Dealertrack Information Security Controls – Lender Products

Information Security Program Maintenance

- Dealertrack will maintain an information security program consistent with industry standards and will maintain a SOC 2 Type 2 (SSAE 18) report or equivalent for the duration of this Agreement. If applicable, the report will be made available to Lender upon request.

- The production and disaster recovery environments used by Dealertrack to provide services to Lender will be hosted in a SSAE 18 SOC 2 compliant data center for the duration of this Agreement. If applicable, the report will be made available to Lender upon request.

Personnel Security

- Dealertrack will maintain policies and procedures designed to subject all employees, subcontractors' employees, and temporary staff that have access to Lender Customer Information to appropriate background checks at time of most recent hire date.

- The criminal background checks currently conducted with respect to individuals located in the U.S.A. include the current and past places of residence of Dealertrack's personnel for the previous seven (7) years.

- The background checks for individuals located outside of the U.S.A will be reasonable in scope and subject to applicable law and custom.

- Upon request, Dealertrack will provide Lender with an executive summary of the then current background check procedures.

- Subject to applicable law, Dealertrack will not assign any personnel to perform services under this Agreement if the background check reveals a criminal conviction or pretrial diversion for crimes involving fraud, financial dishonesty, breach of trust, or theft.

- Dealertrack will only provide its employees and subcontractors with levels of access required to fulfill their job duties.

- Dealertrack will maintain Confidentiality or Non-Disclosure Agreements with its employees and contractors for the protection of confidential information, including Lender's Confidential Information.

Security Training

- Dealertrack will maintain a new hire and annual security awareness training program for all employees and subcontractors with access to Lender Customer Information. Upon request, during Lender's audits conducted in accordance with this Agreement, Dealertrack will allow Lender to review Dealertrack's security awareness training materials.

Subcontractors

- Dealertrack will maintain a due diligence program to monitor and manage subcontractors.
- If Dealertrack uses Material Subcontractors under this Agreement, Dealertrack will have appropriate controls in place designed to ensure that such Material Subcontractors meet the objectives of this Schedule, and will exercise reasonable oversight over them for the purpose of monitoring their compliance with this Agreement.

Application Security

- Dealertrack will assign individual accounts to users of systems that access, transmit or store Lender's Confidential Information to provide accountability.
- Dealertrack will follow formal processes to approve and track system access that is granted. Dealertrack will follow similar formal processes for the removal of access upon separation, or reassignment of job responsibilities.
- Dealertrack will periodically review employee access to verify appropriate access assignments.
- Dealertrack will use a granular role based permission system. This provides a detailed level of access controls built upon the principles of "least privilege" and "need to know." Roles allow the lender administrator to manage user permissions based on a particular user's role.
- Dealertrack will maintain appropriate password parameters for systems that access, transmit or store Lender's Confidential Information. These password parameters will include at a minimum:
    a. Password length must be at least 8 characters.
    b. Password must have at least 1 alpha character and 1 numeric character.

c. Password history of 5 must be enforced.

d. Password cannot be the same as the user's Login ID.

e. Password must be case-sensitive.

f. Password must expire every 90 days.

g. Users must be locked out after no more than 5 incorrect attempts.

- To safeguard user passwords, all client-server communication is exchanged via the TLS encrypted protocol and all passwords subsequently stored are encrypted with a strong hashing algorithm in the database.
- Dealertrack will maintain data-masking technology to protect Nonpublic Personal Information from inappropriate or unauthorized disclosure.
- Dealertrack will implement data at rest encryption technology of select sensitive data elements within the database.
- Dealertrack will maintain a vulnerability assessment program and perform application security assessments on an annual (or more frequent) basis. Dealertrack will review and remediate material vulnerabilities that are discovered.
- Dealertrack's website will maintain https/TLS 128-bit encryption to secure confidential information as it traverses public networks.

Audit Logs

- Dealertrack will maintain and archive website audit logs that monitor and record information from the Dealertrack production systems for a minimum period of 1 year. The audit logs will include information to identify the user, the date-time stamp of activity, the source IP address of the user and summary of activity performed.

