TermTrax

Software Review Report

Stripe

Generated: 2026-08-10T18:48:15.413Z
Schema Version: 1.2.0

Table of Contents

Review Summary

Review ID: d1et2aysv81tsw4iokl8gowj
Status: ANALYSIS
Decision: Pending
Created At: 2026-07-11T19:20:16.518Z
Submitted At: Not submitted
Submitted By: N/A
Analysis Completed At: 2026-07-12T15:33:08.860Z
General Notes: None
Usage Conditions: None
AI Jurisdiction: Conditional: California (State of California, USA) for US-based Stripe Account holders; Ireland for EEA users; England and Wales for UK/Switzerland/Gibraltar users. Definitive jurisdiction requires confirmation of User's Stripe Account Country, which is not specified in the intake brief. No tenant default jurisdiction was provided. Human input required to finalize.
Human Jurisdiction: N/A

Intake Form

Purpose: process payments for purchasing our product
Risk Concerns: None
Review Priorities: None

Playbook Items

Name	Category	Weight	AI Color	Human Color
Termination for Convenience	Termination	ACCEPTABLE_TO_DEVIATE	At Risk	Unaddressed
License Grant – Vendor to Our Company	License Grant	HIGH	Needs Review	Unaddressed
Security Certifications	Governance & Risk Transfer	HIGH	Aligned	Unaddressed
Data Protection Officer (DPO)	Governance & Risk Transfer	MEDIUM	Aligned	Unaddressed
Audit Logging	Security Operations	HIGH	Aligned	Unaddressed
Subprocessor Change Notification	Subprocessors	HIGH	Needs Review	Unaddressed
Data Processing Security Policies	Security Operations	HIGH	Aligned	Unaddressed

Name	Category	Weight	AI Color	Human Color
Compliance with Referenced Laws	Legal & Compliance	HIGH	Needs Review	Unaddressed
License Grant to Data – Our Company to Vendor	License Grant	CRITICAL	Aligned	Unaddressed
Our liability	Limitation of Liability	ACCEPTABLE_TO_DEVIATE	Needs Review	Unaddressed
Termination Obligations	Termination	MEDIUM	Needs Review	Unaddressed
Employee Access Control	Access & Personnel	HIGH	Aligned	Unaddressed
Confidentiality	Confidentiality	HIGH	Aligned	Unaddressed
Warranty & Remedy	Commercial Terms	ACCEPTABLE_TO_DEVIATE	At Risk	Unaddressed
Non-Solicitation of Employees	Operations	MEDIUM	Aligned	Unaddressed
Subprocessor Agreements	Subprocessors	CRITICAL	Needs Review	Unaddressed
Assignment	Legal & Compliance	ACCEPTABLE_TO_DEVIATE	Needs Review	Unaddressed
Vendor Audit Rights	Governance & Risk Transfer	HIGH	Needs Review	Unaddressed
Publicity	Publicity	HIGH	At Risk	Unaddressed
Password Encryption	Encryption	HIGH	Aligned	Unaddressed
Employee Offboarding Access	Access & Personnel	HIGH	Needs Review	Unaddressed
Physical Security Controls	Security Operations	HIGH	Aligned	Unaddressed
Exclusivity	Operations	HIGH	Aligned	Unaddressed
Payment Terms	Commercial Terms	HIGH	Needs Review	Unaddressed
Data Retention & Deletion	Data Handling	HIGH	Needs Review	Unaddressed
Employee Confidentiality Agreements	Access & Personnel	HIGH	Needs Review	Unaddressed
Governing Law	Legal & Compliance	ACCEPTABLE_TO_DEVIATE	Needs Review	Unaddressed
User Authentication Policies	Security Operations	HIGH	Aligned	Unaddressed
Modification of Terms	Legal & Compliance	HIGH	Needs Review	Unaddressed
Insurance	Commercial Terms	ACCEPTABLE_TO_DEVIATE	Needs Review	Unaddressed
Disaster Recovery Testing	Business Continuity	HIGH	Needs Review	Unaddressed
Termination for Cause	Termination	ACCEPTABLE_TO_DEVIATE	Aligned	Unaddressed
Cyber Risk Insurance	Governance & Risk Transfer	MEDIUM	Needs Review	Unaddressed
Processing Location Restrictions	Data Handling	HIGH	Needs Review	Unaddressed
Encryption at Rest	Encryption	HIGH	Aligned	Unaddressed
Encryption in Transit	Encryption	HIGH	Aligned	Unaddressed
No AI/ML Training on Our Data	Data Handling	CRITICAL	At Risk	Unaddressed
Data Ownership	Data Handling	CRITICAL	At Risk	Unaddressed
Authorized Equipment & Software	Access & Personnel	HIGH	Needs Review	Unaddressed
Anti-Virus Solution	Security Operations	HIGH	Needs Review	Unaddressed
Restrictions on Use	Operations	HIGH	Aligned	Unaddressed
Data Subject Rights Assistance	Governance & Risk Transfer	HIGH	Aligned	Unaddressed

Name	Category	Weight	AI Color	Human Color
Breach Notification Timeline	Breach & Incident Response	CRITICAL	Needs Review	Unaddressed
Retention of Our Rights to Our Property	Intellectual Property	CRITICAL	Needs Review	Unaddressed
Regulatory Disclosure Procedure	Breach & Incident Response	HIGH	Needs Review	Unaddressed
Data Segregation	Data Handling	HIGH	Needs Review	Unaddressed
Vendor's liability	Limitation of Liability	HIGH	Needs Review	Unaddressed
Indemnification – Our Company to Vendor	Indemnification	MEDIUM	Needs Review	Unaddressed
Automatic Renewal	Commercial Terms	ACCEPTABLE_TO_DEVIATE	Needs Review	Unaddressed
Security Training	Access & Personnel	MEDIUM	Aligned	Unaddressed
Compliance Monitoring	Governance & Risk Transfer	HIGH	Needs Review	Unaddressed
Indemnification – Vendor to Our Company	Indemnification	MEDIUM	Needs Review	Unaddressed
Ownership of Custom Deliverables	Intellectual Property	HIGH	At Risk	Unaddressed
Processing Limitation	Data Handling	CRITICAL	Needs Review	Unaddressed
Data Backup & Restoration	Business Continuity	HIGH	Needs Review	Unaddressed
Breach Indemnification	Governance & Risk Transfer	HIGH	Needs Review	Unaddressed
Arbitration or other dispute resolution process	Legal & Compliance	MEDIUM	At Risk	Unaddressed
Subprocessor Audit Rights	Subprocessors	MEDIUM	Needs Review	Unaddressed
Cybersecurity Prevention Systems	Security Operations	HIGH	Aligned	Unaddressed

Termination for Convenience

AI Comment: The acceptable position has three components: (1) User may terminate for convenience; (2) Stripe (vendor) may NOT terminate for convenience; and (3) upon any termination for convenience, User is entitled to a pro-rata refund of prepaid but unused fees.

Component 1 is satisfied. Section 10.1(a)(i) allows User to terminate at any time by closing the Stripe Account — unrestricted and unambiguous.

Component 2 fails. Section 10.1(b)(ii)(1) grants Stripe an unrestricted right to terminate for convenience at any time, subject only to notification "in accordance with Law" — which imposes no specific minimum notice period in the General Terms. This directly contradicts the requirement that the vendor cannot terminate for convenience. For Australian users (Regional Terms §13.6) and New Zealand users (Regional Terms §13.7), these regional provisions expressly replace §10.1(b)(ii)(1) and require 30 days' advance notice before Stripe exercises this right, providing a partial mitigation. However, Stripe's fundamental right to terminate for convenience survives in both jurisdictions — only the notice requirement is added. No other regional terms modify this right.

Component 3 fails. Section 7.1(b) expressly states that "payment obligations are non-cancelable and Fees paid are non-refundable" absent written agreement or legal requirement. No carve-out for termination events appears anywhere in the Agreement. Section 10.2 further reinforces this, confirming that termination does not relieve User of any payment obligations accrued prior to the effective date. There is no pro-rata refund mechanism anywhere in the document set.

Because two of three components of the acceptable position are actively contradicted by the contract — not merely absent — the overall classification is RED. Given the weight of "Acceptable to Deviate," this finding is noted for comment but does not constitute a blocking issue. The most significant practical exposure is Stripe's ability to close the account at will without any notice obligation under the General Terms (e.g., for US-based users), which could disrupt payment processing for User's products with no compensation available for prepaid fees.

— Superseding reasoning —
For Australian users, Regional Terms §13.6 expressly replaces General Terms §10.1(b)(ii)(1), adding a mandatory 30-day advance notice requirement before Stripe may exercise its termination-for-convenience right. For New Zealand users, Regional Terms §13.7 imposes the identical modification. Pursuant to General Terms §13 ("If there is a conflict between the General Terms and the Regional Terms, the Regional Terms prevail"), these jurisdiction-specific provisions supersede the general provision in their respective jurisdictions. The modification is partial: Stripe's underlying termination-for-convenience

right is preserved; only the notice requirement changes. This does not alter the overall RED determination, as the acceptable position requires Stripe to have no termination-for-convenience right at all.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Unless otherwise agreed in writing, Stripe may terminate this Agreement or close User's Stripe Account at any time. Stripe will notify User in accordance with Law."
2. "Unless otherwise agreed in writing, Stripe may terminate this Agreement or close User's Stripe Account at any time upon 30 days' notice to User. Stripe will notify User in accordance with Law."
3. "Unless otherwise agreed in writing, Stripe may terminate this Agreement or close User's Stripe Account at any time upon 30 days' notice to User. Stripe will notify User in accordance with Law."

> *"**

> *(a) _Termination by User._*

> *(i) _Termination for Convenience._ User may terminate this Agreement at any time by closing its Stripe Account via the Stripe Dashboard.*

> *"*
> — Stripe Services Agreement - General Terms
> *"Unless User and Stripe otherwise agree in writing or if Law requires, payment obligations are non-cancelable and Fees paid are non-refundable.*

> *"*
> — Stripe Services Agreement - General Terms
> *"In no event will termination relieve User of its obligation to pay any amounts payable to Stripe for the period prior to the effective date of termination. "*
> — Stripe Services Agreement - General Terms

License Grant – Vendor to Our Company

AI Comment: The Stripe Services Agreement (§2.1) grants User a worldwide, royalty-free, non-exclusive license to use Stripe Technology solely for User's Business Purposes during the Term. The defined term "Business Purpose" is broad — it encompasses all commercial operational activities and objectives, which clearly includes payment processing for purchasing User's products (the stated intake purpose). The **intended use** requirement is therefore satisfied.

Direct user coverage is also effectively met: the license runs to "User" (the contracting entity), and authorized representatives and employees who access Stripe Technology on User's behalf operate within the scope of the User grant — consistent with standard enterprise SaaS interpretation.

Affiliate coverage is the critical gap. The §2.1 license is explicitly "non-sublicensable," and §2.5 directly prohibits User from sublicensing, sharing, or redistributing Stripe Technology to any third party — including affiliates — without Stripe's prior written authorization. The Agreement's "User Group" and "User Entity" framework confirms that affiliates are treated as separate entities that must enter their own independent agreements with Stripe. There is no automatic affiliate extension under the User license. This directly conflicts with the playbook requirement that the license scope cover affiliates.

Additional vulnerabilities: the license is explicitly "revocable" (allowing Stripe to withdraw it, subject to the Agreement's termination provisions) and "non-transferable" (assignment requires Stripe's prior consent except in qualifying M&A events under §11.10). These are standard SaaS terms but represent structural constraints.

The absence of affiliate coverage does not completely defeat the payment-processing purpose for the contracting entity itself. However, it constitutes a material gap against the playbook's three-element requirement (intended use + users + affiliates). For a High weight item, documented justification is required if any affiliate entities of User also need to process payments via Stripe — each would require a separate Stripe agreement.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Subject to this Agreement, Stripe (or its Affiliates, as applicable) grants User a limited, worldwide, royalty-free, non-exclusive, non-transferable (except as allowed under Section 11.10 (Assignment)…"
2. ""Business Purpose" means the operational activities, functions, or objectives of User, including, but not limited to, activities relevant to carrying out its organizational, commercial, non-profit, or…"

> *"User must not rent, lease, lend, sell, share, redistribute, or sublicense the Stripe Technology, or enable others to do so, in each case unless expressly permitted under this Agreement or otherwise authorized by Stripe in writing."*
> — Stripe Services Agreement - General Terms

Security Certifications

AI Comment: The DPA Data Security Exhibit explicitly references SOC reports, stating: "SOC 1 and 2 reports are produced annually and will be provided upon request." This substantially meets the acceptable position, which requires a current SOC 2 Type II report or ISO 27001 certification available on request.

What the contract satisfies:
- SOC 2 reports are explicitly referenced and committed to. '
- Reports are produced on an annual cadence. '
- Reports are provided upon request. '
- PCI Level 1 certification is separately confirmed (annual QSA review), evidencing a high-bar external audit posture beyond the playbook's threshold.
- A security questionnaire process is also available annually upon written request, providing an additional transparency mechanism.

Residual gap — Type II vs. Type I:
The contract does not explicitly state "Type II." It refers only to "SOC 1 and 2 reports…produced annually." SOC 2 Type II is an ongoing effectiveness assessment over a defined period (typically 6–12 months); SOC 2 Type I is a point-in-time design assessment. Annual production is characteristic of — and commercially associated with — Type II for major financial infrastructure providers, but the contract language alone does not foreclose Type I. This is the principal uncertainty.

ISO 27001: Not referenced anywhere in the document set.

Classification rationale: Under the functional-equivalence standard, the provision substantially achieves the same protection as the acceptable position — Stripe contractually commits to providing SOC 2 reports on request with annual production — and no language caps the commitment at Type I only. The gap is the absence of the explicit "Type II" label, which introduces a moderate interpretive uncertainty rather than a demonstrated deficiency. For a High-weight item, this is sufficient for GREEN but warrants a note to the reviewer to confirm report type upon first receipt. Confidence is MODERATE due to the Type II ambiguity within the four corners of the documents.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SOC Reports. Stripe maintains Service Organization Controls ("SOC") auditing standards for service organizations issued under the AICPA. SOC 1 and 2 reports are produced annually and will be provided …"
2. "To the extent applicable to the Services, Stripe is responsible for providing the Services in a manner that is consistent with the highest certification level (PCI Level 1) provided by the PCI-DSS req…"
3. "Upon written request, and no more frequently than annually, Stripe will complete a written data security questionnaire of reasonable scope and duration regarding Stripe's business practices and data t…"

> *"Each party will maintain commercially reasonable administrative, technical, and physical safeguards designed to protect data in its possession or under its control from unauthorized access, accidental loss, and unauthorized modification."*
> — Stripe Services Agreement - General Terms

Data Protection Officer (DPO)

AI Comment: Stripe explicitly designates a Data Protection Officer (DPO) with a dedicated contact email (dpo@stripe.com) referenced consistently throughout its Privacy Policy across multiple jurisdictional contexts. This satisfies both the acceptable position ("named privacy point of contact with sufficient qualifications") and the ideal preference ("qualified Data Protection Officer").

Key evidence: (1) Stripe names an individual DPO — "Adi Gilad" — in its Brazil-specific Privacy Policy provisions, establishing that a specific, named person holds the DPO role. (2) A dedicated DPO contact (dpo@stripe.com) is referenced for EEA/UK, Brazil, Indonesia, Malaysia, Singapore, Switzerland, Thailand, India, and US contexts. (3) A separate "Global Head of Privacy" (privacy@stripe.com) is designated for Canadian users as the person in charge under PIPEDA and the Quebec Private Sector Act. (4) The general data subject rights section in the Privacy Policy refers US users to the DPO at dpo@stripe.com for appeals.

The ideal preference is met: Stripe has designated a DPO (not merely a generic privacy inbox). For EEA/UK users — governed by Irish law (GDPR), the most likely applicable jurisdiction given the conditional governing jurisdiction note — the GDPR Articles 37–39 impose mandatory qualification standards for DPOs. Stripe's explicit GDPR-context DPO designation implies legal qualification requirements are satisfied under EU law. The DPO's qualifications are not individually described in the documents, which introduces minor residual uncertainty, but the formal role designation and multi-jurisdictional scope are consistent with a qualified appointment.

