

Service Provider Risk Assessment

Questionnaire requested by **FIELDS BMW, BMW of Asheville, FIELDS BMW - NORTH FIELD, FIELDS CADILLAC OF ORANGE PARK, FIELDS CADILLAC, LLC, FIELDS CHRYSLER JEEP DODGE, FIELDS COLLISION CENTER JACKSONVILLE, FIELDS LAND ROVER VOLVO JAGUAR, FIELDS LAND ROVER WINNETKA, FIELDS LANDROVER, FIELDS LEXUS GLENVIEW, FIELDS MOTORCARS ASHEVILLE, FIELDS MOTORWORKS, FIELDS OPR, INC.DBA MERCEDES-BENZ OF ORLAND PARK, FIELDS VOLVO OF HIGHLAND PARK, JAGUAR LANDROVER MADISON, LAND ROVER ASHEVILLE.**

Name of Person Completing This Questionnaire	Service Provider Name	Date Completed
Norm Crawford	Text2Drive, LLC	6-8-2023

1. Are you an employee or authorized representative of this vendor/company? Indicate the Person's Name in the comments. Yes Person's Name: Norm Crawford

2. Does your company offer software applications as part of its services? Yes

3. Is client data encrypted at rest and in transit? If not, why not? Yes

4. Has your company experienced a data breach in the past 12 months that affected customers' personal information? No

5. Does your company have insurance coverage for a data breach that may involve our customer information that your company acquires while doing business with us? Yes

6. Does your company require security awareness training for all employees? If so, please answer how often it is provided in the comments section. Yes Security Training Frequency: Annual training + quarterly simulated tests on our own employees with mandatory re-training or disciplinary action on any failures.

7. Does your company monitor for the effectiveness of employee security training by testing your users with simulated attacks? Yes

8. Does your company have a process for restricting access to customer files on a need-to-know basis? Yes

9. Do you have a written information security program? Yes

10. Does your company conduct annual risk assessments that assess electronic, physical, and administrative information safeguards? Yes

11. Does your company have systems in place to securely dispose of documents that have personal identifiable information on them? Yes

12. Does your company have systems in place to restrict access to files/documents containing customers personal Yes

information to those with proper authorization?

13. Does your company have due diligence processes and procedures for vetting subcontractors, including having them sign processing agreements that are compliant with applicable federal and state laws?	Yes
14. Has your company performed penetration testing of its systems within the past 12 months?	Yes
15. Has your company conducted a vulnerability assessment of your systems within the past 6 months?	Yes
16. Does your company maintain end-of-life or unsupported operating systems or software? If so, are these systems used to manage or maintain customer data?	No
17. Does your company regularly patch or update systems and third-party software and monitor for noncompliance?	Yes
18. Does your company have a written incident response plan in the event of a security breach?	Yes
19. Does your company require users to create complex passwords with 9 characters or greater?	No MFA is mandatory. Complex password requirements are enforced from our Information Security policies.
20. Does your company prohibit shared logins?	Yes
21. Does your company require multi-factor authentication to log into your systems?	Yes
22. Do you have an account lockout policy?	No Account logins are monitored within our database, suspicious activity is addressed manually so as not to falsely lock out dealership users while they are helping customers.

Date	Signature of Authorized Agent of Service Provider	Title
6-8-2023	Norm Crawford	COO

Submitted on June 8, 2023 at 4:47 PM by 65.29.160.93.