Dealr Data Processing Addendum (DPA)

Effective October 1, 2026 · v1.0.0

This Data Processing Addendum ("**DPA**") forms part of the Agreement between Dealr, Inc. ("**Dealr**") and **Customer** and governs Dealr's Processing of Personal Data in Customer Content. Capitalized terms used but not defined in this DPA have the meanings given in Section 2 of the MSA General Terms, including the terms Section 2 identifies as defined in other components of the Agreement.

1. Definitions

- "**Applicable Data Protection Law**" means all U.S. federal and state privacy, data-protection, and data-security laws applicable to the Processing of Personal Data under the Agreement, including the state consumer privacy laws listed in Annex 3 and, where applicable to Customer, the Gramm-Leach-Bliley Act ("**GLBA**") and the FTC Safeguards Rule (16 C.F.R. Part 314).
- "**Consumer Request**" means a request by a natural person to exercise privacy rights under Applicable Data Protection Law (access, deletion, correction, portability, opt-out, etc.).
- "**De-identified Data**" means data meeting the de-identification standard in MSA §8.5 and Applicable Data Protection Law's de-identification requirements.
- "**Personal Data**" means information in Customer Content that identifies, relates to, or could reasonably be linked to an identified or identifiable natural person, including "personal information," "personal data," and "nonpublic personal information" as defined by Applicable Data Protection Law.
- "**Process/Processing**" means any operation performed on Personal Data (collection, storage, use, disclosure, deletion, etc.).
- "**Security Incident**" means a confirmed or reasonably suspected breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Personal Data Processed by Dealr. Unsuccessful attempts (e.g., blocked scans, failed logins, firewall-repelled attacks) that do not compromise Personal Data are not Security Incidents.
- "**Subprocessor**" means a third party engaged by Dealr that Processes Personal Data to provide the Services. (Entities all customers connect to at Customer's direction — e.g., a lender receiving a credit application Customer submits — are recipients acting for Customer, not Subprocessors. Independent financial service providers and independent consumer reporting agencies that Process Personal Data under their own regulatory obligations and their own agreements — e.g., payment facilitators, account-verification providers, and background-check consumer reporting agencies — are not Subprocessors; where Dealr engages such a provider of its own choosing, it is disclosed on the Subprocessor List in a separate section. Also not Subprocessors: providers whose services Customer itself contracts for and authorizes Dealr to connect to — e.g., Customer's own payroll or DMS provider, or a Customer email environment that Customer's administrator authorizes the Services to access — and providers of AI applications that Customer's End Users authorize to access Customer Content through an AI Client Connection (MSA §10.2(d)), all of which process data as Customer's own service providers under Customer's or its End Users' agreements with them; and government authorities — e.g., state DMVs, county clerks, and tax authorities — that receive filings and submissions required for the Services or by law.)

2. Roles; Scope

2.1 **Roles.** For Personal Data in Customer Content, Customer is the controller (or "business") or, where Customer processes on behalf of another party, a processor. Dealr is Customer's processor/service provider and, under GLBA, Customer's service provider under 16 C.F.R. §314.4(f). Annex 1 (processing details) describes the Processing.

2.2 **Scope.** This DPA covers all Services under the Agreement, including the DTS Registration & Title Services under Schedule B. It also covers Personal Data in AI Interaction Records (AI Addendum §3.6), which Dealr Processes as Customer's service provider for the service-operations purposes stated there. Those services involve sensitive Personal Data such as Social Security numbers, driver's license numbers, dates of birth, and financial account information. Where Schedule B or Dealr's state-contract obligations impose stricter requirements for particular data (e.g., State Records), the stricter requirement controls for that data.

2.3 **Dealr independent-controller activities.** Dealr acts as a controller, not Customer's processor, only for: (a) account, billing, and relationship data about Customer and its End Users; (b) De-identified/Aggregate Data created under MSA §8.5 (Aggregate Data); and (c) data Dealr must Process to comply with its own legal, regulatory, and state-contract obligations. These activities are described in Dealr's privacy policy.

