differ, the copy is not identical; if they match, "it is highly improbable that the original and copy are not identical." The rule therefore allows self-authentication by a certification of a qualified person "that she checked the hash value of the proffered item and that it was identical to the original," and it is written to accept other "reliable means of identification provided by future technology" (FRE 902, 2017 Committee note, paragraph (14)).

Two consequences follow. The original's hash must be computed at collection, recording who computed it, when and with which algorithm. And a hash proves identical bytes, not true content: the same note says a defendant can still challenge hearsay on the drive and whether the defendant put the data there. The Electronic Discovery Reference Model (EDRM) defines preservation as "safeguarding relevant ESI [electronically stored information] and documents against alteration or destruction" (EDRM Model), and ISO/IEC 27037:2012 gives guidelines for collecting and preserving digital evidence (ISO/IEC 27037:2012). A documented chain of custody connects the hash recorded at collection to the hash certified for trial.

Machine-generated output versus human statements

Hearsay requires a statement, and Rule 801 defines a statement as "a person's oral assertion, written assertion, or nonverbal conduct" and the declarant as "the person who made the statement" (FRE 801(a)-(b)). Output generated by a machine without a human assertion is therefore commonly argued not to be hearsay at all. The Advisory Committee's May 2026 report takes that view of AI: "The hearsay rule is likely to be inapplicable because the solution to hearsay is cross-examination, and an AI process cannot be cross-examined" (Advisory Committee report, 17 May 2026, p. 6). The Reporter's October 2026 memorandum quotes an academic analysis to the same effect: "the hearsay rule applies to human statements" and an AI translating device's output "is not hearsay because the glasses are not a 'person'" (Evidence Rules agenda book, 15 October 2026, pp. 163, 166).

For a database this produces a field-level distinction:

- **Human-entered values** (a technician's free-text note, a manually keyed lot number) are statements of a person. Offered for their truth, they need a hearsay route, usually 803(6).
- **System-generated values** (a sensor reading, a server timestamp, an automatically assigned sequence number) are not a person's assertions. Their admissibility turns mainly on authentication under 901(b)(9) or 902(13), and on whether the process is accurate.
- **Mixed records** contain both, and each kind of field needs its own foundation.

This gap is why the Committee is studying a reliability rule for AI output: without hearsay, the remaining screens are authentication, which the Committee describes as "a low standard of admissibility" (Advisory Committee report, 17 May 2026, p. 11), and the general power to exclude under Rule 403 (Evidence Rules agenda book, 15 October 2026, p. 166).

AI output: proposed Rule 707 and draft Rule 901(c), status at 28 October 2026

Rule 707. The Standing Committee approved, with one member objecting, publication of a new Rule 707 (Machine-Generated Evidence) for comment in August 2025; it would apply Rule 702's expert-testimony standards to machine-generated evidence that would be subject to Rule 702 if a witness testified to it (Judicial Conference report, September 2025). The comment period closed on 16 February 2026 (draft minutes of the May 2026 meeting, in Evidence Rules agenda book, 15 October 2026, p. 25). On 7 May 2026 the Advisory Committee decided not to recommend action on the published rule, revised it, and chose not to republish the revision for comment at that time (Advisory Committee report, 17 May 2026). The revised draft would require the proponent of AI output offered without an expert to meet Rule 702's reliability elements, would ordinarily require an expert, and adds a notice requirement (same source). Expert panels on the draft were scheduled for the Committee's 15 October 2026 meeting (Evidence Rules agenda book, 15 October 2026). No outcome of that meeting had been published when this article was verified. Rule 707 is not in force.

Rule 901(c), deepfakes. The Committee's May 2026 view is that an amendment to Rule 901 for deepfakes "is not warranted" for now, while it refines a working draft to hold in reserve (Advisory Committee report, 17 May 2026). Under that draft, a party claiming fabrication by generative AI must first present evidence sufficient to

support a finding of fabrication; the proponent must then show the item is more likely than not authentic. The draft would apply to items offered under 901 or 902 and require pretrial notice of a fabrication claim.

What to document now. The draft Committee Note to Rule 707 lists what a court would usually examine: whether inputs and training data are sufficient and representative, whether the process was validated in similar circumstances, "what records the system keeps, what is deleted, and whether the output can be reproduced or audited", independent evaluation and access, and whether the opponent received enough information on how the process works (same source, p. 9). It also says 902(13) self-authentication is not enough for AI output equivalent to expert testimony. Whether or not Rule 707 is adopted, a proponent would need model and version identifiers, the prompt or input, retrieved source documents, configuration, timestamps, validation results and an audit trail of changes.