— Note —
The AI cited 5 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "the right to appeal any decision by Stripe relating to your rights by contacting Stripe's Data Protection Officer ("DPO") at dpo@stripe.com"
2. "You may exercise your rights by contacting our DPO Adi Gilad at dpo@stripe.com."
3. "You may exercise your rights by contacting our DPO at dpo@stripe.com. If you are a resident of the EEA or the Stripe entity accountable for your Personal Data is otherwise subject to the GDPR, and you…"

4. "Stripe's Global Head of Privacy is the person in charge of personal information, including under the Quebec Private Sector Act. You may contact them via email at privacy@stripe.com."
5. "If you have any questions or complaints about this Policy, please contact us."

Audit Logging

AI Comment: The playbook item requires that it be possible to examine whether and by whom personal data has been entered into, modified, or removed from data processing systems — i.e., audit logging of access to PII. This requirement is directly and explicitly addressed in Stripe's Data Processing Agreement (DPA), specifically in the Data Security Exhibit's "Entry Controls" section. That section commits Stripe to implementing "measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, including logging and reporting systems, and audit trails and documentation." This language maps precisely to every element of the playbook requirement: (1) whether data was entered, (2) whether data was changed, (3) whether it was removed, (4) by whom, and (5) via logging/audit trail systems. Reinforcing this, the DPA Exhibit's "Technical Access Controls / Data access control" subsection explicitly lists "access monitoring and logging" and "access reports" among Stripe's implemented measures. The Network and Operations Management section separately references "audit logs" as part of Stripe's documented policies and procedures. The General Terms (§4.6 Controls) further commit both parties to "commercially reasonable administrative, technical, and physical safeguards" and expressly incorporate the DPA's Data Security Exhibit obligations on Stripe. Because the DPA prevails over the General Terms on Personal Data processing matters (DPA §7), the DPA Exhibit is the definitive and controlling source on this item. The combined weight of these provisions satisfies the playbook's acceptable position for audit logging at a HIGH confidence level. No preference was specified, so aiPreferenceMet is left false (no ideal threshold to evaluate against).

— Superseding reasoning —
No superseding conflict exists among the multiple references identified. The General Terms (§4.6) explicitly delegate the audit-logging obligation to Stripe's Data Security Exhibit in the DPA. Per DPA §7, the DPA prevails over the General Terms on Personal Data processing matters. The DPA Exhibit, the DPA's data access controls, and the General Terms §4.6 are fully consistent and mutually reinforcing — the DPA Exhibit is the most specific and controlling document. No provision in any document contradicts or weakens this commitment.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Data access control. Stripe implements measures to ensure that persons entitled to use a data processing system gain access only to the Personal Data allowed for their access rights, and that Personal…"

> *"Stripe implements measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, including logging and reporting systems, and audit trails and documentation."*
> — Data Processing Agreement
>
> *"These policies and procedures address hardening, change control, segregation of duties, separation of development and production environments, technical architecture management, network security, malware protection, protection of data in transit and at rest, data integrity, encryption, audit logs and network segregation."*
> — Data Processing Agreement
>
> *"Each party will maintain commercially reasonable administrative, technical, and physical safeguards designed to protect data in its possession or under its control from unauthorized access, accidental loss, and unauthorized modification. Stripe will comply with its obligations in the Data Security Exhibit to the DPA."*
> — Stripe Services Agreement - General Terms

Subprocessor Change Notification

AI Comment: The playbook's acceptable position requires three discrete elements: (1) at least 30 days' advance notice of any new or replacement subprocessor; (2) at least 30 days in which User may raise a reasonable objection; and (3) a User-initiated termination right with pro-rata refund of unused fees if Stripe proceeds with the contested subprocessor over User's objection. The contract across the document set addresses elements (1) and (2) but fails to deliver element (3), and element (1) is conditional for non-EEA users.

PRIMARY PROVISION — DPA Section 3.2(a): This is the operative general provision applicable to all users regardless of jurisdiction. It provides a 30-day advance email notification and a 30-day objection window—but the notification is not automatic. It activates only "if User subscribes to email notifications at the Stripe Sub-processors List," meaning a User who has not affirmatively subscribed receives no formal notice and would lack the predicate to exercise the objection right. This conditionality is a meaningful compliance gap against the playbook's mandatory notification requirement. Additionally, the sole stated consequence of a valid User objection is that Stripe "will not be obligated to provide User the Services for which Stripe uses that Sub-processor"—a unilateral service-limitation by Stripe, not a User-initiated termination right, and zero refund is provided.

EEA-SCOPED PROVISION — EEA SCCs Module 2, Clause 9(a) (Data Transfers Addendum): For data transfers governed by EEA DP Law, this provision (which prevails over DPA Section 3.2(a) per DPA Section 7(b)'s document-hierarchy rule) upgrades the notification to an unconditional written obligation before sub-processor engagement occurs. This satisfies the ideal timing preference for the subset of processing covered by EEA law. However, the EEA SCCs also do not create any explicit termination right or pro-rata refund remedy for an unresolved objection; the consequence of objecting is left to the underlying contractual framework, which—as noted above—does not provide a termination+refund remedy.

GAP SUMMARY: (a) Notification is conditional on subscription under the general provision (non-EEA users); (b) no provision in any document creates a User-initiated termination right coupled with a pro-rata refund of unused fees when Stripe proceeds with an objected subprocessor. The General Terms' fee non-refundability clause (§7.1(b)) further

underscores the absence of any refund pathway. Classified YELLOW: the notification and objection mechanisms are substantially addressed but the termination/refund remedy required by the playbook's acceptable position is absent across all documents.

— Superseding reasoning —
DPA Section 3.2(a) and EEA SCCs Module 2 Clause 9(a) both address subprocessor change notifications but with different scope and strength. For EEA data transfers, DPA Section 7(b) expressly states that "the provisions of the Data Transfers Addendum will prevail" over the DPA in case of conflict. The EEA SCCs (incorporated via the Data Transfers Addendum) impose an unconditional written notification at least 30 days in advance of engagement—stricter than the DPA's conditional, subscription-dependent notification. Accordingly, for EEA-scoped transfers, the EEA SCCs Module 2 Clause 9(a) supersedes DPA Section 3.2(a) on the notification mechanism. DPA Section 3.2(a) remains the governing provision for all non-EEA transfers (e.g., a US-based User processing domestic customer data). Neither provision, in any scope, provides a termination-with-refund remedy for unresolved objections.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "User consents to Stripe's use of its existing Sub-processors, as set out on the Stripe Sub-processors List, and grants Stripe a general written authorization to engage Sub-processors as necessary to p…"

> *"The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object."*
> — Data Transfers Addendum

Data Processing Security Policies

AI Comment: The playbook requirement — that data processing systems have adequate security and that adequate policies exist to prevent unauthorized access to those systems — is comprehensively met across two primary layers of contractual obligation.

Layer 1 — Mutual Contractual Commitment (General Terms §4.6): Both parties are contractually required to maintain "commercially reasonable administrative, technical, and physical safeguards designed to protect data in its possession or under its control from unauthorized access, accidental loss, and unauthorized modification." Stripe further commits to comply with its obligations in the DPA's Data Security Exhibit.

Layer 2 — Specific Technical and Organizational Controls (DPA Data Security Exhibit): The DPA, incorporated by reference into the SSA, contains a detailed Data Security Exhibit that enumerates Stripe's specific security obligations across multiple control domains:

- **Security Programs and Policies:** A formally documented and annually reviewed security program, covering acceptable computer use, data classification, cryptographic controls, access control, removable media, and remote access, with regular testing of key controls.
- **Technical Access Controls — Unauthorized Access Prevention:** Explicit controls to prevent data processing systems from being used by unauthorized persons, including MFA (NIST 800-63B compliant), user identification and authentication procedures, automatic blocking, break-in-attempt monitoring, and role-based data access controls with access monitoring and logging.
- **Network and Operations Management:** Documented policies covering hardening, change control, segregation of duties, separation of development and production environments, network security, malware protection, encryption, audit logging, and network segregation, supplemented by periodic vulnerability assessments and penetration testing.
- **Independent Third-Party Certification:** PCI DSS Level 1 compliance (highest level, confirmed annually by a QSA) and annual SOC 1 and SOC 2 reports available on request — providing independent validation that security controls are not merely stated but operational and audited.
- **Encryption:** Industry-standard AES-256 at rest, TLS 1.2 for inbound/outbound traffic, and mTLS for internal production network connections.

The combination of a mutual contractual security obligation, a comprehensive and specific policy enumeration, independent third-party certification, and concrete technical standards clearly meets the acceptable position for this High-weight item. No ideal preference was specified, so aiPreferenceMet is set to false.

Note on jurisdiction: Governing law is conditional on User's Stripe Account Country (California, Ireland, or England & Wales). The data security obligations in the DPA Exhibit are jurisdiction-agnostic and apply globally. Classification: GREEN, HIGH confidence.

— Note —
The AI cited 5 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Stripe maintains and enforces a security program that addresses how Stripe manages security, including its security controls. The security program includes:
- documented policies that Stripe formally…"
2. "Stripe implements measures to prevent data processing systems from being used by unauthorized persons, including

the following measures:
- user identification and authentication procedures;
- ID/pass…"
3. "Stripe implements policies and procedures for network and operations management. These policies and procedures address hardening, change control, segregation of duties, separation of development and p…"
4. "To the extent applicable to the Services, Stripe is responsible for providing the Services in a manner that is consistent with the highest certification level (PCI Level 1) provided by the PCI-DSS req…"
5. "Stripe applies data encryption mechanisms at multiple points in Stripe's service to mitigate the risk of unauthorized access to Stripe data at rest and in transit. Access to Stripe cryptographic key m…"

> *"Each party will maintain commercially reasonable administrative, technical, and physical safeguards designed to protect data in its possession or under its control from unauthorized access, accidental loss, and unauthorized modification. Stripe will comply with its obligations in the Data Security Exhibit to the DPA."*
> — Stripe Services Agreement - General Terms

Compliance with Referenced Laws

AI Comment: The Stripe Services Agreement (General Terms, Stripe Payments Terms, Stripe Financial Services Terms, and the Data Processing Agreement) contains an extensive body of statutory and regulatory compliance obligations imposed on User. These fall into several distinct categories: (1) a sweeping general obligation to comply with "all Laws applicable to its business" — not limited to laws governing Stripe usage; (2) sole responsibility for multi-jurisdictional tax law compliance; (3) US export control and sanctions law representations and warranties; (4) full data protection law (GDPR, CCPA, UK GDPR, and all DP Law) compliance including lawful basis, data subject rights, and privacy notice obligations; (5) broad and continuously amendable Card Network Rules (Visa, Mastercard, American Express) that can be updated at any time without notice; (6) Card Network security programs (e.g., Visa AIS Program); (7) PCI-DSS Standards compliance for own systems and all third-party service providers; (8) consumer protection law and UDAAP compliance; (9) Financial Provider Terms compliance, which expressly PREVAIL over the Agreement in case of conflict and may be amended by continued use; (10) an immediate data breach notification obligation to Stripe; and (11) jurisdiction-specific statutory obligations (India: CERT-In security incident reporting; Canada: mandatory cross-border privacy disclosures). Per playbook instruction, every finding is classified YELLOW because whether User can abide by each obligation is not determinable from the documents alone — human reviewer confirmation is required for each. The ideal preference of "no compliance obligations beyond laws applicable to our own use of the services" is clearly not met: the Agreement imposes compliance obligations under external regulatory frameworks (card network rules, Financial Provider Terms, PCI Standards, DP Law, US trade control law, tax statutes, and regional cybersecurity mandates) that extend well beyond the scope of laws governing User's own use of the payment service.

— Note —
The AI cited 9 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "User must notify Stripe immediately if User becomes aware of any unauthorized acquisition, modification, disclosure, access to, or loss of Personal Data on User's systems that was provided to or used …"
2. "User must comply with all Financial Provider Terms that apply to User's use of the Services. If there is any inconsistency between any provision of this Agreement and the Financial Provider Terms, the…"
3. "User must comply with Payment Method acceptance and use requirements which may be incorporated into the Stripe API and other Stripe Technology described in the Documentation, or set out in the Payment…"
4. "When accepting payment card Transactions, User must comply with all applicable Card Network Rules, including the Visa Rules specified by Visa, the Mastercard Rules specified by Mastercard, and the Ame…"
5. "User must comply with the Card Networks' security standards, requirements and programs (e.g., the Visa Account Information Security Program), and all Card Network Rules governing the privacy, protecti…"
6. "If User elects to store or hold "Account Data," as defined in the PCI Standards (including Customer card account number or expiration date), User must maintain a system that complies with the PCI Stan…"
7. "User must, and will ensure that User's third-party service providers that store, access or transmit Payment Method Account Details, comply with the PCI Standards, to the extent they apply."
8. "If any security breach, leak, loss, or compromise of Data occurs on User's systems, website, or application, and it affects User's compliance with this Agreement or User's obligations under applicable…"
9. "User must disclose to User's Customers in User's Privacy Policy that Personal Data may be transferred, processed, and stored outside of Canada and, as a result, may be subject to disclosure as Law req…"

> *"Each party must comply with all Laws applicable to its business in its performance of obligations or exercise of rights under this Agreement."*
> — Stripe Services Agreement - General Terms
> *"User is solely responsible for evaluating and configuring the Services to comply with User's legal obligations."*
> — Stripe Services Agreement - General Terms
> *"User has sole responsibility and liability for:*
>
> *(i) determining which, if any, Taxes or fees apply to the sale of its products and services, acceptance of donations, or payments it receives in connection with its use of the Services; and*
>
> *(ii) assessing, collecting, reporting, and remitting Taxes for its business to the appropriate tax and revenue authorities."*
> — Stripe Services Agreement - General Terms
> *"User must not use or otherwise export, re-export, or transfer the Stripe Technology except as authorized by United States law and the laws of the jurisdiction(s) in which the Stripe Technology was distributed and obtained, including by providing access to Stripe Technology (a) to any individual or entity ordinarily resident in a High-Risk Jurisdiction; or (b) to any High-Risk Person. By using the Stripe Technology, User represents and warrants that User is not (i) located in or organized under the laws of any High-Risk Jurisdiction; (ii) a High-Risk Person; or (iii) owned 50% or more, or controlled,*

by individuals and entities (x) located in or, as applicable, organized under the laws of any High-Risk Jurisdiction; or (y) any of whom or which is a High-Risk Person."
— Stripe Services Agreement - General Terms
"User must not use the Services or Stripe Technology for any purposes prohibited by Law, including the development, design, manufacture or production of missiles, nuclear, chemical, or biological weapons."
— Stripe Services Agreement - General Terms
"User must comply with and perform User's obligations under DP Law, including with regard to Data Subject rights, data security and confidentiality, and ensure User has an appropriate legal basis for the Processing of Personal Data as described in the Agreement, including this DPA"
— Data Processing Agreement
"User must provide all necessary notices (including by making available a Privacy Policy) to, and obtain all necessary rights, permissions and consents from, Data Subjects (including Customers), to enable Stripe to lawfully Process any Personal Data provided by User as described in the Agreement, including this DPA."
— Data Processing Agreement
"If User engages in Transactions with Customers who are consumers, User must provide the disclosures Law requires, and must not engage in unfair, deceptive, or abusive acts or practices."
— Stripe Services Agreement - Services Terms

License Grant to Data – Our Company to Vendor

AI Comment: The Stripe Services Agreement contains three distinct license grants from User to Stripe, all of which are explicitly non-exclusive — satisfying the acceptable position of this Critical-weight playbook item. However, the ideal preference (revocable AND limited to providing the service to User) is not met for the two most broadly applicable licenses.

Why GREEN (Acceptable Position Met): Every license User grants to Stripe is consistently qualified as "non-exclusive." This term appears verbatim in §5.1(c) (Content license), §5.2 (Feedback license), and §5.3(a) (Marks license). There is no provision in which User grants Stripe an exclusive license. The acceptable-position threshold is therefore satisfied with HIGH confidence.

Why aiPreferenceMet = false: The ideal preference requires the license to be (a) revocable and (b) scoped solely to providing the service to User. This preference is not met by the two most consequential licenses:

1. **§5.1(c) — Content License (most significant for a payment-processing use case):** Stripe receives a "perpetual, worldwide, non-exclusive, irrevocable, royalty-free license to use the Content to develop, improve, and provide Services and Stripe Technology *and for Stripe's internal business purposes.*" The license is irrevocable (not revocable), perpetual (survives agreement termination), and the scope extends to Stripe's internal business purposes beyond merely providing the contracted service. "Content" is broadly defined as all text, images, and other non-Personal-Data information User provides to Stripe — including product/service descriptions, storefront copy, and anything else User uploads in connection with the Services. For a payment processing deployment, this captures a meaningful range of User-supplied materials.