3. Processing Instructions & Purpose Limitation

3.1 **Instructions.** Dealr will Process Personal Data only: (a) to provide, secure, support, and maintain the Services per the Agreement; (b) per Customer's documented instructions given through the Services' features and configurations; (c) as permitted for AI-assisted verification, document-processing, and audit functions under the AI Addendum, including its disclosed service-limited training provisions and safeguards (AI Addendum §§3.1–3.3); (d) to create De-identified Data; and (e) as required by Applicable Law or Dealr's state-contract and DMV-authorization obligations. In the case of clause (e), Dealr will inform Customer of the legal requirement before Processing. This notice is not required where the law prohibits it. The Agreement, including this DPA, is Customer's complete and final instruction set. Additional instructions require a written agreement.

3.2 **Prohibitions.** Dealr will not:

(a) sell or share Personal Data (as those terms are defined in Applicable Data Protection Law);

(b) retain, use, or disclose Personal Data outside the direct business relationship with Customer or for any purpose other than those in Section 3.1 (instructions); or

(c) combine Personal Data received from Customer with personal data from other sources except to provide the Services, for security and fraud prevention, or as Applicable Data Protection Law permits for service providers.

The purposes prohibited by clause (b) include any commercial purpose of Dealr's own, except as Section 2.3 (independent-controller activities) and the AI Addendum disclose. Dealr certifies it understands these restrictions and will comply with them.

3.3 **Unlawful-instruction notice.** Dealr will notify Customer if it determines an instruction violates Applicable Data Protection Law. Dealr may suspend the affected Processing until resolved.

4. Confidentiality of Processing

Dealr limits Personal Data access to personnel and contractors who need it to perform under the Agreement, binds them to written confidentiality obligations, and trains them on data protection consistent with the Security Exhibit.

5. Security

5.1 **Program.** Dealr maintains a written information-security program with administrative, technical, and physical safeguards appropriate to the size and complexity of its business and the sensitivity of the Personal Data, as described in Annex 2 (Security Exhibit). The program is designed to satisfy the safeguards a financial institution must require of its service providers under 16 C.F.R. §314.4(f).

5.2 **Evidence.** Dealr maintains an annual SOC 2 Type II examination (Security, Availability, Confidentiality) covering the Services. Dealr may update specific controls as technology and threats evolve, provided overall protection is not materially diminished during a Service Term.

6. Subprocessors

6.1 **Authorization; list.** Customer generally authorizes Dealr to engage Subprocessors. The current list, including AI vendors, is published at the Policy Center (the "**Subprocessor List**"). Dealr will bind each Subprocessor by written terms, which may be the Subprocessor's standard commercial terms, that require it to keep Personal Data confidential and to protect it with appropriate security measures. Where a Subprocessor offers a data processing agreement, Dealr will enter into it. For DTS data, Dealr will also flow down obligations no less protective than Dealr's state-contract flow-down duties. Dealr remains responsible for its Subprocessors' performance.

6.2 **Subprocessor changes; objection; cancellation right.**

(a) *Change Notice.* Dealr will notify Customer by email to Customer's Authorized Contacts and the account's administrative email, and will record the change in the Subprocessor List's version history at the Policy Center, at least thirty (30) days before a new Subprocessor Processes Personal Data (a "**Change Notice**").

(b) *Objection.* Customer may object in writing, on reasonable and documented data-protection grounds, within the thirty (30)-day notice period (the "**Objection Window**").

(c) *Dealr's response; default is to proceed.* Dealr will consider a timely objection in good faith and may, in its sole discretion, (i) decline to deploy the Subprocessor for Customer, (ii) offer Customer a reasonable alternative configuration, or (iii) proceed with the change. Unless Dealr notifies Customer before the end of the Objection Window that it elects clause (i) or (ii), Dealr is deemed to have elected to proceed, and no further notice from Dealr is required. The "**Proceed Date**" is the earlier of (x) the date Dealr notifies Customer that it will proceed and (y) the end of the Objection Window.

(d) *Cancellation right.* If Customer objected within the Objection Window and Dealr proceeds (by notice or by default under paragraph (c)), Customer may cancel the affected Services by written notice given within fifteen (15) days after the Proceed Date. Cancellation takes effect thirty (30) days after Customer's cancellation notice. Cancellation under this Section 6.2 is not an early termination under MSA §6.3 (early termination of annual terms): no

exit fee applies to the affected Service, and Dealr will refund prepaid unused fees for the affected Service pro rata.

