



Service Provider Risk Assessment

Questionnaire requested by FIELD'S AUTO GROUP

Name of Person Completing This Questionnaire	Service Provider Name	Date Completed
1. Are you an employee or authorized representative of this vendor/company? Indicate the Person's Name in the comments.	Yes No N/A	Person's Name: Brian Sizemore
2. Does your company offer software applications as part of its services?	Yes No N/A	
3. Is client data encrypted at rest and in transit? If not, why not?	Yes No N/A	
4. Has your company experienced a data breach in the past 12 months that affected customers' personal information?	Yes No N/A	
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 No N/A	
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 No N/A	Security Training Frequency: Annually
7. Does your company monitor for the effectiveness of employee security training by testing your users with simulated attacks?	Yes No N/A	
8. Does your company have a process for restricting access to customer files on a need-to-know basis?	Yes No N/A	
9. Do you have a written information security program?	Yes No N/A	
10. Does your company conduct annual risk assessments that assess electronic, physical, and administrative information safeguards?	Yes No N/A	
11. Does your company have systems in place to securely dispose of documents that have personal identifiable information on them?	Yes No N/A	



12. Does your company have systems in place to restrict access to files/documents containing customers personal information to those with proper authorization?	Yes No N/A	
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 No N/A	
14. Has your company performed penetration testing of its systems within the past 12 months?	Yes No N/A	
15. Has your company conducted a vulnerability assessment of your systems within the past 6 months?	Yes No N/A	
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?	Yes No N/A	We have a small number of end-of-life systems that have enhanced monitoring and networking restrictions. These systems are used to process various data related to the iPacket product, but they do not manage or maintain PII.
17. Does your company regularly patch or update systems and third-party software and monitor for noncompliance?	Yes No N/A	
18. Does your company have a written incident response plan in the event of a security breach?	Yes No N/A	
19. Does your company require users to create complex passwords with 9 characters or greater?	Yes No N/A	
20. Does your company prohibit shared logins?	Yes No N/A	
20. Does your company prohibit shared logins?	Yes No N/A	
22. Do you have an account lockout policy?	Yes No N/A	We utilize Google Workspace's built-in suspicious activity detections to block malicious sign in attempts and to disable accounts when suspicious activity has been detected.

08 - 07 - 25 Brian Sizemore
Security Team Lead

iPacket



August 7, 2025

A handwritten signature in black ink, appearing to be "R. J. Smith".

Security Team Lead

Date

Signature of Authorized Agent of Service Provider

Title