2. **§5.2 — Feedback License:** The Feedback license is "perpetual, worldwide, non-exclusive, irrevocable, royalty-free" and permits use "for any purpose." Like the Content license, it is irrevocable and unlimited in scope relative to the service-provision preference.

3. **§5.3(a) — Marks License (most favorable; closely aligns with preference):** The Marks license is non-exclusive, non-transferable, non-sublicensable (with limited carve-outs), during the Term only, and restricted "solely to provide the Services to User." This license comes closest to the ideal preference — it is effectively revocable upon termination and purpose-limited — but it covers Marks only (logos, service marks, trademarks), not data or content more broadly.

Summary for reviewers: The non-exclusive requirement is clearly and consistently satisfied across all license grants. The material concern is that the Content license (§5.1(c)) is irrevocable, perpetual, and expressly extends to Stripe's internal business purposes. In a payment processing deployment, User will provide Stripe with non-Personal-Data content (product/service descriptions, branding, etc.) under a license that survives termination and permits Stripe to use it internally without restriction. Human review should assess whether the perpetual, irrevocable, beyond-service-scope grant in §5.1(c) is acceptable given the organization's risk tolerance, even though it meets the minimum non-exclusive threshold. The Marks license (§5.3(a)) demonstrates that Stripe is capable of drafting a term-limited, purpose-limited, non-exclusive license when it chooses to — raising the question of why the Content license is drafted more broadly.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "User grants to Stripe, on behalf of itself and its Affiliates, a perpetual, worldwide, non-exclusive, irrevocable, royalty-free license to use the Content to develop, improve, and provide Services and…"
2. "Subject to this Agreement, each party (or its applicable Affiliates) grants to the other party a worldwide, non-exclusive, non-transferable (except as allowed under Section 11.10 (Assignment)), non-su…"

"Except as indicated in Section 1.4, Feedback is voluntary and User grants to Stripe, on behalf of itself and its Affiliates, a perpetual, worldwide, non-exclusive, irrevocable, royalty-free license to use that Feedback for any purpose."
— Stripe Services Agreement - General Terms

Our liability

AI Comment: The Stripe Services Agreement contains a bilateral liability cap in General Terms §8.4 that limits a party's total aggregate liability to the total fees User paid to Stripe in the 12-month period preceding the first event giving rise to liability. This nominally satisfies the acceptable position of "our liability limited to amount paid."

However, the cap is substantially undermined by the Excluded Claims definition (§12), which removes four categories of User liability from the cap entirely: (a) User's gross negligence, fraud, or willful misconduct (broadly standard market practice); (b) User's breach of the Restrictions clause (§1.2); (c) User's breach of Confidentiality (§6); and — most impactfully — (d) all amounts payable under §9.1 Indemnities. The §9.1(a) General Indemnity is drafted to cover "all Losses arising from User's use of the Services or Stripe Technology," a trigger so wide that virtually any claim Stripe would assert against User could be framed as arising from service use, rendering the cap effectively non-operative for Stripe's most likely causes of action against User.

Additionally, the Stripe Payments Terms §11 — which prevails over the General Terms per the §11.9 Order of Precedence (Service Terms > General Terms) — explicitly states that the §8.3 and §8.4 limitations "do not apply" to fraudulent transaction losses, a significant and foreseeable exposure given the payment-processing use case (Stripe is being used to process product purchases). Financial Provider audit costs triggered by User's use of the Payments Services are also excluded from the cap under §11.

User's payment obligations (Fees, Assessed Fines, Taxes) are also expressly excluded from the cap within §8.4 itself.

In summary: a general fee-based cap exists (meeting the acceptable position in form), but the Excluded Claims — particularly the broad indemnity carve-out and the Payments Terms fraudulent-transaction override — materially dilute the protection such that the User's liability is not reliably "limited to amount paid" in foreseeable scenarios. The weight is Acceptable to Deviate, which limits the severity of this finding, but the gaps are substantive enough to warrant YELLOW rather than GREEN.

— Superseding reasoning —
The Stripe Payments Terms (Service Terms) prevail over the General Terms per §11.9 Order of Precedence. Section 11 of the Stripe Payments Terms contains explicit language removing the General Terms §§8.3 and 8.4 liability limitations from application to fraudulent transaction losses. This specific carve-out in the higher-precedence document controls over the general liability cap for that category of claim.

— Note —
The AI cited 4 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Except for Excluded Claims, a party's total aggregate liability for damages and Losses for all claims arising out of or relating to the Agreement (including Data Incident Losses) is limited to the tot…"
2. "" **Excluded Claims**" means: (a) a party's gross negligence, fraud, or willful misconduct, (b) User's breach of Section 1.2 (Restrictions), (c) a party's breach of Section 6 (Confidentiality) but exc…"
3. "Subject to Section 9.2 (Limitations on Indemnity), User will indemnify Stripe, its Affiliates, and their directors, employees, and agents for all Losses arising from User's use of the Services or Stri…"
4. "As between the parties, User is responsible for all (a) losses, damages, and costs Stripe and its Affiliates incur due to fraudulent Transactions, and the limitations on liability in Sections 8.3 and …"

> *"Except for Excluded Claims, to the maximum extent permitted by Law, neither party will have any liability in relation to this Agreement for any indirect, consequential, special, reliance, incidental, or punitive damages, lost revenue, profits, savings or goodwill, business interruption, personal injury, property damage, or loss of data, whether in contract, negligence, strict liability, tort, or other legal or equitable theory, even if these losses, damages, or costs are foreseeable, and whether or not any party has been advised of their possibility."*
> — Stripe Services Agreement - General Terms

Termination Obligations

AI Comment: The acceptable position requires that upon termination, the Vendor (Stripe) must return or make available **all** of the User's data. The contract partially addresses this requirement, but coverage is fragmented across multiple documents, conditioned in material ways, and expressly absent for certain categories of data.

What is covered:

1. **Personal Data (DPA §3.1(h))**: The DPA contains an explicit obligation requiring Stripe, at User's choice, to either delete or return all Personal Data processed in connection with the Services following termination. The User controls whether data is returned or deleted, which is a meaningful protection. However, exceptions exist where Stripe may retain data (when required by its own contractual rights, or by law), and this obligation is narrowly scoped to "Personal Data" as defined—it does not extend to other categories of User data.

2. **Payment Method Account Details (Stripe Payments §7.2)**: Card/payment credential data can be transferred upon termination, but only: (a) to a third-party PCI-DSS Level 1-certified payment processor (not directly to User); (b) when termination is not caused by User's breach; (c) "to the extent commercially reasonable"; and (d) subject to Stripe's right to refuse if it deems the receiving processor inadequate or if Law/Financial Provider Terms prohibit it. This falls materially short of "return or make available to User" — it is an indirect transfer with multiple gating conditions.

What is not covered or actively cuts against the requirement:

3. **General Terms §4.4**: Stripe is expressly *not obligated* to retain data after the Term (outside narrow exceptions). There is no affirmative obligation to return or make available general business data, Content, or transaction history to User post-termination. The absence of a retention obligation means such data may simply become unavailable.

4. **Stripe Data**: Defined in §12 as data from API interactions, security/fraud data, and aggregated information — this is characterized as belonging to Stripe under §5.1(a), with User's use restricted to the DPA framework. No return obligation exists.

5. **API/Dashboard access**: The DPA Exhibit references programmatic data portability via the Stripe API, but this is an in-Term mechanism. Post-termination access is not guaranteed, and §10.2 (Effect of Termination) confirms User's rights to use the Services and Stripe Technology immediately cease upon termination.

Overall: The "all data" standard in the playbook item is not met. Personal Data has a meaningful DPA-based protection (user-choice return or deletion), but card data return is indirect and heavily conditioned, and other data categories (general business records, Stripe Data, transaction history outside Personal Data) have no affirmative return mechanism. The General Terms §4.4 actively disclaims any Stripe obligation to retain data post-termination. This combination of partial coverage, data-type gaps, and significant conditions supports a YELLOW classification for this Medium-weight item.

— Superseding reasoning —
Multiple provisions across different document tiers address different sub-categories of data, and document hierarchy governs which controls each category:

1. For **Personal Data**: DPA §7(a) expressly states that the DPA prevails over the Agreement on Personal Data Processing matters. Therefore, DPA §3.1(h) (return or deletion at User's choice) supersedes and governs over the General Terms §4.4 (no retention obligation) for Personal Data specifically.

2. For **Payment Method Account Details**: The Stripe Payments Terms are Service Terms and sit above the General Terms in the §11.9 precedence hierarchy (Service Terms > General Terms > incorporated terms). Stripe Payments §7.2 therefore governs over General Terms §4.4 for this data category.

3. For **general data/Stripe Data**: Only the General Terms §4.4 applies (no superseding Service Term or DPA provision governs this category). That provision disclaims any Stripe retention obligation post-termination, with no affirmative return obligation.

There is no conflict between hierarchy clauses in this instance—the documents do not disagree about their own precedence.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "at User's choice, delete or return to User all Personal Data Processed in connection with the Services, and delete existing copies, following termination of the Agreement, except that Stripe will not …"
2. "If these Stripe Payments Terms terminate for reasons other than User's breach, then within 30 days after the termination date, User may request in writing that Stripe provide all relevant Payment Meth…"

> *"Stripe is not obligated to retain data that it receives from or through User after the Term, except as (a) required by Law; (b) reasonably required for Stripe to perform any post-termination obligations; (c) this Agreement otherwise states; or (d) the parties otherwise agree in writing."*
> — Stripe Services Agreement - General Terms
> *"The Stripe API enables Users to programmatically access the data stored for transfer, excluding PCI-scoped data. The portability process for PCI data to other PCI-DSS Level 1 compliant payment processors can be found at https://stripe.com/docs/security/data-migrations/exports."*
> — Data Processing Agreement

Employee Access Control

AI Comment: The acceptable position requires that the vendor grant system access only to authorized personnel, on a need-to-know basis, strictly limited to what is required to fulfill their function. Stripe's contractual documents directly and explicitly satisfy all three elements of this requirement across multiple instruments.

The primary governing commitment appears in DPA § 3.1(b), which expressly obligates Stripe — when acting as a Data Processor — to "ensure that all persons Stripe authorizes to Process Personal Data are granted access to Personal Data on a need-to-know basis and are committed to respecting the confidentiality of that Personal Data." This language maps directly and verbatim to the playbook item's "need-to-know" and "authorized personnel" requirements.

The DPA's Data Security Exhibit operationalizes this commitment with granular technical and organizational measures: (i) access controls preventing unauthorized use of processing systems; (ii) data access controls ensuring personnel can only reach the Personal Data their access rights permit, implemented through differentiated access rights (profiles, roles, actions, objects), access monitoring and logging, and formal access procedures; and (iii) a Separation Controls section that explicitly invokes a "least privilege" limitation on data access by internal services, directly addressing the "strictly limited to what is required to fulfill their function" element.

The Data Transfers Addendum (EEA SCCs Module 2 § 8.6(b) and Module 3 § 8.6(b)) adds an additional layer of obligation

applicable to cross-border Personal Data transfers: personnel access granted "only to the extent strictly necessary for the implementation, management and monitoring of the contract," plus a mandatory confidentiality commitment for all authorized personnel.

The General Terms § 4.6 general security safeguards provision (applicable to both parties for data in their control) is less specific for Personal Data processing contexts and is superseded by the DPA provisions pursuant to DPA § 7, which gives DPA provisions precedence over the Agreement regarding Personal Data Processing.

Collectively, Stripe's commitments on employee access control are explicit, multi-layered, and directly aligned with each element of the acceptable position. Classification: GREEN. No gaps identified. Note: No ideal preference was specified, so aiPreferenceMet is set to false.

— Superseding reasoning —
The DPA Section 7 establishes an explicit document hierarchy: "To the extent of any conflict between the provisions of this DPA and any provision of the [Agreement] regarding Personal Data Processing, the provisions of this DPA will prevail." General Terms § 4.6 articulates only a general "commercially reasonable safeguards" standard for both parties, while DPA § 3.1(b) and the Data Security Exhibit impose specific, mandatory, named access control obligations on Stripe as Data Processor (need-to-know; differentiated access rights; least privilege; logging). For the purpose of this playbook item — employee access control as it relates to Stripe's handling of Personal Data — the DPA provisions are both the governing hierarchy tier and the more specific instrument, and they supersede the General Terms general security language.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Access control. Stripe implements measures to prevent data processing systems from being used by unauthorized persons, including the following measures:
- user identification and authentication proced…"
2. "Data access control. Stripe implements measures to ensure that persons entitled to use a data processing system gain access only to the Personal Data allowed for their access rights, and that Personal…"
3. "Stripe implements measures to ensure that Personal Data collected for different purposes can be Processed separately, including:
- "least privilege" limitation of access to data by internal services;
…"

> *"ensure that all persons Stripe authorizes to Process Personal Data are granted access to Personal Data on a need-to-know basis and are committed to respecting the confidentiality of that Personal Data;"*
> — Data Processing Agreement
> *"The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality."*
> — Data Transfers Addendum
> *"Each party will maintain commercially reasonable administrative, technical, and physical safeguards designed to protect data in its possession or under its control from unauthorized access, accidental loss, and unauthorized modification."*
> — Stripe Services Agreement - General Terms

Confidentiality

AI Comment: The Stripe Services Agreement (Section 6) contains a mutual confidentiality framework that substantially meets the acceptable position. Both parties are obligated to use "reasonable care" to prevent disclosure of the other's Confidential Information, satisfying the mutuality requirement. The standard carve-outs are all present (public domain, prior knowledge, independent development, rightful third-party receipt), and the definition of Confidential Information covers information "designated as confidential or that reasonably should be understood to be confidential" — a standard and acceptable formulation.

On the core acceptable position requirement — that User can share CI with subcontractors/subprocessors on a need-to-know basis — Section 6 expressly permits User to disclose to its "directors, employees, contractors, agents, professional advisors, and third-party auditors" who have "a legitimate need to know" and are "subject to confidentiality obligations at least as protective as this Agreement." This directly satisfies the playbook's acceptable position for User-side sharing.

On the reciprocal requirement — that Stripe (Vendor) must not disclose User's CI to third parties except those needing it to perform the services — Section 6 satisfies this in substance, but with a notable asymmetry: when Stripe is the recipient, it may additionally disclose to "Financial Providers and their respective Affiliates, and Stripe's third-party service providers, as reasonably necessary to perform the Services." Critically, all these recipients must still (a) have a "legitimate need to know" and (b) be "subject to confidentiality obligations at least as protective as this Agreement." The "reasonably necessary" and "legitimate need to know" dual constraints functionally match the playbook's "need to know in order to perform the services" standard, supporting a GREEN classification for the overall item. However, the extension to Financial Providers' Affiliates — entities that may be large corporate groups only tangentially connected to service delivery — is broader than User's equivalent disclosure rights and warrants noting.

Additional provisions strengthen the overall posture: (1) breach of Section 6 is carved out of the aggregate liability cap as an "Excluded Claim," meaning full damages can be sought for confidentiality breaches; (2) Section 11.15 expressly entitles the non-breaching party to seek specific performance or injunctive relief for material breaches of Section 6; and (3)

confidentiality obligations survive termination for three years (indefinitely for trade secrets) under Section 10.3(e).

The ideal preference — that Stripe will not share User's Confidential Information with any third party — is clearly not met. Stripe has explicit, contractual rights to share with Financial Providers, their Affiliates, and its own service providers, which is expected given Stripe's role as a payment infrastructure provider but defeats the ideal preference. Confidence is MODERATE given the interpretive question of how broadly "Financial Providers and their respective Affiliates" may be applied in practice.

— Note —
The AI cited 4 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "The recipient may disclose Confidential Information only to its and its Affiliates' directors, employees, contractors, agents, professional advisors, and third-party auditors (and where Stripe is the …"
2. "These confidentiality obligations do not apply to information that the recipient can prove through written documentation: (a) is or becomes publicly available through no fault of the recipient; (b) it…"
3. ""Excluded Claims" means: (a) a party's gross negligence, fraud, or willful misconduct, (b) User's breach of Section 1.2 (Restrictions), (c) a party's breach of Section 6 (Confidentiality) but excludin…"
4. ""Confidential Information" means all information disclosed by a party ("Disclosing Party") to the other party ("Receiving Party"), whether orally or in writing, that is designated as confidential or t…"

> *"The recipient will use reasonable care to prevent the disclosure of the discloser's Confidential Information."*
> — Stripe Services Agreement - General Terms
> *"The recipient may disclose Confidential Information if required by Law, subpoena, or court order, or if directed by a Governmental Authority, as long as (if permitted by Law) it notifies the discloser in advance (to the extent legally permitted) and provides reasonable assistance, at the discloser's cost, if the discloser wishes to contest the disclosure."*
> — Stripe Services Agreement - General Terms
> *"trade secrets, indefinitely, and all other confidentiality obligations, for 3 years after the date of termination."*
> — Stripe Services Agreement - General Terms
> *"Any material breach by a party of Sections 2, 4, 5, and 6 could cause the non-breaching party irreparable harm for which the non-breaching party has no adequate remedies at Law. Accordingly, the non-breaching party is entitled to seek specific performance or injunctive relief for the breach."*
> — Stripe Services Agreement - General Terms

Warranty & Remedy

AI Comment: The Stripe Services Agreement explicitly and comprehensively contradicts the playbook item's acceptable position on both required elements — a warranty of material performance per documentation and a pro-rata refund fallback.