(e) *Processing pending cancellation.* Where practicable, Dealr will not deploy the new Subprocessor for the objecting Customer's Personal Data until the cancellation takes effect. If Dealr deploys it sooner, that Processing does not waive Customer's objection or cancellation right.

(f) *Shortened notice.* Where security or continuity requires, Dealr may give the Change Notice on shorter notice, or promptly after deployment. In that case the Objection Window is fifteen (15) days after the Change Notice, and paragraphs (c) through (e) apply in the same way.

---

7. Consumer Requests & Assistance

7.1 Dealr will promptly forward to Customer any Consumer Request it receives that identifies Customer and will not respond except to direct the requester to Customer (or as Applicable Law requires).

7.2 Taking into account the nature of the Processing, Dealr will provide reasonable assistance for Customer to respond to Consumer Requests and to meet its security, breach-notification, and assessment obligations. Dealr provides this assistance primarily through the Services' search, export, correction, and deletion features. Assistance beyond the Services' standard features may be billed at Dealr's then-current professional-services rates.

---

8. Security Incidents

8.1 **Notice.**

(a) *Timing.* Dealr will notify affected Customers without undue delay and in any event within seventy-two (72) hours after becoming aware of a Security Incident. Where Applicable Law requires Dealr, as an entity maintaining computerized data owned or licensed by Customer, to notify Customer of the incident within a shorter period, that shorter period applies.

(b) *Awareness.* "Aware" means Dealr has confirmed, or has a reasonable basis to suspect, a Security Incident affecting Customer's Personal Data. It does not mean that Dealr has completed its investigation or determined full impact.

(c) *Permitted delay.* Dealr may delay notice (i) to the extent a law-enforcement agency determines that notice would impede a criminal investigation and requests the delay, or (ii) as strictly necessary to contain the incident and restore system integrity. In either case Dealr will notify Customer as soon as the basis for the delay ends. For law-enforcement delays, that means as soon as reasonably practicable after the agency confirms notice will no longer impede the investigation.

8.2 **Contents; updates.** The initial notice is preliminary and will include what is then known: the nature of the incident, categories of Personal Data and, where known, of affected individuals, measures taken, and a contact point. Dealr will supplement the notice as material information becomes available and will provide reasonable cooperation for Customer's own notification obligations. Those obligations include Customer's own obligations under 16 C.F.R. §314.4(j), where Customer is a financial institution under that rule, and under state breach-notification laws.

8.3 **Remediation; costs.** Dealr will investigate, mitigate, and remediate Security Incidents arising from its systems.

(a) *Incidents from Dealr's breach.* Where a Security Incident results from Dealr's breach of this DPA, Dealr will bear, as direct damages not excluded by MSA §13.1, the reasonable, documented costs of legally required notifications to affected individuals. This cost obligation is subject to the cap in MSA §13.3 (security super-cap).

(b) *Incidents from Customer's side.* This paragraph (b) applies where a Security Incident results from Customer's or its End Users' acts, omissions, credentials, or configurations (including compromised End User credentials, compromised or misused AI Client Connection tokens, and a connected AI application's handling of data it received) and not from a failure of Dealr's Security Program. Dealr will still provide the notice and cooperation in Sections 8.1–8.2 and will secure its own systems. Customer is responsible for its own investigation, remediation, and notification costs. Dealr's assistance beyond the Services' standard incident support may be billed at Dealr's then-current professional-services rates, consistent with Section 7.2 (assistance).

8.4 **No admission.** Neither the occurrence of a Security Incident nor notice of one is itself an admission of fault or liability or a breach of this DPA or the Agreement. Whether Dealr has breached this DPA is determined by whether Dealr complied with its obligations under it, including maintaining the Security Program described in Section 5 (security) and Annex 2.

