Sample Risk Assessment Questionnaire for Service Providers

***Physical and Administrative Questions***

1. Does your company have a written information security program?

⭘Yes ⭘No ⭘N/A

2. Does your company perform physical, administrative, and electronic risk assessments relating to information safeguards at least annually?

⭘Yes ⭘No ⭘N/A

3. Does your company perform training on security awareness for all employees at least annually?

⭘Yes ⭘No ⭘N/A

4. Does your company have a cybersecurity insurance policy that covers data breaches affecting customer personal information that you collect, receive, store, or process on our behalf?

⭘Yes ⭘No ⭘N/A

5. Does your company have a process and/or policy that limits the ability to request and access files (whether stored physically or electronically) containing customer information to only authorized individuals with a need-to-know basis?

⭘Yes ⭘No ⭘N/A

6. Does your company provide a mechanism for the secure destruction and disposal of documents containing personal information, such as locked shredding bins?

⭘Yes ⭘No ⭘N/A

7. Does your company ask that each of your service providers and sub-processors sign a data processing agreement that complies with applicable state and federal data privacy laws?

⭘Yes ⭘No ⭘N/A

8. Does your company use and share only fictitious or test data (not real customer information) for training, development, or testing purposes?

⭘Yes ⭘No ⭘N/A

9. Has your company experienced a data breach affecting consumer personal information in the past 12 months?

⭘Yes ⭘No ⭘N/A

***Electronic & Technical Questions***

1. Does your company conduct social engineering and phishing simulations?

⭘Yes ⭘No ⭘N/A

2. If your company offers a software or application as part of its services, does it support multi-factor authentication, such as SMS or email tokens?

⭘Yes ⭘No ⭘N/A

3. Has your company performed a full penetration test in the last 12 months?

⭘Yes ⭘No ⭘N/A

4. Does your company regularly run internal and external vulnerability scans or have a system for continuous monitoring of threats?

⭘Yes ⭘No ⭘N/A

5. Does your company store network user credentials securely by ensuring such credentials are not stored in plain, readable text or in a vulnerable format?

⭘Yes ⭘No ⭘N/A

6. Does your company restrict access to sensitive data stored in files and on your network and ensure that only authorized employees with a business need have access to personal information?

⭘Yes ⭘No ⭘N/A

7. If your company offers a software or application as part of its services, does it require the use of complex and unique passwords (alpha-numeric and non-dictionary words) for all systems containing personal information?

⭘Yes ⭘No ⭘N/A

8. If your company offers a software or application as part of its services, does it protect against brute-force attacks by suspending or disabling user credentials after a certain number of unsuccessful login attempts?

⭘Yes ⭘No ⭘N/A

9. If your company offers a software or application as part of its services, does it use properly configured and industry-tested methods of encryption to keep sensitive information secure in transit and at rest?

⭘Yes ⭘No ⭘N/A

10. If your company offers a software or application as part of its services, do you (1) employ engineers trained in secure coding, (2) test for common vulnerabilities, (3) follow platform and OS guidelines for security, and (4) verify that privacy and security features work as intended?

⭘Yes ⭘No ⭘N/A

11. Does your company regularly update and patch third-party software (e.g., antivirus, firewalls) and test your network to ensure that such updates and patches have been successfully installed on all applicable devices?

⭘Yes ⭘No ⭘N/A