Foundation checklist

Rule	What the system must show	Records to keep
803(6)(A)	Entry made at or near the time, by or from a person with knowledge	Creation timestamp per entry; user or source-system identity; time zone
803(6)(B)-(C)	Kept in a regular activity; recording it was regular practice	SOPs or system documentation showing the record is routinely created; evidence of use in operations
803(6)(E)	No sign the record was made for litigation or is otherwise untrustworthy	Change history with before and after values; access controls; separation of operational records from litigation work product
803(7)	The matter would have been recorded if it had occurred	Proof the system was the mandatory place for that event type; coverage and outage logs
901(b)(4)	Distinctive characteristics tie the item to its source	Stable record identifiers, system metadata, export manifests
901(b)(9), 902(13)	The process produces an accurate result	System description, validation or calibration records, error and exception logs, version history
902(11)/(12)	Qualified person can certify the 803(6)(A)-(C) facts	Named custodian role; declaration template meeting 28 U.S.C. 1746 or the foreign-signature rule; notice log
902(14)	Copy is identical to the original	Hash of original at collection, algorithm, who computed it and when; hash of produced copy; custody log
Draft 707 (not in force)	AI output reliable and reproducible	Model and version, inputs, retrieved sources, parameters, validation studies, retention and deletion policy

Worked example: Halden Therapeutics AG (fictional)

Halden Therapeutics AG, a fictional Swiss pharmaceutical company, sues a fictional US distributor in federal court over a vaccine shipment allegedly spoiled by a cold-chain failure. It offers four items.

1. **Shipment records from its enterprise resource planning (ERP) system.** Staff enter receipt and dispatch events as they occur: human statements offered for their truth, so 803(6) applies. Because the records are kept in Switzerland and the case is civil, Halden uses a 902(12) certification from its supply-chain records custodian covering 803(6)(A) to (C), and gives the 902(11) notice.
2. **Temperature-logger readings.** Loggers record readings automatically every five minutes. There is no human declarant; the issue is authentication and accuracy. Halden offers a 902(13) certification from a qualified engineer describing the logger model, calibration certificates and the upload process.
3. **The exported database tables.** Halden's e-discovery vendor computed a SHA-256 hash of each export at collection and again before production. A 902(14) certification states that the values match. This authenticates the copy only; it does not prove the readings are accurate, which is item 2's job.
4. **A language-model summary of deviations,** generated by Halden's counsel in 2026 for the lawsuit. It fails 803(6) on its face: it was not made in a regular activity, and the 2014 note's "anticipation of litigation" argument applies directly. It is also the kind of output the draft Rule 707 targets. The better course is to offer the underlying records through an expert, retaining the prompt, model version, sources and outputs in case reliance on the tool is challenged under Rule 702.

To prove under 803(7) that no deviation report exists for the shipment, Halden must show every deviation is regularly recorded in its quality system, so it keeps the SOP that makes the system mandatory and logs showing no outage in the relevant weeks.

Limits and jurisdictions

This article reads the Federal Rules of Evidence; state rules may differ in wording and application. Admissibility is decided by the judge in each case; a certification under 902 leaves the opponent free to object on other grounds, and the 2017 notes add that a challenge may require "a forensic technical expert" and that this bears on whether notice was fair. Rule 707 and Rule 901(c) are drafts. For sector context see legal, and for keeping cited sources stable over time see preserving evidence when cited sources change.

Reliable Context is a system of record built around source-backed values.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. https://www.law.cornell.edu/rules/fre/rule_901
2. https://www.law.cornell.edu/rules/fre/rule_803
3. https://www.law.cornell.edu/rules/fre/rule_902
4. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
5. https://edrm.net/edrm-model
6. https://www.iso.org/standard/44381.html
7. https://www.law.cornell.edu/rules/fre/rule_801
8. https://www.uscourts.gov/sites/default/files/document/advisory_committee_on_evidence_rules_may_2026.pdf
9. https://www.uscourts.gov/sites/default/files/document/2026-10_evidence_rules_agenda_book_9-23_final.pdf

10. https://www.uscourts.gov/sites/default/files/document/rules_report_for_sept_2025_jcus_session.pdf

THE PUBLISHER

About Reliable Context

Reliable Context is a system of record for organizations that fuse private and public information and must defend every value they act on.

The guarantees

One canonical record per real thing: duplicates resolve by rule, ambiguity is shown rather than hidden, and related organizations relate without ever being merged. A verbatim, cited source and an observation date sit behind every value. Unknowns are declared as not found, blocked or not applicable with a reason, never left as an empty cell. Any past state of the record is reproducible, together with what changed since.

Where it runs

It runs inside the customer's perimeter, one database per organization. Permitted sources, model routing, reader clearance and retention are set as the customer's own policies, and every value is exportable with its chain of custody for an auditor or regulator.

What it is not

It is not a vector database or a RAG framework, not a data catalog, MDM or data-quality suite, not a CRM or data-enrichment vendor, and not a chatbot or AI assistant. Where a reader needs one of those, the honest answer is to say so and point them there.

Visit

See Reliable Context.

Reliable Context is in production use in two sectors; more than six thousand of its identity decisions were made by rule and none has been reversed. Articles published here explain general practice, cite their primary and academic sources, and name the jurisdiction of any regulatory rule they describe. They are not legal, regulatory or compliance advice for a specific organization, and requirements change.

Website: https://reliablecontext.com

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.