---

9. Audits

9.1 **Primary mechanism.** Customer's audit and assessment rights under this DPA and Applicable Data Protection Law are satisfied by Dealr providing, upon request and no more than annually:

(a) for all Customers, Dealr's then-current SOC 3 report, Dealr's public security overview, and written responses to a reasonable security questionnaire. The SOC 3 report is the general-use report issued from Dealr's annual SOC 2 examination;

(b) for Customers on an Enterprise plan, Dealr's then-current SOC 2 Type II report under the confidentiality terms of MSA §11.3 (security reports). Another plan the Order Form or plan documentation identifies as qualifying is treated as an Enterprise plan for this purpose; and

(c) for any Customer that certifies in writing that it is required to review the detailed report to satisfy a legal or regulatory assessment obligation (including 16 C.F.R. §314.4(f)(3) or a state processor-assessment right), Dealr's then-current SOC 2 Type II report under the confidentiality terms of MSA §11.3.

9.2 **Independent assessment in lieu of audits.**

(a) *Independent assessment.* As permitted by Applicable Data Protection Law, Dealr elects to satisfy assessment obligations by (i) arranging, at least annually and at its own expense, an independent assessment of its security program by a qualified third-party assessor using recognized procedures and standards, and (ii) making the resulting reports available as provided in Section 9.1 (primary mechanism). The assessment is currently the SOC 2 Type II examination described in Section 5.2 (evidence).

(b) *No on-site audits.* Customer on-site audits of Dealr facilities and systems are not provided.

(c) *Post-incident information.* Following a Security Incident affecting Customer's Personal Data, Dealr will provide the additional written information and remote cooperation reasonably necessary for Customer to meet its legal obligations regarding that incident.

(d) *Current report.* A report is "**current**" for purposes of this Section 9 if it covers an assessment period that ended within the preceding twenty-four (24) months.

(e) *Gap-period remote assessment.* If at any time Dealr does not have a current report, then, until Dealr obtains one, Customer may conduct — itself or through a qualified independent third party bound by confidentiality obligations at least as protective as MSA §11 (confidentiality) — a reasonable remote assessment of the Dealr controls relevant to Customer's Personal Data, by security questionnaire, documentation review, and remote interviews of relevant Dealr personnel, at mutually agreed times, no more than once during any such gap period, and at Customer's expense. Dealr will cooperate in good faith. This Section 9.2 does not create any on-site access right.

(f) *Rights not limited.* Nothing in this Section limits examination rights that a governmental authority with supervisory jurisdiction exercises directly under Applicable Law. Likewise, nothing in this Section 9 limits any audit, inspection, or data-sharing-disclosure right that a state dealer-data or DMS statute applicable to Customer's business grants Customer and does not permit to be waived. Sections 9.1–9.2 do not purport to satisfy or waive any such right. MSA §10.4 (state-specific rider) governs such rights, notwithstanding Section 12.2 (order of precedence). Dealr will satisfy such rights in the manner and to the extent that statute requires.

9.3 **Compliance information; cooperation.** Upon Customer's reasonable written request, Dealr will make available to Customer, regardless of plan, information in Dealr's possession reasonably necessary to demonstrate Dealr's compliance with its obligations under this DPA and Applicable Data Protection Law. That information includes Dealr's public security overview, written responses to a reasonable security questionnaire, and written attestations of Dealr's compliance. Upon Customer's reasonable written request, Dealr will also cooperate with reasonable assessments to the extent Applicable Data Protection Law requires. Dealr may satisfy this obligation through the mechanisms in Section 9.1 (primary mechanism) and its published documentation. Any information provided under this Section is Dealr's Confidential Information under MSA §11 (confidentiality).

---

10. Data Return & Deletion

10.1 **During the term.** Customer controls Customer Content through the Services and may export it per MSA §10.3 (export; deletion).

10.2 **After termination.** Following the 60-day post-termination export window, Dealr will delete Personal Data in Customer Content from its active systems within ninety (90) days of termination. On written request, Dealr will provide a certificate of deletion, identifying any categories of Personal Data retained under Section 10.3 (carve-outs) and the applicable retention basis. AI Interaction Records (AI Addendum §3.6 (AI Interaction Records; retention)) are deleted on a rolling basis no later than six (6) months after creation. On termination or account-level deletion, they are deleted no later than the deadline above or the six-month date, whichever is earlier.