Element 1 — Warranty of material performance per documentation: §8.2 (Disclaimers) provides that Stripe offers its Services and Stripe Technology strictly "as is" and expressly disclaims all warranties — express, implied, statutory, and arising from course of dealing — including implied warranties of fitness for a particular purpose and merchantability. Critically, §8.2 further specifies that Stripe does not warrant that services will be uninterrupted or error-free. This is an unambiguous categorical denial of any warranty that services perform materially per documentation, directly contradicting the playbook's acceptable position.

Element 2 — Pro-rata refund if vendor cannot repair/replace: No repair-or-replace obligation, no pro-rata refund mechanism, and no remedy of any kind is offered in the event of service underperformance. §8.1 closes any potential gap by providing that all disclaimer provisions survive and remain in effect even if any limited remedy fails of its essential purpose — eliminating any equitable fallback.

Jurisdiction-specific partial exception: For Australian users who qualify as "consumers" under the Australian Consumer Law, §13.3.1 (Australia Regional Terms) preserves non-excludable statutory service quality guarantees that §8.2's disclaimer cannot legally eliminate. Where such guarantees are breached, §13.3.2 limits Stripe's liability to re-supplying the services or paying the cost of re-supply. The Regional Terms prevail over the General Terms in the event of a conflict (per the Regional Terms precedence clause). This constitutes a partial functional equivalent to the "repair or replace at no cost" element of the playbook for Australian users only — but: (a) no pro-rata refund exists even for Australian users; (b) the remedy election is Stripe's, not User's; and (c) this carve-out applies only if the Stripe Account Country is Australia, which is unconfirmed.

Governing analysis for this review: Because the intake brief does not specify the User's Stripe Account Country, the jurisdiction is unresolved. The General Terms apply as the baseline, under which the warranty disclaimer governs in full — yielding a RED classification. The Australia Regional Terms are flagged as a conditional partial mitigant should the governing jurisdiction be confirmed as Australia.

Practical risk context: The weight is "Acceptable to Deviate," meaning this finding is noted but is not a blocking risk. "As-is" disclaimers with no performance warranties are the universal standard in payment processing SaaS agreements; Stripe's language is consistent with this market norm. Stripe does provide basic business and technical support under §1.3, which is operational mitigation (though not a warranty substitute). Confidence is HIGH — the disclaimer language is explicit, unambiguous, and comprehensive.

— Superseding reasoning —
The Australia Regional Terms (§13.3.1 and §13.3.2) expressly prevail over the General Terms in cases of conflict, per the Regional Terms precedence clause at the opening of §13 ("If there is a conflict between the General Terms and the Regional Terms, the Regional Terms prevail"). For Australian users, §13.3.1 overrides §8.2's "as is" disclaimer with respect

to non-excludable statutory service quality guarantees, and §13.3.2 overrides §8.2's blanket denial of remedies by providing a re-supply remedy for breaches of non-excludable conditions. This superseding is conditional: it applies only where the User's Stripe Account Country is Australia and the User qualifies as a "consumer" under the Australian Consumer Law. For all other jurisdictions, the General Terms disclaimers govern in full without modification.

— Note —
The AI cited 4 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Stripe provides the Services and Stripe Technology "as is", and to the maximum extent permitted by Law, Stripe does not make any, and disclaims all, warranties (other than those stated as a "warranty"…"
2. "Stripe does not warrant that User's use of the Services and Stripe Technology will be uninterrupted or error-free or that User's use of the Services and Stripe Technology comply with Law."
3. "To the extent that User acquires goods or services from Stripe as a consumer within the meaning of the Australian Consumer Law as set out in the Competition and Consumer Act 2010 (Cth), User has certa…"
4. "To the extent that the Australian Consumer Law permits, a party's liability for breach of a Non-excludable Condition is limited, at the party's option, to (i) in the case of services, supplying the se…"

> *"The exclusions and limitations in this Section 8 (Limitation of Liability) apply regardless of the legal theory or form of action and will survive and apply even if any limited remedy in this Agreement fails of its essential purpose."*
> — Stripe Services Agreement - General Terms

Non-Solicitation of Employees

AI Comment: The entire Stripe document set — General Terms, Services Terms (all sub-terms), Data Processing Agreement, Data Transfers Addendum, Prohibited and Restricted Businesses list, and Privacy Policy — is completely silent on non-solicitation of employees. No provision in any document restricts User's ability to solicit, recruit, or hire Stripe personnel through any channel.

Critically, the nature of this playbook item inverts the standard silence-analysis logic. Standard silence analysis asks whether a USER PROTECTION is missing from the contract; here, the item asks whether the VENDOR HAS IMPOSED A RESTRICTION on User. The silence therefore operates in User's favor: the complete absence of a non-solicitation clause means User faces zero contractual limitations on soliciting or hiring Stripe employees — whether through general public postings, direct outreach, or recruiter referrals.

Acceptable position analysis: The acceptable threshold requires, at minimum, that any non-solicitation clause carve out applicants who respond to general public job postings. Because no non-solicitation clause exists at all, this threshold is fully met — there is no restriction from which a carve-out would even be needed.

Ideal preference analysis: The ideal preference is (a) no limitations on solicitation whatsoever, and (b) an express disclaimer of recruiter referrals. The silence satisfies condition (a) entirely: User is unrestricted. Condition (b) calls for an express carve-out within a restricting clause; because no restricting clause exists, the practical concern underlying condition (b) — freedom to hire through recruiter channels — is achieved by the absence of any prohibition. The ideal preference is substantively met.

Jurisdiction note (informational, not dispositive): Under California law, the applicable governing law for US-based Users per Section 13.1 of the General Terms, non-solicitation of employee clauses are broadly unenforceable under California Business and Professions Code § 16600, which voids contractual restraints on trade. Even if Stripe were to add such a provision in a future amendment, it would face significant enforceability challenges for US-based Users under the governing law. This reinforces the already-favorable position established by the silence.

Classification: GREEN. Silence is the favorable outcome here. User has complete contractual freedom to solicit and hire Stripe employees through any channel, which meets and exceeds both the acceptable threshold and the ideal preference. aiPreferenceMet is set to true because the substance of the ideal preference — no limitations on solicitation — is fully achieved.

Subprocessor Agreements

AI Comment: The playbook item has two distinct requirements that must both be satisfied: (1) Stripe must enter into written agreements with all subprocessors imposing obligations at least as strict as the DPA; and (2) where a subprocessor would have privileged access, Stripe must either prohibit its use or obtain User's prior approval.

Requirement 1 — Written Agreements: Substantially addressed across multiple document layers, but with a deviation in standard. DPA §3.2(b) commits Stripe to written agreements with each Sub-processor imposing obligations "comparable to those imposed on Stripe under this DPA," including data security measures, and preserves Stripe's full liability for subprocessor failures. General Terms §11.16 independently confirms the written-agreement obligation. For EEA transfers, the Data Transfers Addendum Module 2 Clause 9(b) elevates the standard to "in substance, the same data protection obligations … including in terms of third-party beneficiary rights for data subjects." Per DPA §7(b), the DTA prevails over the DPA itself, so the stronger "in substance, the same" standard governs EEA-context transfers. For non-EEA users (e.g., US-based), the "comparable" language of DPA §3.2(b) applies — a notable but modest deviation from "at least as strict." Stripe's retained liability for subprocessor failures (DPA §3.2(b), second sentence) partially compensates for the weakened standard, but does not fully substitute for an "at least as strict" commitment.

Requirement 2 — Privileged Access Controls: Completely absent from all reviewed documents. No provision in the General Terms, DPA, Data Transfers Addendum, or Services Terms prohibits or restricts the use of subprocessors with privileged access to User data, nor establishes any mechanism for User's prior approval specifically for such subprocessors.

The general objection mechanism in DPA §3.2(a) — 30-day advance notice, objection on "legitimate grounds," and general authorization — is neither designed for nor adequate as a privileged-access control. Its practical enforceability is further undermined by DPA §3.2(a)'s explicit statement that if User objects to a Sub-processor, Stripe is not obligated to provide the relevant Services. This means the "objection right" is effectively a right to lose services, not a true veto over privileged-access subprocessor deployment.

Overall: YELLOW for this Critical weight item. The core written-agreement obligation is substantially present (precluding RED), but two material gaps prevent GREEN: (a) the "comparable" standard for non-EEA transfers falls short of "at least as strict"; and (b) the privileged access control requirement — prohibition or prior approval — is entirely unaddressed in any document. Jurisdiction remains unconfirmed, meaning the weaker non-EEA standard may govern. Human review is warranted to assess whether the "comparable" obligation is contractually sufficient and to negotiate express privileged-access subprocessor controls.

— Superseding reasoning —
Two superseding determinations apply across the four PIFs. First, for EEA-transfer contexts, the Data Transfers Addendum Module 2 Clause 9(b) supersedes DPA §3.2(b) pursuant to DPA §7(b)'s explicit hierarchy (DTA prevails over DPA for conflicts), applying the stronger "in substance, the same data protection obligations" standard in place of DPA §3.2(b)'s "comparable obligations." Second, DPA §3.2(b) supersedes General Terms §11.16 as the specific data-protection instrument governing subprocessor agreements — per DPA §7(a) (DPA prevails over the Agreement for personal data matters) and the specific-over-general interpretive principle, as §11.16 sets only a general "appropriate agreements" standard while §3.2(b) provides a specific data-protection standard.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "User consents to Stripe's use of its existing Sub-processors, as set out on the Stripe Sub-processors List, and grants Stripe a general written authorization to engage Sub-processors as necessary to p…"

> *"Stripe will enter into a written agreement with each Sub-processor that imposes on that Sub-processor obligations comparable to those imposed on Stripe under this DPA, including the obligation to implement appropriate Data Security Measures. If a Sub-processor fails to fulfill its data protection obligations under that agreement, Stripe will remain liable to User for the acts and omissions of its Sub-processor to the same extent Stripe would be liable if performing the relevant Services directly under this DPA."*
> — Data Processing Agreement
>
> *"Stripe may use subcontractors or its Affiliates in the performance of its obligations under this Agreement. Stripe remains responsible for its overall performance under this Agreement and for having appropriate written agreements in place with its subcontractors and Affiliates to enable Stripe to meet its obligations under this Agreement."*
> — Stripe Services Agreement - General Terms
>
> *"Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses."*
> — Data Transfers Addendum

Assignment

AI Comment: Section 11.10 of the General Terms explicitly addresses assignment but only partially meets the playbook's acceptable position, which requires: (1) both parties may freely assign to M&A successors without consent, and (2) any non-M&A assignment by Vendor (Stripe) requires User's prior consent.

User-side (compliant): §11.10 restricts User's general assignment right to cases where Stripe's prior consent is obtained (with a reasonableness qualifier), while carving out free assignment to M&A successors upon prompt written notice and assumption of obligations. This structure is consistent with the first part of the playbook's acceptable position.

Vendor-side (non-compliant — the key gap): §11.10 states unambiguously that "Stripe may assign and transfer its rights and obligations under this Agreement (in whole or in part) without User's consent." There is no limitation to M&A-related assignments, no requirement for User's prior consent for any assignment, and no notice obligation under the General Terms applicable to the most likely governing jurisdiction (California/US). Stripe could therefore assign to any party — including unknown third parties — without User's knowledge or approval.

Jurisdictional note: Australian regional terms (§13.9) and New Zealand regional terms (§13.10) each add a "prior written notice" obligation for Stripe's assignments. This is a partial improvement, but notice is materially weaker than the prior consent required by the playbook's acceptable position. These provisions apply only if User's Stripe Account Country is Australia or New Zealand; the intake brief indicates a US-based payment processing use case, making California (US) the most probable governing jurisdiction — where no equivalent protection exists under the US Regional Terms.

Risk calibration: The imbalance between the parties' assignment rights — User must obtain Stripe's consent for non-M&A assignments, Stripe can assign freely — is widespread in enterprise SaaS and payment processing agreements and reflects Stripe's need to reorganize corporate entities and transfer obligations to affiliates. Given the "Acceptable to Deviate" weight, this is an informational finding. No approval or justification is required, though a comment noting the gap is recommended per the risk matrix.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "User may not assign or transfer any of its rights or obligations under this Agreement without Stripe's prior consent (which consent will not be unreasonably withheld or delayed). However, User may ass…"

> *"If Stripe assigns and transfers its rights and obligations under this Agreement as described in Section 11.10 (Assignment), Stripe will provide prior written notice to User."*
> — Stripe Services Agreement - General Terms

Vendor Audit Rights

AI Comment: The playbook item requires that User has the right to audit Stripe's systems and its compliance with the DPA. The topic is addressed across multiple documents, but the protections provided are materially weaker than a conventional direct audit right.

What Stripe provides:
DPA Section 3.1(g) is the operative provision. It does not grant a right of direct inspection or appointment of an independent auditor to examine Stripe's systems. Instead, it limits Stripe's obligation to two mechanisms: (1) making pre-existing audit reports available (i.e., third-party audit reports such as SOC 1/2 reports and PCI QSA certifications, as referenced in the DPA Exhibit); and (2) completing a written data security questionnaire. Both mechanisms are capped at once annually and all outputs are Stripe's confidential information.

The DPA Exhibit confirms this architecture: SOC 1 and 2 reports are produced annually and provided on request; PCI Level 1 certification is confirmed annually by a qualified security assessor — but these are third-party audits of Stripe's own choosing, not User-directed audits. User has no right to direct the scope, timing, or methodology.

The EEA SCCs issue (and DTA channeling):
EEA SCCs Module 2, Clause 8.9 (incorporated into the DTA) facially provides broader rights: Stripe must "allow for and contribute to audits... [which] may include inspections at the premises or physical facilities" conducted by the data exporter or an independent auditor with reasonable notice. Standing alone, this would satisfy the playbook item (GREEN). However, DTA Section 8.4 explicitly channels these rights back into the DPA mechanism: "User exercises User's audit right under Clause 8.9... by instructing Stripe, LLC to comply with the audit measures described in the DPA." Since the DPA audit measures are limited to reports and questionnaires, the DTA effectively collapses the broader SCC audit right into the narrower DPA mechanism.

Competing hierarchy tension — flag for human review:
EEA SCCs Module 2, Clause 5 states: "In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties...these Clauses shall prevail." If DTA Section 8.4's channeling of on-site inspection rights to a reports/questionnaire-only mechanism is characterized as a "contradiction" with Clause 8.9(d), the SCCs would prevail and the broader audit right (including on-site inspection) would survive. Stripe might argue DTA 8.4 merely specifies how — not whether — to exercise the right, making it an implementation detail rather than a contradiction. This interpretive question has material practical significance and should be reviewed by counsel. Per the DPA's conflict clause (§7(b)), the DTA prevails over the DPA, but the SCC hierarchy clause potentially overrides the DTA's own channeling language.

Net assessment:
Regardless of which interpretation governs, the operative audit mechanism as presented by Stripe is limited to reports and questionnaires. A direct audit of Stripe's systems (involving User-appointed auditors, on-site access, or scope-controlled inspection) is not unambiguously available. This is a meaningful gap from the acceptable position, warranting a YELLOW classification. If the SCC interpretation (broader audit rights) is upheld, the classification improves, but that requires legal judgment not resolvable on the face of the documents alone.