Physical & Environmental Security

- Dealertrack will implement physical security policies and procedures, systems, technology and staff, including access control mechanisms designed to prevent unauthorized access to Dealertrack facilities hosting or processing Lender's Confidential Information.

The Data Center physical and environmental controls will include:

a. Security cameras (which are monitored on a 24x7 basis within the facilities that are hosting or processing lender information) and applicable video retention.

b. Physical access control system that monitors points of ingress and egress for each data center, notifying appropriate security operations personnel of any alarms generated by the system.

c. Physical access mechanisms (e.g., access cards, biometric devices, mantraps, and portals) which are administered by local operations staff so that only authorized individuals have the ability to access the data center.

d. Backup power supply system designed to guard against electrical outages and provide for ongoing power support for systems that require such service based on recovery plans.

e. Fire detection and suppression system(s) designed to protect Dealertrack's computing equipment and Lender materials entrusted to our care, if applicable (e.g. title documents, contracts, etc.); and monitoring thereof.

f. Facility built to effectively withstand natural disasters (e.g., fire, flood, earthquakes) and with zoned temperature control systems and multiple HVAC units to verify correct temperatures in critical areas.

g. Security systems with dedicated 24x7 uninterruptible power supply (UPS) systems and standby emergency power support (i.e., generators).

h. Maintenance procedures that are performed periodically to test and validate the operation of all power management systems, fire detection and suppression systems, HVAC systems as well as humidity, temperature and water detection sensors.

Infrastructure & Network Controls

- Dealertrack will maintain system hardening procedures to restrict services on devices and servers to only those services needed for the system or device to function.

- Dealertrack will maintain appropriate network perimeter controls such as firewalls at all perimeter connections and Intrusion Detection Systems. Intrusion Detection System and firewall traffic will be monitored for abnormal behavior. Storage of Lender Information will be secured behind multi-tiered firewalls.

- Dealertrack will implement critical security–related software patches on a timely basis.

- Dealertrack will maintain an anti-virus solution to protect its servers and workstations against viruses, worms, Trojan horses and other forms of malware that may cause damage. Dealertrack will install and maintain malware detection software, to include virus detection and malware detectors, on systems used to access, process or store Lender information. In addition, definition files will be updated regularly.

- Dealertrack will perform external and internal network vulnerability assessments on an annual (or more frequent) basis to test for security vulnerabilities. Dealertrack will review and remediate material vulnerabilities that are discovered.

- Dealertrack will utilize a data loss prevention tool to monitor and/or prevent sensitive and personal data from being transmitted outside the organization.

Change Management

- Dealertrack production systems will follow a formal and documented change control process that provides for distinct roles and segregation of duties.

- Dealertrack will maintain physically and logically segregated distinct environments for Production, Disaster Recovery and pre-Production environments.
- Dealertrack's environment will have changes executed within documented maintenance windows, and only after obtaining appropriate authorizations from technical and business approvers to maintain the segregation of duties principle.

- Dealertrack will utilize code management software for its developers to develop code and maintain version control.

- Dealertrack will maintain software to monitor and audit the change control process so that unauthorized code changes are not promoted to the production environment.

Business Continuity & Disaster Recovery

- Dealertrack will maintain a documented Business Continuity and Disaster Recovery plans for the duration of this Agreement. The Business Continuity plan will include a periodic business impact analysis; procedures for the identified contingencies; and documented testing of the plan. The Disaster Recovery plan will include all locations hosting the systems providing services as per this Agreement. At a minimum, the plan will be updated annually and testing of the plan will be documented and shared with Lender upon request.

Incident Response and Management

- Dealertrack will maintain an Incident Response plan that will be updated at least annually and will document at a minimum, procedures and response actions; responsibilities of personnel; and identify relevant notification procedures and timelines.

Compliance & Right to Audit

- Dealertrack will perform periodic internal control testing to test the effectiveness of security controls and verify that it is in compliance with the requirements set forth in this Exhibit and all applicable regulatory, legal and contractual requirements.

- Lender will have the right to audit Dealertrack as specified in this Agreement.