10.3 **Carve-outs.** Deletion does not apply to:

(a) data Dealr must retain under Applicable Law, legal hold, or its state-contract, DMV-authorization, and audit obligations (including Schedule B's digital-record retention period), which Dealr will continue to protect under this DPA and delete when the retention obligation ends;

(b) De-identified/Aggregate Data; and

(c) **routine backup and disaster-recovery media, from which Personal Data is purged in the ordinary course of Dealr's backup rotation, currently within approximately six (6) months**. Backup copies are not restored to active use except for disaster recovery, and remain protected under this DPA until purged.

---

11. Data Location; International

11.1 **Data Location.**

(a) *Dealr hosting.* Dealr hosts the production systems that store Personal Data for the Services in data centers and cloud regions located in the United States.

(b) *Subprocessor locations.* Subprocessors may Process Personal Data in the United States and in other countries, under the written terms described in Section 6.1 (authorization; list). Dealr does not require Subprocessors to process Personal Data only in the United States.

(c) *Vendor personnel access.* Vendor personnel may access data from other locations for support and operations under the vendor's contractual safeguards. This does not apply where a Product Schedule, the State Contract, or Applicable Law requires otherwise.

(d) *State Records.* For State Records, Schedule B and Dealr's state contract impose U.S. processing independently. Dealr will send State Records only to Subprocessors that Process them in the United States.

11.2 **International hooks.** The Services are offered to U.S. businesses. If the parties later agree in writing that Dealr will Process personal data subject to the GDPR, UK GDPR, or PIPEDA, the parties will execute the appropriate transfer mechanisms before such Processing begins. Appropriate mechanisms include, for example, EU Standard Contractual Clauses with a UK addendum. No such data is in scope today.

---

12. Liability; Order of Precedence; Term

12.1 Each party's liability under this DPA is subject to MSA §13 (limitation of liability), including the §13.2 general cap and the §13.3 security super-cap. This DPA does not create third-party-beneficiary rights in any consumer or other person.

12.2 For Personal Data Processing and security matters, this DPA prevails over conflicting terms of the Agreement. This does not apply to an Order Form provision that expressly states an intent to vary this DPA; see MSA §1.2 (order of precedence). This DPA is effective as long as Dealr Processes Personal Data under the Agreement, including the post-termination periods in Section 10.

Annex 1 — Processing Details

Item	Description
Subject matter	Provision of the dealr.cloud DMS, dealr.tax, and DTS Registration & Title Services to Customer per the Agreement.
Duration	The Agreement term plus the export, deletion, and retention periods in Section 10.

Item	Description
Nature & purposes	Hosting, storage, transmission, display, analysis, document processing (including OCR/AI-assisted extraction and verification per the AI Addendum), communications facilitation (calls/texts/email per the AUP), payment facilitation (per Schedule B / payments exhibit), transaction auditing and state-system submission (DTS), support, security, and service improvement via De-identified Data.
Categories of data subjects	Customer's consumers (vehicle buyers, sellers, borrowers, service customers, lead contacts); Customer's End Users and personnel; guarantors and co-signers.
Categories of Personal Data	Identity and contact data; government identifiers (driver's license, SSN where required for title/finance/KYC flows); vehicle and transaction data (VINs, titles, registrations, deal terms); financial data (bank statements, credit-application data, payment records, loan performance); communications content and metadata (calls, texts, emails, recordings and transcripts where enabled); usage data.
Sensitive data	SSNs, driver's license numbers, financial account data; occasional disability-related documents in title flows (handled as sensitive personal information with heightened access controls; no HIPAA/BAA framing — Dealr is not a covered entity or business associate).
Subprocessors	Per the Subprocessor List at the Policy Center (all vendor categories listed there, including cloud hosting, AI/document processing, e-signature, communications, and analytics/operations).

