Safeguards Rule Compliance Summary for Customers

Effective October 1, 2026 · v1.0.0

Why this matters to your business

If your business arranges or extends vehicle financing, you are almost certainly a "financial institution" under the FTC Safeguards Rule (16 C.F.R. Part 314). The Rule makes *you* responsible for the vendors that touch your customers' information: you must select service providers capable of maintaining appropriate safeguards, require those safeguards by contract, and periodically assess them (§314.4(f)).

Here's how Dealr helps you satisfy each of those duties — by contract and with independent audit evidence.

---

1. "Select a capable service provider" — the evidence

Dealr maintains an annual SOC 2 Type II examination (Security, Availability, and Confidentiality trust criteria) covering dealr.cloud, dealr.tax, and Dealer Title Solutions, performed by an independent CPA firm. A Type II report tests controls operating over time, not just on paper. Every customer receives, on request, Dealr's SOC 3 report, security overview, and questionnaire responses. The SOC 3 report is the independent auditor's general-use report from the same examination. Qualifying plans (identified in your Order Form or plan documentation), and any customer that certifies a legal or regulatory need, receive the full SOC 2 report under confidentiality.

---

2. "Require safeguards by contract" — the DPA

Dealr's standard agreement includes a Data Processing Addendum with a Security Exhibit and a dedicated GLBA/Safeguards Annex — designed to serve as the written safeguards contract §314.4(f)(2) requires you to obtain. If your business is on an earlier form of agreement, contact us to move to the current terms.

---

3. How Dealr's controls support the Rule's elements — for the systems we host for you

These controls cover Dealr's systems and the customer information you entrust to us. They complement your business's own information-security program; they do not replace it (see §3.5 below).

Safeguards Rule element	**Dealr commitment (DPA, including its Security Exhibit)**
§314.4(a) Qualified Individual *(Dealr's program)*	Designated senior security owner accountable for Dealr's program
§314.4(b) Risk assessment *(Dealr's program)*	Risk assessments performed and refreshed periodically, driving control updates
§314.4(c)(1) Access controls	Role-based, least-privilege access with periodic reviews

Safeguards Rule element	Dealr commitment (DPA, including its Security Exhibit)
§314.4(c)(3) Encryption	Customer information encrypted in transit and at rest
§314.4(c)(4) Secure development	Code review and security testing consistent with the SOC 2 program; production and non-production environments separated
§314.4(c)(5) Multi-factor authentication	MFA for personnel access to systems Processing Personal Data; MFA is also required for every customer user sign-in and cannot be turned off
§314.4(c)(6) Disposal	Secure deletion schedules; micro-cut destruction of physical documents
§314.4(c)(7) Change management	Documented change management with review and approval
§314.4(c)(8) Logging & monitoring	Centralized security logging, monitoring, and alerting
§314.4(d) Testing	Vulnerability management and security testing consistent with the SOC 2 program (penetration testing and/or continuous scanning)
§314.4(e) Training	Security training for all personnel, at hire and periodically thereafter
§314.4(f) Service providers	Dealr flows safeguards down to its own subprocessors (published list + change notice)
Connected AI applications *(where your plan includes AI Tools)*	Access only if your admin grants it; limited to each user's permissions (your business is responsible for any changes a connected app makes); short-lived tokens you can revoke; request logs. The AI provider itself is your service provider, not Dealr's
§314.4(h) Incident response plan *(Dealr's program)*	Written, tested IR plan — including customer notification
§314.4(j) Breach notification *(your FTC filing)*	Customer notice without undue delay, in any event within 72 hours of Dealr's awareness, with limited law-enforcement and containment delays per DPA §8.1 (incident notice). Dealr also provides the incident details your filing needs (DPA Annex 4 §4, breach support). The FTC notice itself remains yours to file, on your clock; it is due no later than 30 days after your organization discovers a qualifying event involving 500+ consumers' unencrypted information (or encrypted information where the encryption key was also compromised)

3.5 What stays on your side

The Rule still requires your business to:

(1) designate your own Qualified Individual (§314.4(a));

(2) maintain your own written risk assessment (§314.4(b));

(3) run your program and train your own personnel (§314.4(e));

(4) **oversee your other service providers** (§314.4(f)), including any AI application your staff connect to Dealr through AI Tools. That AI provider receives your customer information under its own terms, so choose business accounts that don't train on your data;

(5) **evaluate and adjust** your program in light of testing results and operational changes (§314.4(g));

(6) maintain your own incident response plan (§314.4(h));

(7) have your Qualified Individual report in writing at least annually to your board of directors or a senior officer (§314.4(i)); and

(8) **notify the FTC** of qualifying breaches (§314.4(j)).

Dealr's controls and the DPA give you the vendor-side inputs for that program. They do not replace it.

Smaller-business note: if your business maintains customer information on fewer than 5,000 consumers, the written form of the risk assessment (§314.4(b)(1)), the specified testing cadence (§314.4(d)(2)), the written incident response plan (§314.4(h)), and annual board reporting (§314.4(i)) do not apply to you. The remaining duties above still do. Source: 16 C.F.R. §314.6.

---

4. "Periodically assess" — how to do it with Dealr

Each year:

(a) request our current SOC 2 report (for qualifying plans; see your Order Form or plan documentation) or our security overview and questionnaire responses. If your compliance program requires the detailed report, certify that need in writing to receive the full SOC 2 Type II report under confidentiality (DPA §9.1(c), certified-need report access);

(b) review our subprocessor list and change notices; and

(c) keep this summary, the report or questionnaire responses, and your notes as part of your vendor-assessment records.

Whether your assessment satisfies §314.4(f)(3) depends on your business's own risk determination. This summary is an **input** to that assessment, not the assessment itself. Your compliance vendor can direct questions to security@dealr.cloud.

Reflects Dealr's SOC 2 Type II report for the period May 22, 2025–May 22, 2026. The current version is always available in the Policy Center at dealr.com/policies and supersedes any downloaded copy. This summary is informational only — it creates no representation, warranty, or contractual commitment; the DPA governs contractually. It is not legal advice: your Safeguards Rule program remains your business's responsibility.