— Superseding reasoning —
DTA Section 8.4 supersedes the EEA SCCs Module 2, Clause 8.9 audit provision by explicitly specifying that User's audit right under Clause 8.9 is exercised exclusively through the DPA's audit measures (reports and questionnaires). This is a SPECIFIC_OVER_GENERAL superseding: Clause 8.9 states the general right to audit (including on-site inspection); DTA §8.4 is a specific provision in the same instrument that governs how that right is operationalized. However, a competing hierarchy argument exists: Clause 5 of the EEA SCCs states the SCCs prevail over related agreements in case of contradiction, and if restricting "on-site inspection" rights to reports-only is characterized as a contradiction, the SCCs' broader right would prevail over the DTA channeling provision. This conflict is flagged for human review. Under Stripe's intended reading, the governing language is the DPA's audit mechanism; under the SCC-prevails reading, the broader right (including on-site inspection with reasonable notice by User's appointed auditor) would apply.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "following User's written request, contribute to audits or inspections by making audit reports available to User. Following this request, and no more frequently than once annually, Stripe will promptly…"
2. "Upon written request, and no more frequently than annually, Stripe will complete a written data security questionnaire of reasonable scope and duration regarding Stripe's business practices and data t…"
3. "The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow …"

> *"User acknowledges and agrees that User exercises User's audit right under Clause 8.9 of Module 2 (Transfer:*

Controller to Processor) and/or Module 3 (Transfer: Processor to Processor) of the EEA SCCs by instructing Stripe, LLC to comply with the audit measures described in the DPA."
— Data Transfers Addendum

Publicity

AI Comment: The playbook's acceptable position requires User's prior consent before Stripe may use User's logo/marks for marketing purposes. The ideal preference further restricts any license to service-provision use only, unless prior written consent is obtained for broader use.

Stripe's General Terms §5.3 (Marks Usage) directly and materially conflict with both standards on the core marketing-consent issue:

Service-provision use (§5.3(a)): The mutual license grant limits each party's use of the other's Marks to "solely to provide the Services to User and to identify Stripe as User's service provider." This component is consistent with the ideal preference's carve-out for service-provision use.

Stripe's additional permitted uses (§5.3(b)): Stripe separately and unilaterally pre-grants itself the right to: (i) list User as a customer on Stripe webpages and apps; (ii) use User's Marks in "Stripe sales and marketing materials and communications"; and (iii) use User's Marks in promotional activities to which the parties agree in writing. Uses (i) and (ii) require **no prior consent from User**, directly contradicting the acceptable position. Use (iii) requires written agreement—this subset partially aligns with the acceptable position.

The usage-guidelines clause does not cure the conflict: Stripe is required to comply with any usage terms or guidelines User provides in writing, but this is optional (only "if any" are provided), and critically, it regulates *how* Stripe uses User's Marks once it elects to do so—it does not require User's affirmative consent *before* use for marketing or customer-listing purposes.

The pre-granted, consent-free license for (i) listing User on customer-identification pages and (ii) use in sales and marketing materials constitutes a direct conflict with the acceptable position. This is a High-weight item. The overall classification is RED.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Subject to this Agreement, each party (or its applicable Affiliates) grants to the other party a worldwide, non-exclusive, non-transferable (except as allowed under Section 11.10 (Assignment)), non-su…"
2. "Stripe and its Affiliates may use User's Marks:

(i) on Stripe webpages and apps that identify Stripe's customers or users;

(ii) in Stripe sales and marketing materials and communications; and

(iii)…"
3. "When using User's Marks, Stripe must comply with the usage terms or guidelines that User provides to Stripe in writing (if any)."

"Stripe and its Affiliates may refer to User as a user of Services in their financial disclosure documents."
— Stripe Services Agreement - General Terms

Password Encryption

AI Comment: The playbook item requires that passwords are always stored in encrypted form. This is a High-weight security control. The DPA Data Security Exhibit addresses the requirement through two complementary provisions that together satisfy the acceptable position.

First, Stripe commits to "ID/password security procedures, including stronger digital authentication measures based on NIST 800-63B including MFA." NIST SP 800-63B §5.1.1.2 explicitly mandates that memorized secrets (passwords) be stored using a suitable one-way key derivation function — in practice, a salted cryptographic hash — and prohibits plain-text or reversibly-encrypted password storage. This directly satisfies the playbook requirement that passwords be stored in cryptographically protected (encrypted/hashed) form. The reference to NIST 800-63B for password procedures is the most specific and probative provision.

Second, Stripe's encryption-at-rest commitment — AES-256 for all production data stored in server infrastructure — provides a universal cryptographic layer that encompasses any credential or password data held in Stripe's systems, independently confirming encrypted storage.

These two provisions are consistent and mutually reinforcing; neither supersedes the other.

Confidence is assessed as MODERATE rather than HIGH because: (a) no single clause contains an explicit statement such as "passwords are stored in hashed or encrypted form"; (b) the NIST 800-63B implication requires a step of inference (the playbook analyst must know that NIST 800-63B §5.1.1.2 mandates salted hashing); and (c) there is marginal ambiguity over whether these data-security obligations apply universally across all password types in scope for the review (e.g., Stripe account passwords, API keys, and any customer credential data Stripe processes on behalf of User). That said, the combined evidence is sufficiently clear and specific to support a GREEN classification for a High-weight item — the topic is

addressed, and the standard referenced exceeds the "encrypted form" threshold. No ideal preference was stated, so aiPreferenceMet remains false.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Encryption at rest. To protect data at rest, Stripe uses industry standard encryption (AES-256) to encrypt all production data stored in server infrastructure."

> *"ID/password security procedures, including stronger digital authentication measures based on NIST 800-63B including MFA"*
> — Data Processing Agreement
> *"Each party will maintain commercially reasonable administrative, technical, and physical safeguards designed to protect data in its possession or under its control from unauthorized access, accidental loss, and unauthorized modification. Stripe will comply with its obligations in the Data Security Exhibit to the DPA."*
> — Stripe Services Agreement - General Terms

Employee Offboarding Access

AI Comment: The playbook item requires the processor to have policies and systems ensuring employee access is offboarded or modified **within 24 hours** of termination or a job function change.

Stripe's DPA Data Security Exhibit expressly addresses this topic: it commits that upon "termination or applicable role change, [Stripe] promptly removes or updates Personnel access rights and requires Personnel to return or destroy Personal Data." The Technical Access Controls section of the same Exhibit further lists "change procedure" and "deletion procedure" as implemented access-control measures, and the General Terms §4.6 confirms Stripe's obligation to comply with the Data Security Exhibit.

This language substantively addresses the playbook requirement's subject matter—access removal upon termination or role change—but falls short of the acceptable position in one critical respect: **no specific maximum timeframe is contractually committed**. The playbook requires "in no event later than 24 hours," while Stripe only pledges "promptly," an undefined and non-enforceable time horizon. "Promptly" in a security context is generally understood to mean without unreasonable delay, but it does not guarantee compliance within the 24-hour outer bound the playbook requires, nor does it give the User a contractual enforcement right tied to that specific timeframe.

Because the topic is addressed (access offboarding upon termination/role change is covered) but the protection is weaker than the acceptable position (no 24-hour guarantee), this is YELLOW. For a High weight item, the absence of a specific, enforceable timing commitment is a meaningful gap—Stripe could theoretically argue that several days constitutes "promptly" under the terms as written. Human review is recommended to negotiate the addition of an explicit maximum timeframe, or to assess whether Stripe's standard security practices in practice satisfy the 24-hour threshold based on supplemental due diligence.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "differentiated access rights (profiles, roles, actions and objects);
access monitoring and logging;
access reports;
access procedure;
change procedure; and
deletion procedure."

> *"upon termination or applicable role change, promptly removes or updates Personnel access rights and requires Personnel to return or destroy Personal Data."*
> — Data Processing Agreement
> *"Stripe will comply with its obligations in the Data Security Exhibit to the DPA."*
> — Stripe Services Agreement - General Terms

Physical Security Controls

AI Comment: The playbook item requires the processor to maintain system controls and policies preventing unauthorized physical access. Stripe's documents satisfy this requirement comprehensively, primarily through the Data Security Exhibit appended to the DPA (Document 3), which contains a dedicated "Physical access controls" section explicitly enumerating the measures deployed.

The DPA Exhibit catalogues a substantial set of physical security measures, including: a physical access control system and program at Stripe premises; a 24×7 Global Security Operation Center monitoring physical security systems; security video and alarm systems; access control roles and area zones; access control audit measures; an electronic tracking and management program for keys; an access authorizations process for employees and third parties; electrified door locking; and trained uniformed security staff. Notably, Stripe hosts production infrastructure with reputable third-party data center providers and explicitly confirms it reviews third-party audit reports to verify those providers maintain appropriate physical access controls — a standard and industry-accepted delegation model with oversight.

Independent third-party validation of the physical security posture is corroborated by Stripe's PCI-DSS Level 1 certification (the highest level, confirmed annually by a qualified security assessor) and its annual SOC 1 and SOC 2 reports, both of which encompass physical security controls within their audit scope.

The General Terms Section 4.6 provides a further baseline contractual commitment: each party will maintain "commercially reasonable administrative, technical, and physical safeguards" to protect data from unauthorized access. This is supplemental and consistent with the more detailed DPA Exhibit language; there is no conflict between the two provisions.

Taken together, the DPA Data Security Exhibit, the supporting certification/audit framework, and the General Terms baseline safeguards clause fully satisfy the requirement that the processor has system controls and policies to prevent unauthorized physical access. The classification is GREEN. Confidence is HIGH: the relevant language is explicit, detailed, and directly on-point.

No ideal/preference was specified for this playbook item; aiPreferenceMet is therefore set to false, as there is no stated ideal threshold against which to confirm the vendor exceeds the acceptable position.

— Superseding reasoning —
The DPA Data Security Exhibit (Document 3) and the General Terms Section 4.6 (Document 1) both address physical safeguards and do not conflict — the DPA Exhibit elaborates with specific enumerated measures while the General Terms provide a general baseline. Per Section 7 of the DPA, "to the extent of any conflict between the provisions of this DPA and any provision of the Agreement regarding Personal Data Processing, the provisions of this DPA will prevail." No genuine conflict exists here, so no formal superseding determination is required; both provisions collectively support the GREEN finding, with the DPA Exhibit being the governing and more detailed authority on data processing physical security.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Stripe uses reputable third-party service providers to host its production infrastructure. Stripe relies on these third parties to manage the physical access controls to the data center facilities tha…"
2. "PCI Compliance. To the extent applicable to the Services, Stripe is responsible for providing the Services in a manner that is consistent with the highest certification level (PCI Level 1) provided by…"

> *"Each party will maintain commercially reasonable administrative, technical, and physical safeguards designed to protect data in its possession or under its control from unauthorized access, accidental loss, and unauthorized modification."*
> — Stripe Services Agreement - General Terms

Exclusivity

AI Comment: The acceptable position — no exclusivity accepted — is met for the described use case of payment processing for purchasing products. The Stripe Services Agreement does not impose exclusivity obligations on User in the core payment processing context. Critically, the license governing Stripe Technology (§2.1 General Terms) is explicitly granted as "non-exclusive," affirmatively confirming User's freedom to contract with and use alternative payment processors and technology providers simultaneously. The marks license (§5.3(a) General Terms) is likewise non-exclusive. Neither the General Terms nor the Stripe Payments Terms contain provisions requiring User to route all payment volume exclusively through Stripe, to refrain from engaging competing processors, or to satisfy minimum exclusivity-triggering volume commitments.

One material carve-out warrants proactive awareness: the Stripe Capital for Platforms Terms (§2.7) impose a conditional exclusivity — if User elects to offer Stripe Capital financing through its platform, User must process all payments for Financing Recipients (those with outstanding capital obligations) and active Prospects exclusively through Stripe Payments until those obligations are fully satisfied. This exclusivity is confined to a specific, optional, opt-in service (a financing/lending product for platforms) that falls outside the described use case of basic payment processing. It is not triggered by ordinary use of the Stripe Payments service. However, it exists within the Agreement framework and would become binding if User's relationship with Stripe expands to include Capital for Platforms services, making it a future-watch item.

No superseding logic is required. The GREEN classification applies to the described use case at the time of this review. The aiPreferenceMet field is set to false because no separate ideal preference was specified beyond the acceptable position; the finding confirms the acceptable threshold is met but there is no higher bar against which to assess preference attainment.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Subject to this Agreement, Stripe (or its Affiliates, as applicable) grants User a limited, worldwide, royalty-free, non-exclusive, non-transferable (except as allowed under Section 11.10 (Assignment)…"
2. "Subject to this Agreement, each party (or its applicable Affiliates) grants to the other party a worldwide, non-exclusive, non-transferable (except as allowed under Section 11.10 (Assignment)), non-su…"

> *"Except as otherwise permitted by Stripe in writing, User must use the Stripe Payments Services for (a) all Financing Recipients with outstanding obligations under a Stripe Capital Financing until those obligations have been fully satisfied, and (b) all Prospects whose eligibility for Stripe Capital Financing is then-currently under review."*
> — Stripe Services Agreement - Services Terms

Payment Terms

AI Comment: The playbook requires at least 30 days from receipt of invoice to pay fees, with a carve-out for credit card autopay (for which less than 30 days is acceptable). Stripe's General Terms address fee collection through three mechanisms: (1) automatic deduction from the User's Stripe Account balance, (2) charging the User's primary Payment Method (which may be a credit card), and (3) invoicing the User. The triggering obligation is simply that fees are payable "when due," but "when due" is not defined in the Agreement.

For the Stripe Payments service — the service relevant to this review — no explicit payment period (30-day or otherwise) is established in the General Terms or the Stripe Payments Service Terms for invoiced amounts. When Stripe elects to collect via credit card (option 2), that mechanism squarely satisfies the playbook's autopay carve-out. When Stripe deducts from the Stripe Account balance (option 1), fees are netted against transaction proceeds before settlement, which is functionally an immediate, automatic collection model and analogous to autopay in practical effect. However, when Stripe elects to invoice (option 3), the Agreement provides no defined payment period — meaning there is no contractual guarantee of even 30 days, which creates a gap against the acceptable position for invoiced amounts.

Notably, one service-specific provision within the Stripe Treasury for Platforms – Platform Terms (§6.3 Setoff) does provide explicit 30-day invoice payment terms: "User must pay the fees within 30 days after the date of the invoice." This demonstrates Stripe is capable of contractually committing to 30-day terms. However, this provision applies only to the Treasury for Platforms service and is not operative for the Stripe Payments / general payment processing engagement at issue here.

Overall classification is YELLOW because: (a) the credit card autopay and automatic balance-deduction mechanisms are acceptable under the playbook carve-out; (b) the invoicing mechanism lacks a defined payment period and does not guarantee the 30-day minimum required by the acceptable position; and (c) Stripe retains unilateral discretion to choose among collection methods, including invoicing without defined terms. The gap is material because there is no contractual protection against Stripe demanding immediate payment upon invoice issuance for any invoiced amounts. Confidence is MODERATE because Stripe's dominant fee collection model (automatic deduction from processing proceeds) makes traditional 30-day invoice terms structurally unusual for this vendor category, and the practical risk of an invoice-without-notice scenario is lower than in a conventional SaaS or professional-services billing context.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Stripe may collect all amounts owed by User by deducting them from User's Stripe Account balance, charging User's primary Payment Method (e.g., a credit card), or invoicing User for those amounts."
2. "RSP may deduct, recoup or setoff all fees User owes RSP (if any) from funds in User's Financial Account, even if this would cause an overdraft. Alternatively, RSP may invoice User for some or all of t…"

> *"Unless User and Stripe otherwise agree in writing or if Law requires, payment obligations are non-cancelable and Fees paid are non-refundable."*
> — Stripe Services Agreement - General Terms
> *"User must pay, or ensure that Stripe is able to collect, Fees, Taxes, and other amounts User owes to Stripe under this Agreement, or under any other agreement with a Stripe Entity, when due."*
> — Stripe Services Agreement - General Terms

Data Retention & Deletion

AI Comment: The Data Retention & Deletion playbook item has two threshold requirements: (1) the vendor must specify its retention and deletion practices, and (2) it must commit to deleting requested data from production systems within 30 days and cycling deleted data out of backups within 364 days. The ideal preference requires production deletion within 10 days.

Stripe addresses retention and deletion across four provisions, but no single provision — nor the provisions read together — satisfies the acceptable position's specific timing requirements.

DPA Section 3.1(h) [governing provision]: The most substantive deletion commitment. Stripe agrees to delete or return all Personal Data at User's choice following Agreement termination, with exceptions for legal retention requirements and DP Law. Two critical gaps relative to the acceptable position: (a) this obligation is triggered by Agreement termination, not by individual deletion requests made during the Term; and (b) no deletion timeline is specified — neither 30 days (acceptable threshold) nor 10 days (ideal preference). The exceptions for legal retention, post-termination obligations, and DP Law are broad and unquantified.