Annex 2 — Security Exhibit

Dealr maintains, at minimum, the following controls (the "**Security Program**"), audited annually under SOC 2 Type II (Security, Availability, Confidentiality) covering dealr.cloud, dealr.tax, and DTS:

1. **Governance.** A written information-security program with a designated senior owner ("Qualified Individual" for Safeguards Rule purposes); risk assessments performed and refreshed periodically; policies reviewed at least annually; security training for all personnel at hire and periodically thereafter; background screening of personnel consistent with law and, for DTS-related roles, with Dealr's state-contract obligations.
2. **Asset inventory.** Dealr maintains and periodically reviews an inventory of the systems, devices, and infrastructure that store or process Customer Personal Data, with assigned ownership for inventoried assets.
3. **Access control.** Role-based access on least-privilege principles; unique accounts; multi-factor authentication for personnel access to systems Processing Personal Data; timely deprovisioning on role change or departure; periodic access reviews; credential-management standards including rotation requirements. The Services also require multi-factor authentication for every Customer End User sign-in; it cannot be turned off.
4. **Encryption.** Personal Data encrypted in transit (TLS 1.2+) and at rest using industry-standard algorithms; key management with restricted access.
5. **Network & infrastructure.** Segmented environments; firewalls and security groups; hardening baselines; vulnerability management with risk-based remediation timelines; penetration testing and/or continuous vulnerability scanning consistent with the SOC 2 program; anti-malware/endpoint protection on managed endpoints.
6. **Secure development.** Separation of production and non-production environments; no production Personal Data in non-production environments except under equivalent controls; code review and security testing practices consistent with the SOC 2 program.

7. **Change management and patching.** Dealr maintains documented change-management procedures requiring review and approval before production deployment, applies security patches to supported systems in a timely manner, and performs vulnerability scanning at least monthly.
8. **Logging & monitoring.** Centralized logging of security-relevant events for systems Processing Personal Data; monitoring and alerting; log protection and retention consistent with the SOC 2 program.
9. **Incident response.** A written incident-response plan with defined roles, escalation, containment, eradication, recovery, and post-incident review, including the customer-notification track supporting Section 8 (security incidents) and (for DTS) the immediate State-notification lane; plan tested periodically.
10. **Availability & resilience.** Redundant infrastructure across availability zones; documented backup procedures with periodic restoration testing; disaster-recovery plan; backup media protected with encryption and purged per Section 10.3(c) (backup media).
11. **Physical security.** Production systems hosted in U.S. regions of SOC 2/ISO 27001-audited cloud data centers operated by the cloud infrastructure providers on the Subprocessor List; Dealr office controls for any physical documents per Schedule B's handling and micro-cut destruction standards.
12. **Vendor management.** Subprocessor due diligence before engagement; written data-protection terms per Section 6.1 (subprocessor authorization; list); periodic review of Subprocessor attestations; the standing rule that no AI vendor Processes Personal Data without a commitment not to train AI models on Customer Content (written terms or a documented, configuration-enforced no-training setting; de-identified use to improve the vendor's own service is permitted per AI Addendum §3.1(a)), limited-retention terms, contractual confidentiality and data-protection terms (which may be the vendor's standard commercial terms), and Subprocessor List placement (per AI Addendum §3.5); a vendor's training of a Dealr-scoped model at Dealr's direction is Dealr's own disclosed service-limited use under AI Addendum §§3.1(b) and 3.3(b), and the vendor's no-training commitment must still cover the vendor's own and third-party models.
13. **Data minimization & disposal.** Retention per the Agreement and published retention schedules; secure deletion/destruction of Personal Data and media (including NIST 800-88-consistent sanitization and micro-cut shredding of physical documents).

Annex 3 — U.S. State Privacy Law Schedule

1. **Covered laws.** This Annex applies where a U.S. state consumer-privacy law applies to Personal Data Processed under the Agreement and is not displaced by a GLBA data- or entity-level exemption. Covered laws include the California Consumer Privacy Act as amended by the CPRA, the Colorado Privacy Act, and the comparable laws of other states, together with their regulations.
2. **Service-provider/processor terms.** Dealr is Customer's "service provider"/"processor." Sections 3.1–3.2 (purpose limitation, no sale/share, no out-of-relationship retention or combination), 4 (confidentiality), 5 (security), 6 (subprocessor flow-down), 7 (request assistance), 9 (audit; and the Section 9.3 compliance-information covenant), and 10 (deletion/return) implement the contract requirements of those laws. Those requirements include Cal. Civ. Code §1798.100(d)/§1798.140(ag) and C.R.S. §6-1-1305(5).
3. **Compliance certification; same protection; notice of non-compliance.** Dealr will comply with obligations applicable to service providers/processors under covered laws, will provide the same level of privacy protection for Personal Data as covered laws require of Customer, certifies