General Terms Section 4.4 [superseded by DPA]: Addresses post-Term retention from Stripe's angle — Stripe is not obligated to retain data post-Term except for legal or contractual reasons. This is a permissive framing (Stripe may not retain) rather than a protective obligation (Stripe must delete within X days). For Personal Data, DPA Section 3.1(h) supersedes this provision per DPA Section 7(a).

DPA Data Security Exhibit — Data Retention and Deletion: Confirms that Stripe "implements and maintains data retention policies and procedures related to Personal Data and reviews these policies and procedures as appropriate." This is an attestation of process existence, not a commitment to specific timelines. No deletion deadlines are stated.

Privacy Policy Section 5: Describes Stripe's actual operational retention practices and confirms data may be retained after account closure for legal obligations, fraud monitoring, tax reporting, financial partner contractual requirements, and payment method mandates. This broad multi-factor retention framework is consistent with the legal exceptions in DPA

Section 3.1(h) but reinforces that retention may extend well beyond 30 days in practice.

Classification: YELLOW. The topic is substantively addressed — Stripe is not silent — but the protections provided are materially weaker than the acceptable position requires. Specific deficiencies: (1) no 30-day production deletion timeline is stated anywhere; (2) no backup cycling commitment (364-day threshold) exists in any document; (3) the primary deletion commitment (DPA 3.1(h)) is linked to Agreement termination, not to in-Term deletion requests; (4) broad legal and compliance exceptions are unquantified and could substantially defer or prevent deletion. RED is not warranted because Stripe does make a substantive deletion commitment for Personal Data. The ideal preference (10-day production deletion) is clearly unmet. Weight is High !' YELLOW !' requires documented assessment by reviewing legal professional.

— Superseding reasoning —
DPA Section 7(a) explicitly provides that DPA provisions prevail over Agreement (General Terms) provisions where they concern Personal Data Processing. Accordingly, DPA Section 3.1(h) — which specifically governs Personal Data deletion obligations — supersedes General Terms Section 4.4, which addresses post-Term data retention more generally. Both provisions are YELLOW, so the superseding determination does not change the overall item classification, but it identifies DPA Section 3.1(h) as the governing contractual commitment for data deletion purposes.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "at User's choice, delete or return to User all Personal Data Processed in connection with the Services, and delete existing copies, following termination of the Agreement, except that Stripe will not …"

> *"Stripe is not obligated to retain data that it receives from or through User after the Term, except as (a) required by Law; (b) reasonably required for Stripe to perform any post-termination obligations; (c) this Agreement otherwise states; or (d) the parties otherwise agree in writing."*
> — Stripe Services Agreement - General Terms
> *"Stripe implements and maintains data retention policies and procedures related to Personal Data and reviews these policies and procedures as appropriate."*
> — Data Processing Agreement
> *"We retain your Personal Data for as long as we continue to provide the Services to you or our Business Users, or for a period in which we reasonably foresee continuing to provide the Services. Even after we stop providing Services directly to you or to a Business User that you're doing business with, and even after you close your Stripe account or complete a transaction with a Business User, we may continue to retain your Personal Data to:*
>
> *- Comply with our legal and regulatory obligations;*
> *- Enable fraud monitoring, detection, and prevention activities; and*
> *- Comply with our tax, accounting, and financial reporting obligations, including when such retention is required by our contractual agreements with our Financial Partners, and where data retention is mandated by the payment methods you've used."*
> — Privacy Policy

Employee Confidentiality Agreements

AI Comment: The playbook requires that Stripe's employees who access data must enter into written confidentiality agreements. The contract set addresses confidentiality obligations for personnel with data access across multiple documents, but does not explicitly require written individual employee confidentiality agreements.

The most relevant provisions are: (1) General Terms §6 requires that employees and others with access to Confidential Information be "subject to confidentiality obligations at least as protective as this Agreement" — but does not specify that these obligations must be memorialized in writing; (2) DPA §3.1(b) requires that all persons Stripe authorizes to process Personal Data be "committed to respecting the confidentiality of that Personal Data" — again without specifying written agreements; (3) the DPA Data Security Exhibit states that Personnel "acknowledge their data security and privacy responsibilities under Stripe's policies" — the "acknowledge" language implies some affirmative step (possibly written) but is not equivalent to an explicit written confidentiality agreement; and (4) the EEA SCCs (via the Data Transfers Addendum) require that persons authorized to process Personal Data have "committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality" — the "or statutory obligation" alternative is a meaningful deviation from the playbook requirement, as it permits Stripe to satisfy its obligation through employment law statutory duties rather than individual written agreements.

Collectively, the provisions address the substance of the requirement (employees with data access must have confidentiality obligations) but do not explicitly require those obligations to take the form of written agreements. The permissive "or statutory obligation" carve-out in the EEA SCCs further weakens the commitment relative to the playbook standard. This is YELLOW: the topic is addressed with real protections in place, but the specific written-agreement requirement is not explicitly satisfied. For a High weight item, this requires review and documented justification.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "The recipient may disclose Confidential Information only to its and its Affiliates' directors, employees, contractors, agents, professional advisors, and third-party auditors (and where Stripe is the …"
2. "All (a) Stripe employees; and (b) Stripe independent contractors who may have access to data, including those who Process Personal Data ((a) and (b), collectively " Personnel") acknowledge their data …"

> *"ensure that all persons Stripe authorizes to Process Personal Data are granted access to Personal Data on a need-to-*

know basis and are committed to respecting the confidentiality of that Personal Data"
— Data Processing Agreement
"It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality."
— Data Transfers Addendum

Governing Law

AI Comment: The playbook requires governing law to be one of: (1) Michigan, (2) Delaware, (3) New York, or (4) any jurisdiction with nexus. The Stripe Services Agreement comprehensively addresses governing law through a tiered architecture: §11.3 of the General Terms delegates the governing law question to the applicable Regional Terms, and §13.1 of each Regional Terms block specifies the controlling jurisdiction based on the User's Stripe Account Country.

For a US-based User — the most likely scenario given the intake brief (processing payments for purchasing "our product"), though the Stripe Account Country has not been confirmed — the applicable governing law is **California** (§13.1, US Regional Terms). California is not Michigan, Delaware, or New York. Whether California qualifies under the "any jurisdiction with nexus" prong depends on facts not available in the intake brief: specifically, whether the User has a California nexus through incorporation, operations, or domicile. Stripe, LLC is headquartered in San Francisco, CA, giving Stripe a California nexus, but the playbook's "nexus" language most naturally refers to a nexus for the contracting User. This creates genuine ambiguity that warrants human confirmation of the User's Stripe Account Country and business location.

For EEA-based users, the governing law is Ireland; for UK/Switzerland/Gibraltar users, England and Wales applies. Both are foreign commercial law jurisdictions that plainly do not meet any of the four acceptable positions for a non-EEA/UK User.

The Regional Terms prevail over the General Terms by express hierarchy (§13 preamble), so §13.1 for the applicable jurisdiction controls. Given the "Acceptable to Deviate" weight, the governing law deviation is informational and does not constitute a blocking concern. Classification is YELLOW because the topic is fully addressed but the applicable jurisdiction (California for US users, or foreign law for non-US users) does not clearly satisfy the acceptable threshold — the nexus prong could apply but remains unconfirmed. Human review should confirm the User's Stripe Account Country to resolve which Regional Terms §13.1 applies and whether that jurisdiction qualifies as a nexus jurisdiction under the playbook standard.

Note: The Data Transfers Addendum separately specifies Irish law for EEA Standard Contractual Clauses (Clause 17, Modules 1–3). That DPA-level governing law applies to data protection transfer mechanics only and is distinct from the governing law of the main commercial agreement analyzed here.

— Superseding reasoning —
Section 11.3 of the General Terms does not itself specify a jurisdiction; it delegates the governing law determination entirely to the applicable Regional Terms ("as specified in the Regional Terms"). The §13 preamble of the General Terms establishes an explicit document hierarchy: "If there is a conflict between the General Terms and the Regional Terms, the Regional Terms prevail." Accordingly, each jurisdiction-specific §13.1 Regional Terms block supplies the actual controlling governing law and supersedes §11.3's general reference for users in that jurisdiction. The superseding relationship is conditional on the User's Stripe Account Country: the US Regional Terms §13.1 governs for US users (California), the EEA Regional Terms §13.1 governs for EEA users (Ireland), and the UK/Switzerland/Gibraltar Regional Terms §13.1 governs for UK/CH/GI users (England and Wales). Multiple regional governing law clauses therefore simultaneously supersede §11.3 in their respective scopes, each on a DOCUMENT_HIERARCHY basis.

"This Agreement and any disputes between User and Stripe will be governed by, and construed in accordance with, the Governing Law as specified in the Regional Terms, without giving effect to its conflict of law principles."
— Stripe Services Agreement - General Terms
"The laws of the state of California are the Governing Law."
— Stripe Services Agreement - General Terms
"The laws of Ireland are the Governing Law."
— Stripe Services Agreement - General Terms
"The laws of England and Wales are the Governing Law."
— Stripe Services Agreement - General Terms
"If there is a conflict between the General Terms and the Regional Terms, the Regional Terms prevail."
— Stripe Services Agreement - General Terms

User Authentication Policies

AI Comment: The playbook item requires that the processor has policies for user authentication and password protection. Stripe's documentation satisfies this requirement substantively through its DPA Data Security Exhibit — which is explicitly incorporated by reference into the main Services Agreement via General Terms §4.1 ("Each party will comply with the DPA…which is incorporated into this Agreement by this reference") — and is further reinforced by General Terms §4.6.

Why GREEN: The DPA Security Exhibit contains four directly responsive elements:

1. **Technical Access Controls (authentication-specific):** Stripe explicitly lists "user identification and authentication procedures" and "ID/password security procedures, including stronger digital authentication measures based on NIST 800-63B including MFA" as implemented controls. The reference to NIST SP 800-63B — an established federal authentication standard covering identity proofing and authenticator assurance levels — confirms that Stripe's authentication policy is tied to a recognised, auditable industry framework. Additional controls include automatic blocking (password failure/timeout lockout) and break-in-attempt monitoring, indicating a layered authentication policy.

2. **Personnel authentication:** A separate provision confirms Stripe authenticates each personnel member through "strong passwords, token devices or biometrics," directly evidencing a password protection policy applied to Stripe's internal workforce.

3. **Formal documented policy framework:** The Security Exhibit confirms that Stripe maintains formally documented policies covering "access control" (among other topics) that are approved, internally published, communicated to relevant personnel, and reviewed at least annually. This satisfies the "has policies" framing of the playbook item — i.e., it is not merely ad hoc practice but institutionally documented and maintained policy.

4. **General Terms §4.6 contractual floor:** The main Agreement creates an overarching contractual commitment requiring Stripe to maintain "commercially reasonable administrative, technical, and physical safeguards" against unauthorized access, with an express cross-reference requiring Stripe to comply with its DPA Data Security Exhibit obligations.

No conflicts or ambiguities exist across the documents on this topic. All provisions are mutually reinforcing. The breadth of coverage — NIST-referenced MFA, password procedures, lockout controls, monitoring, formal documented policy lifecycle — goes beyond a minimal acceptable position and represents a strong, well-structured authentication posture. Classification is confidently GREEN.

Note: No ideal preference was specified for this playbook item; accordingly `aiPreferenceMet` is set to false as there is no stated ideal threshold against which to assess.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Stripe implements measures to prevent data processing systems from being used by unauthorized persons, including the following measures:
- user identification and authentication procedures;
- ID/pass…"
2. "Stripe authenticates each Personnel's identity through appropriate authentication credentials such as strong passwords, token devices or biometrics."
3. "The security program includes:
- documented policies that Stripe formally approves, internally publishes, communicates to appropriate personnel and reviews at least annually;
- documented, clear ass…"

> *"Each party will maintain commercially reasonable administrative, technical, and physical safeguards designed to protect data in its possession or under its control from unauthorized access, accidental loss, and unauthorized modification."*
> — Stripe Services Agreement - General Terms

Modification of Terms

AI Comment: The Modification of Terms playbook item (Weight: High) is addressed across multiple provisions in the Stripe Services Agreement, but the governing language falls short of both the ideal preference and—in a practical sense—the full acceptable position.

Acceptable Position Assessment:
The acceptable position requires (1) accessible modified terms with an updated effective date, and (2) that changes not take effect without being ascertainable.

Requirement (1) is technically met: Stripe posts revised terms on the Stripe Legal Page and the documents bear "Last modified" dates. Requirement (2) is met only in a narrow technical sense—changes are publicly posted and therefore theoretically ascertainable. However, the operative mechanism in §11.8 of the General Terms is that (a) modifications take effect "upon posting," (b) no advance proactive notice is required for general agreement modifications, and (c) User bears affirmative responsibility to monitor the Stripe Legal Page regularly. This structure means that changes can bind the User before the User has had any realistic opportunity to review them. The "ascertainable without proactive notice" dimension of the acceptable position is not meaningfully satisfied.

Two narrower provisions partially improve the picture: §7.1(c) provides at least 30 days' advance notice for fee increases and materially adverse subscription plan changes—meeting a higher standard for that category. Section 1.5(a) requires "reasonable notice" for modifications that would materially reduce service functionality, but this provision contains broad carve-outs (security risk, legal/regulatory compliance) that can eliminate notice entirely, and does not specify any minimum notice period.

Certain jurisdiction-specific Regional Terms (Australia §13.7; New Zealand §13.8) explicitly replace §11.8 with a stronger standard—at least 30 days' written notice for material or detrimental modifications—but these apply only to users in those jurisdictions. The pre-computed governing jurisdiction for this review is conditional; for US-based users (California law, most likely applicable given a US payment processing use case), the weaker general §11.8 governs.

Ideal Preference Assessment:
The ideal preference requires advance written notice and an opportunity to terminate with a pro-rata refund. This is not met:
- For general agreement modifications: No advance written notice is required; §11.8 permits modification by posting alone with immediate effect.

- For fee increases: 30 days' notice (§7.1(c)) satisfies the notice component but no refund right is attached.
- For service modifications: Only "reasonable notice" for material functionality reductions (§1.5(a)), no notice for other service changes, and no refund right.
- Pro-rata refund: Directly foreclosed by §7.1(b), which states that "payment obligations are non-cancelable and Fees paid are non-refundable."

Superseding Logic:
Section 7.1(c) (specific provision for fee/subscription modifications, 30-day notice) supersedes §11.8 (general modification clause) for fee-related changes, under the specific-over-general principle. Section 1.5(a) similarly governs material service functionality changes. Regional Terms §13.7/13.8 explicitly prevail over §11.8 for AU/NZ users per §13's override hierarchy. For all other agreement modifications in the most likely governing jurisdiction (US/California), §11.8 controls.

Overall: YELLOW — The item is addressed but with materially weaker protections than the acceptable position contemplates. The gap is significant enough for a High weight item: changes to the agreement (other than fee increases) can be imposed without advance notice; continued use constitutes acceptance; and no termination-with-refund right is available upon modification.

— Superseding reasoning —
Three superseding relationships exist within Document 1. First, §7.1(c) is a specific provision governing fee and subscription plan modifications (30-day advance notice), which supersedes the general modification clause at §11.8 for that narrower category—standard specific-over-general drafting principle. Second, §1.5(a) is a specific provision governing modifications to Services or Stripe Technology that materially reduce functionality, and similarly supersedes §11.8 for that sub-category. Third, the Regional Terms at §13.7 (Australia) and §13.8 (New Zealand) explicitly replace §11.8 for users in those jurisdictions, as confirmed by §1.394 which states Regional Terms prevail in the event of conflict with General Terms. For users governed by US/California law (the most likely jurisdiction given the intake brief), §11.8 remains the controlling provision for general agreement modifications because no US-specific regional modification improvement exists in the document set.

> *"Stripe may modify this Agreement (or any portion of it) at any time by posting a revised version of the modified portion(s) on the Stripe Legal Page or by notifying User. The modified Agreement is effective upon posting or as stated in the notice, if Stripe notifies User. By continuing to use Services after the effective date of any modification to this Agreement, User agrees to be bound by the modified Agreement. User is responsible for checking the Stripe Legal Page regularly for modifications to this Agreement. Except as this Agreement otherwise allows, this Agreement may not be modified except in writing signed by the parties."*
> — Stripe Services Agreement - General Terms
>
> *"Subject to the requirements of Law, Stripe may revise the Fees and Subscription Plans at any time. Stripe will provide User with at least 30 days notice (or longer period if Law requires) of any increase in a Fee or any new Fees for any Service provided to User, or any materially adverse change in a Subscription Plan."*
> — Stripe Services Agreement - General Terms
>
> *"Stripe may modify or discontinue any aspect of the Services or Stripe Technology, including imposing conditions on use of the Services or Stripe Technology or ceasing to offer a Service or Stripe Technology in a specific country or region. Stripe will provide User reasonable notice if the modification or discontinuation would materially reduce the functionality of a Service or Stripe Technology that User is then using, except where Stripe determines such notice would (i) create a security risk for Stripe; or (ii) cause Stripe (or its Affiliates, as applicable) to violate Law or breach an obligation to a Governmental Authority or Financial Provider."*
> — Stripe Services Agreement - General Terms
>
> *"Unless User and Stripe otherwise agree in writing or if Law requires, payment obligations are non-cancelable and Fees paid are non-refundable."*
> — Stripe Services Agreement - General Terms
>
> *"Subject to the requirements of Law, Stripe may reasonably modify this Agreement (or any portion of it) at any time by posting a revised version of the modified portion(s) on the Stripe Legal Page or by notifying User. For any material modifications to the Agreement, or modifications reasonably considered to be detrimental to User, Stripe will provide User with reasonable written notice of at least 30 days (or longer period if Law requires). The modified Agreement is effective upon posting or as stated in the notice, if Stripe notifies User as specified above. For the avoidance of doubt, User may terminate the Agreement at any time under Section 10.1(a)(i) (Termination for Convenience). By continuing to use Services after the effective date of any modification to this Agreement, User agrees to be bound by the modified Agreement. Except as this Agreement otherwise allows, this Agreement may not be modified except in writing signed by the parties."*
> — Stripe Services Agreement - General Terms

Insurance

AI Comment: The entire document set — comprising the Stripe Services Agreement (General Terms), Services Terms (including all product-specific terms), the Data Processing Agreement, the Data Transfers Addendum, the Prohibited and Restricted Businesses list, and the Privacy Policy — is entirely silent on Stripe (the vendor) maintaining any form of insurance coverage. There is no representation, warranty, or covenant anywhere in the agreement suite that Stripe carries general liability, errors and omissions, cyber liability, professional indemnity, or any other class of insurance.

The sole insurance reference across the full document set appears in the Financial Connections Security Addendum, but it is directed at the User — not at Stripe. That clause obligates the User to "Maintain a level of insurance that is reasonable based on the risk associated with User's collection, use, retention and disclosure of Connections Data." This actually underscores the asymmetry: Stripe imposes an insurance obligation on the User but makes no corresponding commitment about its own coverage.

Under the silence-handling decision framework, a silent "Acceptable to Deviate" item defaults to YELLOW. No downgrade to GREEN is warranted here: while it is standard market practice for large SaaS/payment vendors to omit insurance disclosures from their standard terms (insurance is ordinarily verified separately through a certificate of insurance request), the industry norm applies to the form of disclosure, not to the underlying adequacy of coverage. Without any contractual representation or independent documentation, we cannot affirm that the acceptable position is met.

Given the "Acceptable to Deviate" weight, this finding does not rise to a blocking or high-priority issue, and the practical risk is mitigated by Stripe's status as a heavily regulated financial services entity subject to ongoing regulatory capital and operational requirements across multiple jurisdictions (Central Bank of Ireland, UK FCA, and others). However, if insurance verification is required, the appropriate path is to request a certificate of insurance from Stripe directly outside of these standard terms. The item is classified YELLOW rather than RED in recognition of the low weight and the regulatory oversight context.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Maintain a level of insurance that is reasonable based on the risk associated with User's collection, use, retention and disclosure of Connections Data"

Disaster Recovery Testing

AI Comment: The playbook item requires two distinct elements: (1) the existence of disaster recovery AND business continuity plans, and (2) regular testing of those plans at least once annually. The Stripe DPA Data Security Exhibit partially addresses element (1) by confirming the existence of a "disaster recovery plan" under the Availability Controls section, alongside backup procedures, database replication, and hardware redundancy. However, a standalone "business continuity plan" is not mentioned as a distinct construct anywhere in the provided documents. More critically, element (2) — the testing obligation — is entirely absent from explicit contractual language directed at DR/BC plans. The DPA Security Programs section mentions "regular testing of the key controls, systems and procedures," but this is generic security program language and cannot reasonably be read as a specific commitment to test disaster recovery or business continuity plans. Indirect evidence of DR-adjacent testing exists through Stripe's contractual commitments to PCI-DSS Level 1 compliance (confirmed annually by a QSA) and SOC 2 reporting (produced annually); both frameworks require some form of availability/recovery control testing. However, these are compliance attestation references, not explicit contractual obligations to conduct DR/BC plan testing at least annually, and they do not contractually bind Stripe to a testing cadence visible to the User. Classification is YELLOW: the topic is partially addressed (DR plan confirmed, indirect evidence of compliance-framework testing) but materially falls short of the acceptable position — no explicit commitment to test DR/BC plans, no stated frequency, and business continuity planning is not explicitly addressed. For a HIGH-weight item, the absence of an explicit contractual testing obligation is a meaningful gap.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Stripe implements measures to ensure the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, including:
- database repl…"
2. "The security program includes:
- documented policies that Stripe formally approves, internally publishes, communicates to appropriate personnel and reviews at least annually;
- documented, clear ass…"
3. "PCI Compliance. To the extent applicable to the Services, Stripe is responsible for providing the Services in a manner that is consistent with the highest certification level (PCI Level 1) provided by…"

> *"Each party will maintain commercially reasonable administrative, technical, and physical safeguards designed to protect data in its possession or under its control from unauthorized access, accidental loss, and unauthorized modification. Stripe will comply with its obligations in the Data Security Exhibit to the DPA."*
> — Stripe Services Agreement - General Terms

Termination for Cause

AI Comment: The acceptable position — that the User can terminate the agreement if the Vendor (Stripe) breaches — is expressly and unambiguously satisfied by Section 10.1(a)(ii) of the General Terms. That provision grants User the right to terminate immediately upon notice to Stripe if Stripe materially breaches the Agreement, with a 10-day cure window for curable breaches. This aligns directly with the playbook's stated requirement.

No ideal preference was specified for this item, so aiPreferenceMet is set to false — not because the provision is deficient, but because there is no stated ideal threshold against which to measure whether it is exceeded.

Contextual notes worth flagging for the reviewing attorney: (1) The 10-day cure period is on the shorter side compared to the 30-day period commonly seen in enterprise SaaS agreements, but for a payment-processing relationship this compressed timeline is market-standard and generally favors the User in terms of speed of exit; (2) Stripe separately reserves a broad right to terminate the User for convenience at any time with notice per Section 10.1(b)(ii)(1) — this asymmetry is common in payment-processor relationships and noted here for completeness, though it falls outside the scope of this item; (3) The weight of this item is "Acceptable to Deviate," meaning even if the provision were absent, only an informational comment would be required. Since the right is explicitly present, the finding is GREEN with HIGH confidence.

> *"User may terminate this Agreement immediately upon notice to Stripe if Stripe materially breaches this Agreement and, if capable of cure, does not cure the breach within 10 days after receiving notice specifying the breach."*

— Stripe Services Agreement - General Terms

Cyber Risk Insurance

AI Comment: The entire Stripe document set—General Terms, all Service Terms, the DPA (including the Data Security Exhibit), the Data Transfers Addendum, the Prohibited and Restricted Businesses list, and the Privacy Policy—is completely silent on Stripe's obligation to maintain, or its actual maintenance of, any form of cyber risk insurance. No provision addresses: (a) whether Stripe carries cyber risk insurance at all; (b) coverage limits; (c) naming the User as an additional insured; or (d) a waiver of subrogation in favor of the User. The only insurance reference found across all documents is in the Financial Connections Security Addendum (Document 2), which imposes an insurance obligation on the *User*, not on Stripe ("Maintain a level of insurance that is reasonable based on the risk associated with User's collection, use, retention and disclosure of Connections Data"). This is directionally inverse to the playbook item's requirement.

Silence classification: The item weight is Medium, so the default silence classification is YELLOW. A statutory downgrade was evaluated: no applicable statute (GDPR, CCPA, PCI-DSS, or other law referenced in the documents) mandates a vendor to maintain cyber risk insurance of a specified amount or to name counterparties as additional insureds, so no statutory downgrade applies. An industry-norm downgrade was also evaluated: while it is common market practice for large enterprise vendors to carry cyber insurance and to address it outside standard T&Cs (via Certificate of Insurance during procurement), the absence of any attestation here means coverage, limits, additional-insured status, and subrogation waiver cannot be confirmed from the provided documents. Because the User cannot verify even the threshold requirement—let alone the ideal preferences—the industry-norm downgrade to GREEN is not warranted. The classification remains YELLOW.

Practical context: Stripe is PCI-DSS Level 1 certified, maintains SOC 1 and SOC 2 reports, is regulated as an electronic money institution in the EU and UK, and carries extensive data security obligations under its DPA. These factors are consistent with (but do not confirm) professional insurance coverage. The appropriate remediation step is to request a Certificate of Insurance and, if required, negotiate an additional-insured endorsement and waiver of subrogation through the procurement process—provisions that are not achievable through review of the public-facing standard agreements alone.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Maintain a level of insurance that is reasonable based on the risk associated with User's collection, use, retention and disclosure of Connections Data"

Processing Location Restrictions

AI Comment: The playbook requirement has two alternative prongs: (A) all processing occurs in the US, Canada, or EU; or (B) processing is completed under Standard Contractual Clauses (SCCs). The Stripe contract documents substantially address both prongs but fall short of fully satisfying either.

Prong A — Geographic Restriction: Primary processing for US/Americas-based users is confirmed to occur with Stripe, LLC in the United States (DPA §3.9, §6.1), and EU users are served by Stripe Payments Europe, Limited. This satisfies the US and EU prongs for the primary processing relationship. However, the DPA expressly reserves Stripe's right to "transfer Personal Data on a global basis as necessary to provide the Services" including to "Sub-processors in other jurisdictions" (DPA §6.2). The Privacy Policy explicitly confirms India as an identified processing location in two places — in the international transfers section ("including the United States and India") and in the service provider disclosure ("The majority of our service providers are based in the European Union, the United States of America, and India"). India is outside the US/Canada/EU scope. No geographic restriction limiting processing to approved jurisdictions is imposed, and the contract expressly contemplates processing beyond those jurisdictions.

Prong B — SCCs: The Data Transfers Addendum (DTA) contains comprehensive Standard Contractual Clauses — all three Modules of the EU SCCs (Controller-to-Controller, Controller-to-Processor, Processor-to-Processor), the UK International Data Transfer Addendum, Swiss modifications, CBPR/PRP certifications, and Brazilian SCCs. Stripe, LLC is also certified under the EU-US Data Privacy Framework. These mechanisms provide robust SCC coverage for EEA, UK, Swiss, and Brazilian personal data transferred to Stripe in the US. However, these SCCs are scoped to transfers from those specific regulated jurisdictions to Stripe, LLC in the US — they do not explicitly establish SCCs for Stripe's onward transfers to Indian sub-processors or other globally distributed processors. The DPA's sub-processor framework (§3.2) requires "comparable obligations" from sub-processors but stops short of mandating SCCs specifically. The Privacy Policy uses conditional language ("when mandated by applicable law") when referencing transfer mechanisms — confirming that SCCs and equivalent tools are deployed selectively where legally required, not universally across all processing locations.

Overall: YELLOW. The contract addresses data transfer governance with substantial, industry-leading protections (a complete and detailed DTA, the DPF, and a sub-processor framework), but the India processing gap — explicitly disclosed in the Privacy Policy without clearly documented SCC governance for that specific leg — means the acceptable position is not fully met under either prong. The classification is YELLOW rather than RED because the topic is substantively addressed and real protections exist; it is YELLOW rather than GREEN because processing demonstrably extends beyond US/Canada/EU, and the SCCs framework does not universally cover all identified processing paths.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Stripe and its Affiliates may transfer Personal Data on a global basis as necessary to provide the Services. In particular, Personal Data may be transferred to Stripe, LLC in the United States and to …"

2. "Each party will comply with the DPA, including the Data Transfers Addendum, which is incorporated into this Agreement by this reference."

"If User's Stripe Account is located in North America or South America, User enters this DPA with Stripe, LLC."
— Data Processing Agreement

"User acknowledges that in order for Stripe to provide the Services, User transfers Personal Data to Stripe, LLC in the United States."
— Data Processing Agreement

"As a global business, it's sometimes necessary for us to transfer your Personal Data to countries other than your own, including the United States and India."
— Privacy Policy

"The majority of our service providers are based in the European Union, the United States of America, and India."
— Privacy Policy

"Module 1 (Transfer: Controller to Controller), Module 2 (Transfer: Controller to Processor) and Module 3 (Transfer: Processor to Processor) of the EEA SCCs, each as completed and supplemented as set out in this Data Transfers Addendum, apply to a transfer by User to Stripe, LLC of Personal Data that is subject to DP Law in the EEA and Processed under User's DPA."
— Data Transfers Addendum

"The UK International Data Transfer Addendum, completed and supplemented according to this Data Transfers Addendum, applies to a transfer by User to Stripe, LLC of Personal Data that is subject to DP Law in the United Kingdom and Processed under User's DPA."
— Data Transfers Addendum

"Stripe, LLC is self-certified under the Data Privacy Framework. When User transfers Personal Data originating from the EEA, the UK or Switzerland to Stripe in the United States, Stripe, LLC will receive the Personal Data under the Data Privacy Framework and, when processing that Personal Data, will comply with the data privacy principles and relevant supplemental principles set out in the Data Privacy Framework."
— Data Transfers Addendum

"Stripe will enter into a written agreement with each Sub-processor that imposes on that Sub-processor obligations comparable to those imposed on Stripe under this DPA, including the obligation to implement appropriate Data Security Measures. If a Sub-processor fails to fulfill its data protection obligations under that agreement, Stripe will remain liable to User for the acts and omissions of its Sub-processor to the same extent Stripe would be liable if performing the relevant Services directly under this DPA."
— Data Processing Agreement

Encryption at Rest

AI Comment: Stripe's DPA Data Security Exhibit explicitly and unambiguously states: "To protect data at rest, Stripe uses industry standard encryption (AES-256) to encrypt all production data stored in server infrastructure." This directly satisfies the playbook's acceptable position — AES-256 bit (or then-current industry standard) encryption at rest — with no interpretive gap. The DPA is contractually binding on both parties because General Terms §4.1 expressly incorporates it: "Each party will comply with the DPA, including the Data Transfers Addendum, which is incorporated into this Agreement by this reference." AES-256 protection is further confirmed for sensitive payment card and banking data in a segregated vault. The Data Transfers Addendum §7.1 supplies a supplementary commitment that "Personal Data will be encrypted both in transit and at rest," though it does not specify the cipher — this provision is scoped within the Supplemental Clauses to the EEA SCCs and applies primarily to EEA transfer contexts. General Terms §4.6 provides a general "commercially reasonable safeguards" commitment, which alone would be insufficient to confirm AES-256; it is superseded in specificity for encryption-at-rest analysis by the DPA Exhibit (specific-over-general). The operative governing text is the DPA Exhibit's AES-256 statement, which applies globally across all data processed under the Agreement regardless of the Account Country. No ideal preference was separately specified beyond the requirement; because the contract text expressly matches the stated standard (AES-256), aiPreferenceMet is set to true. Confidence is HIGH: the language is precise, contractually binding, and directly on-point.

— Superseding reasoning —
The DPA Data Security Exhibit (PIF index 0) provides the specific AES-256 encryption-at-rest commitment and supersedes the General Terms §4.6 (PIF index 4), which only requires "commercially reasonable administrative, technical, and physical safeguards" without specifying an encryption standard. Under general contract drafting principles, specific provisions control over general ones; §4.6 standing alone could not confirm the AES-256 standard. The DPA Exhibit is the operative governing text for this item.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Stripe applies data encryption mechanisms at multiple points in Stripe's service to mitigate the risk of unauthorized access to Stripe data at rest and in transit."
2. "Each party will comply with the DPA, including the Data Transfers Addendum, which is incorporated into this Agreement by this reference."