that it understands and will comply with the Section 3.2 restrictions, and will notify Customer if it determines it can no longer meet them. Upon notice from Customer of unauthorized use of Personal Data, or upon Dealr's notice under this paragraph, Customer may take the reasonable and appropriate steps covered laws authorize, including directing Dealr to stop the affected Processing, and Dealr will remediate the unauthorized use.

4. **De-identified data.** Dealr will maintain and use De-identified Data only in de-identified form, will not attempt re-identification (except to test de-identification effectiveness), and will contractually require the same of recipients. Dealr takes reasonable measures to ensure De-identified Data cannot be associated with a natural person or household. Dealr publicly commits, including in its published privacy policy, to maintain and use De-identified Data only in de-identified form and not to attempt re-identification.

Annex 4 — GLBA / FTC Safeguards Rule Annex

1. **Status.** Customer may be a "financial institution" under the Safeguards Rule (16 C.F.R. Part 314) because it extends or arranges vehicle financing. For such Customers, Dealr acts as a service provider with access to "customer information" (as defined in §314.2). This Annex plus the Security Exhibit constitute the contractual safeguards §314.4(f)(2) requires Customer to obtain.
2. **Safeguards.** Dealr will: (a) implement and maintain the Security Program in Annex 2, designed to protect customer information consistent with the elements of §314.4; (b) encrypt customer information in transit and at rest (§314.4(c)(3)); (c) enforce MFA for Dealr personnel access to systems containing customer information, per Annex 2 item 3 (§314.4(c)(5) as applied to Dealr's systems; End-User MFA is also required for every End User sign-in on the platform, as Annex 2 item 3 describes); (d) maintain audit logging and monitoring (§314.4(c)(8)); and (e) maintain a written incident-response plan (§314.4(h)).
3. **Oversight.** Dealr supports Customer's periodic-assessment duty under §314.4(f)(3) through the audit mechanisms in Section 9 (audits): (i) the SOC 3 report, security overview, and questionnaire responses for all Customers (§9.1(a)); (ii) the SOC 2 Type II report on qualifying plans (§9.1(b)); (iii) the §9.1(c) written-certification override, under which any Customer that certifies a legal or regulatory assessment need receives the SOC 2 Type II report; and (iv) the Section 9.3 compliance information for all Customers. The §9.1(c) override exists precisely for a §314.4(f)(3) assessment obligation.
4. **Breach support.** Dealr's Section 8 (security incidents) notice (72 hours from awareness) is designed to give Customer adequate runway for its own notification obligation under §314.4(j) and applicable state breach laws. The §314.4(j) obligation is notice to the FTC within 30 days for incidents involving 500+ consumers' unencrypted information (or encrypted information where the encryption key was also compromised). Dealr will provide the incident details reasonably needed for those filings.
5. **NPI handling.** Dealr will not use or disclose nonpublic personal information received from or on behalf of Customer except to provide the Services, as permitted by the service-provider exception in GLBA §502(b)(2) and the exceptions in §502(e) (15 U.S.C. §6802(b)(2), (e)), or as Applicable Law requires, and will comply with the limits on redisclosure and reuse in 16 C.F.R. §313.11 applicable to recipients of nonpublic personal information — consistent with Sections 3.1–3.2 (instructions; prohibitions).
6. **Customer-directed disclosures.** This Annex covers Dealr's Processing. Customer information disclosed through Customer-directed transmissions or AI Client Connections (MSA §10.2(a), (d)) leaves Dealr's Processing when delivered. The recipient, including the provider of a connected AI

application, is Customer's own service provider for §314.4(f) purposes, which Customer selects, contracts with, and oversees.

7. **Safeguards summary.** Dealr publishes a *Safeguards Rule Compliance Summary for Customers* mapping its SOC 2 controls to §314.4 elements, available at the Policy Center.