"To protect data at rest, Stripe uses industry standard encryption (AES-256) to encrypt all production data stored in server infrastructure."
— Data Processing Agreement

"Payment card and bank numbers are separately encrypted using industry standard encryption (AES-256) at the data level and stored in a separate data vault that is highly restricted."
— Data Processing Agreement

"Personal Data will be encrypted both in transit and at rest using encryption technology by Stripe, LLC."
— Data Transfers Addendum

> *"Each party will maintain commercially reasonable administrative, technical, and physical safeguards designed to protect data in its possession or under its control from unauthorized access, accidental loss, and unauthorized modification."*
> — Stripe Services Agreement - General Terms

Encryption in Transit

AI Comment: The playbook item requires encryption in transit using TLS 1.2 or higher, or then-current industry-standard transport encryption. Stripe's DPA Exhibit (Stripe Data Security — "Encryption in transit") explicitly states that "Stripe requires all inbound and outbound data connections to be encrypted using the TLS 1.2 protocol," and additionally that internal production networks use mTLS. This language precisely tracks the acceptable position — TLS 1.2 is named by protocol version, satisfying the requirement without any ambiguity or need for interpretation.

The DPA is contractually binding because it is incorporated by reference into the SSA via Section 4.1 of the General Terms: "Each party will comply with the DPA … which is incorporated into this Agreement by this reference." The DPA's own conflict clause (Section 7) further provides that the DPA prevails over conflicting Agreement provisions on Personal Data processing matters.

Additional corroboration comes from: (1) the general encryption statement in the DPA Exhibit ("Stripe applies data encryption mechanisms at multiple points … at rest and in transit"); (2) Stripe Payments Terms Section 3.7, which commits Stripe to PCI-DSS compliance — PCI-DSS mandates TLS 1.2 or higher for cardholder data in transit; and (3) General Terms Section 4.6, which requires each party to maintain "commercially reasonable … technical … safeguards."

No conflicting provisions exist across the document set. All references are consistent and mutually reinforcing. The governing, most specific provision is the DPA Exhibit. Classification is GREEN at HIGH confidence. aiPreferenceMet is false because no ideal preference was specified in the playbook item — the acceptable threshold is met, but there is no stated ideal to evaluate against.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "For data traversing Stripe's internal production networks, Stripe uses mTLS to encrypt connections between production systems."
2. "Stripe applies data encryption mechanisms at multiple points in Stripe's service to mitigate the risk of unauthorized access to Stripe data at rest and in transit."
3. "Each party will comply with the DPA, including the Data Transfers Addendum, which is incorporated into this Agreement by this reference."

> *"To protect data in transit, Stripe requires all inbound and outbound data connections to be encrypted using the TLS 1.2 protocol."*
> — Data Processing Agreement
> *"Each party will maintain commercially reasonable administrative, technical, and physical safeguards designed to protect data in its possession or under its control from unauthorized access, accidental loss, and unauthorized modification."*
> — Stripe Services Agreement - General Terms
> *"Stripe provides the Services in a manner consistent with PCI-DSS requirements that apply to Stripe."*
> — Stripe Services Agreement - Services Terms

No AI/ML Training on Our Data

AI Comment: **Preliminary Note — Item Naming Discrepancy:** This playbook item is labeled "Business Continuity" but its description addresses AI/ML data training restrictions—a data-use governance concern, not continuity/uptime. This appears to be a naming error in the Review Specific Playbook. The analysis below is conducted strictly against the stated acceptable position and ideal preference as described.

Finding: RED — Critical

The acceptable position requires that Stripe may not use User data (including Personal Data and Confidential Information) to train or improve AI/ML models, except for models used solely for User. The ideal preference goes further: no use of User data for any purpose beyond providing the contracted services.

The Stripe document set directly and explicitly contradicts both the acceptable position and the ideal preference across multiple independent provisions:

1. Broad Content License (General Terms § 5.1(c)): Stripe is granted a *perpetual, worldwide, irrevocable, royalty-free* license to use all "Content" that User provides—defined as non-Personal Data text, images, and data User uploads or provides in connection with the Services—to "develop, improve, and provide Services and Stripe Technology and for Stripe's internal business purposes." The "develop, improve" language expressly encompasses AI/ML model training and improvement. Critically, this license inures to Stripe's entire platform (and its Affiliates), not exclusively to models used for User. The irrevocable and perpetual nature means even contract termination does not extinguish this right.

2. Explicit Fraud Model Training (Stripe Payments Terms § 3.8): Stripe explicitly reserves the right to incorporate User's behavioral data (actions and inactions in response to fraud signals) into "Stripe's fraud and verification model"—a platform-

wide model serving the entire Stripe network. This is textbook AI/ML training on User data for Stripe's general benefit, not a model used solely for User. This directly contradicts the acceptable position.

3. DPA Data Controller Purposes: The DPA expressly identifies "analyze, improve and develop Stripe's products and services" as a purpose for which Stripe processes Personal Data in its capacity as Data Controller. Stripe operates simultaneously as both Data Processor (acting on User's behalf) and Data Controller (acting on its own authority) for the same underlying data. In the Data Controller role, Stripe's AI/ML model training using User-associated Personal Data is explicitly authorized.

4. Privacy Policy Confirmation: Stripe's Privacy Policy independently confirms "Training artificial intelligence models to power our Services and protect against fraud and other harm" as a stated use of Personal Data collected across its services. This is not a hypothetical—it is confirmed operational practice.

5. Partial (Jurisdiction-Limited) Mitigation: The DPA's CCPA-specific provision (§ 3.3) restricts Stripe in its processor capacity from combining Personal Data from User with data from other sources or using it outside its direct business relationship with User. However, this protection is narrow: (a) it applies only in California-governed contexts; (b) it does not constrain Stripe's simultaneously-operative Data Controller role, where AI training is explicitly permitted; (c) it does not address User's non-Personal Data Content, which is covered by the broad irrevocable license in § 5.1(c); and (d) it does not address Confidential Information.

Confidential Information Gap: The Confidentiality section (General Terms § 6) restricts *disclosure* of Confidential Information to third parties but does not restrict Stripe's internal *use* of Confidential Information for AI/ML training. Combined with the Content license, Stripe could use User-provided Confidential Information internally for model development while complying with the confidentiality clause (so long as it does not disclose it externally).

Conclusion: Multiple explicit, independent provisions permit Stripe to use User data—including Content, behavioral data, and Personal Data (in Data Controller capacity)—to train and improve platform-wide AI/ML models. This is a direct, unambiguous conflict with the acceptable position. The ideal preference (no use beyond service provision) is even more clearly unmet given the perpetual Content license and platform-wide fraud model training. At Critical weight, this finding is a blocking issue requiring Board approval and documented exception if the relationship is to proceed.

— Superseding reasoning —
The DPA's CCPA-specific processor restriction (§ 3.3) and the General Terms' Content license (§ 5.1(c)) operate on different data categories and do not conflict with one another in a superseding sense—they address Personal Data in the processor role vs. non-Personal Content respectively. The DPA's Section 7 conflict rule states DPA terms prevail over Agreement terms for Personal Data processing conflicts; however, the DPA itself does not restrict Stripe's Data Controller uses of Personal Data (it expressly authorizes them), so there is no internal DPA conflict to resolve. The General Terms § 11.9 Order of Precedence (Service Terms > General Terms > incorporated terms) does not resolve the AI-training issue because none of the higher-precedence Service Terms restrict AI/ML training—the Payments Terms § 3.8 affirmatively authorizes it. No superseding determination changes the overall RED classification.

— Note —
The AI cited 6 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "User grants to Stripe, on behalf of itself and its Affiliates, a perpetual, worldwide, non-exclusive, irrevocable, royalty-free license to use the Content to develop, improve, and provide Services and…"
2. ""Content" means all text, images, and other data (excluding Personal Data) or information that Stripe does not provide to User and that User uploads, publishes, uses, or provides to Stripe in connecti…"
3. "If Stripe provides User with information regarding the possibility or likelihood that a transaction may be fraudulent or that an individual cannot be verified, Stripe may incorporate User's subsequent…"
4. "When Stripe Processes Personal Data as a Data Controller it:
- has the sole and exclusive authority to determine the purposes and means of Processing Personal Data it receives from or through User; a…"
5. "The purposes of Stripe's Processing of Personal Data in its capacity as a Data Controller when providing Stripe's products and services are to:
- determine and utilize third parties (banks and payment…"
6. "Stripe will not (except to provide Stripe's services as permitted by Law): (a) sell or share (as defined under the CCPA) Personal Data; (b) retain, use or disclose Personal Data outside of its direct …"

> *"Training artificial intelligence models to power our Services and protect against fraud and other harm."*
> — Privacy Policy

> *"Analyzing and drawing inferences from Transaction Data to reduce costs, fraud, and disputes and increase authentication and authorization rates for Stripe and our Business Users."*
> — Privacy Policy

Data Ownership

AI Comment: The playbook item requires that, as between the parties, all Personal Data remains the sole property of User's company. Stripe's terms fail to satisfy this requirement in multiple independently dispositive ways.

Critical failure — Stripe as independent Data Controller: The DPA (Section 2) expressly establishes Stripe as a Data Controller for significant categories of Personal Data processing, holding "sole and exclusive authority to determine the purposes and means of Processing Personal Data it receives from or through User." A Data Controller's exclusive decisional authority over the purposes and means of processing is structurally incompatible with User holding "sole property" over that data. A property owner, by definition, may control and exclude others from use of their property — yet here Stripe retains independent, exclusive authority over Personal Data for Stripe's own purposes.

Stripe uses Personal Data for its own commercial benefit: In its Data Controller capacity, Stripe's stated purposes expressly include "analyze, improve and develop Stripe's products and services" (DPA Section 2, Data Processing Purposes). This is a use of Personal Data for Stripe's own business advantage — directly inconsistent with User's "sole property" claim.

Stripe claims IP ownership over data derived from the Services: General Terms §5.1(a) asserts that Stripe owns all IP Rights in "Stripe Data," which is defined to include "(b) information Stripe uses for security or fraud prevention; and (c) all aggregated information Stripe generates from the Services" (§12 Definitions). Both categories are derived from or related to Personal Data processed through the platform. Stripe's IP ownership claim over these categories is in direct tension with User asserting "sole property" in the underlying Personal Data.

No express ownership grant to User: Neither the General Terms nor the DPA contains any provision expressly stating that Personal Data is the sole property of User. The IP ownership clause (§5.1(a)) contains "as between the parties" language — but it runs in favor of Stripe (for Stripe Data), not User (for Personal Data). There is simply no affirmative ownership grant to User.

Stripe's Privacy Policy confirms independent controller use in practice: Stripe "use[s] End Customers' Personal Data for Stripe's own purposes such as enhancing security; offering, personalizing, and improving our Business Services; and preventing fraud, loss, and other damages" (Privacy Policy §1.2), confirming the independent controller role is operationally active.

Partial mitigants — insufficient to cure the fundamental gap: (a) For processing performed in Stripe's Processor capacity, Stripe acts "on behalf of User, the Data Controller" (DPA §2) — consistent with User directing that processing. However, this applies only to Processor-mode activities; the independent Data Controller role co-exists and is not displaced. (b) The "Content" definition expressly excludes Personal Data (§12), meaning the broad perpetual, irrevocable content license in §5.1(c) does not extend to Personal Data — this is favorable but does not affirmatively establish User's ownership, and does not curtail Stripe's independent Controller-mode use.

DPA hierarchy: Per DPA §7, the DPA prevails over the Agreement (including General Terms) for Personal Data processing questions, making the DPA's dual controller/processor framework the controlling legal framework for Personal Data rights.

The gap between the acceptable position (sole property in User) and Stripe's terms (Stripe as independent Data Controller with exclusive authority, plus IP ownership in data derived from Services) is fundamental and irreconcilable without contractual modification. This is a Critical-weight RED finding — blocking, requiring Board approval and documented exception to proceed.

— Superseding reasoning —
The DPA explicitly prevails over the Agreement on Personal Data Processing matters (DPA §7). This means the DPA's framework — establishing Stripe as both Data Processor (acting on User's behalf for some processing) and independent Data Controller (with "sole and exclusive authority" over purposes and means for other processing) — is the controlling legal framework for Personal Data ownership and control questions, superseding any General Terms provisions that might otherwise be read to affect data rights. Specifically, the General Terms IP ownership clause (§5.1(a)) asserts Stripe's IP rights in "Stripe Data," which includes data derived from the Services (aggregated data, security/fraud-prevention data). Questions about which framework governs data rights are resolved in favor of the DPA, as the DPA is the specific instrument addressing Personal Data and it expressly prevails. The governing outcome after applying this hierarchy is that Stripe holds independent Data Controller authority over significant portions of Personal Data, irreconcilable with User's "sole property" claim.

— Note —
The AI cited 7 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "When Stripe Processes Personal Data as a Data Controller it:
- has the sole and exclusive authority to determine the purposes and means of Processing Personal Data it receives from or through User; a…"
2. "The purposes of Stripe's Processing of Personal Data in its capacity as a Data Controller when providing Stripe's products and services are to:
- determine and utilize third parties (banks and payment…"
3. "To the extent of any conflict between the provisions of this DPA and any provision of the Agreement regarding Personal

Data Processing, the provisions of this DPA will prevail."
4. "'Stripe Data' means data that User obtains via the Services, including (a) information relating to the Stripe API interactions via the Stripe Technology; (b) information Stripe uses for security or fr…"
5. "'Content' means all text, images, and other data (excluding Personal Data) or information that Stripe does not provide to User and that User uploads, publishes, uses, or provides to Stripe in connecti…"
6. "User grants to Stripe, on behalf of itself and its Affiliates, a perpetual, worldwide, non-exclusive, irrevocable, royalty-free license to use the Content to develop, improve, and provide Services and…"
7. "Where allowed, we also use End Customers' Personal Data for Stripe's own purposes such as enhancing security; offering, personalizing, and improving our Business Services; and preventing fraud, loss, …"

> *"When Stripe Processes Personal Data as a Data Processor, it is acting as a Data Processor on behalf of User, the Data Controller."*
> — Data Processing Agreement
> *"As between the parties, Stripe, its Affiliates, and its third party licensors own all IP Rights in the Services, the Stripe Technology, Stripe Data, the Stripe Marks, the Documentation, and the Stripe Website."*
> — Stripe Services Agreement - General Terms

Authorized Equipment & Software

AI Comment: The playbook item requires two distinct controls: (1) employees process client data only on authorized business equipment, and (2) unauthorized hardware and software are prevented from being installed on data-processing systems. Stripe's DPA Security Exhibit and the General Terms provide partial but incomplete coverage of both requirements.

For the **unauthorized software / configuration control** prong, the DPA Security Exhibit's "System Configuration" section is the strongest finding: Stripe describes infrastructure managed as code through formal change control with two-party approvals, deployment automation, and monitoring against "known configuration baselines." This constitutes meaningful control over unauthorized software changes on production infrastructure, though it is scoped to "production infrastructure" rather than all systems that may process User's data.

For the **authorized equipment only** prong, the DPA Security Exhibit references "policies covering, as applicable, acceptable computer use…removable media and remote access" as part of Stripe's security program. This confirms such policies exist and are part of the personnel acknowledgment framework, but the DPA does not elaborate what those policies require — in particular, there is no explicit statement that employees may process client data only on employer-issued or -approved devices. The Network and Operations Management section adds hardening, malware protection, and change control as related but non-specific controls.

The General Terms Section 4.6 commits to "commercially reasonable administrative, technical, and physical safeguards," which would encompass authorized-equipment and software controls as a matter of standard practice, but this is a general-standard clause rather than an explicit control description.

PCI-DSS Level 1 compliance (confirmed in Services Terms § 3.7 and DPA Exhibit) implicitly covers authorized-software requirements for cardholder data environments under PCI-DSS Requirements 6 and 12, but this is scoped to Stripe's card-processing systems and does not directly confirm enterprise-wide endpoint controls.

Net assessment — YELLOW (High weight): The topic is addressed — it is not silent — but with material gaps. The production-systems software configuration controls are well-evidenced. The authorized-equipment-only requirement for personnel is supported only by a policy-existence reference and a general personnel-acknowledgment clause; no explicit restriction on unauthorized device use for processing is stated. For a High weight item, this incomplete coverage warrants YELLOW and requires review and documented assessment before acceptance.

— Note —
The AI cited 4 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Stripe maintains and enforces a security program that addresses how Stripe manages security, including its security controls. The security program includes:
- documented policies that Stripe formally…"
2. "Stripe implements measures for ensuring system configuration, including default configuration measures for internal IT and IT security governance.
Stripe relies on deployment automation tools to deplo…"
3. "All (a) Stripe employees; and (b) Stripe independent contractors who may have access to data, including those who Process Personal Data ((a) and (b), collectively 'Personnel') acknowledge their data s…"
4. "Stripe implements measures to prevent data processing systems from being used by unauthorized persons, including the following measures:
- user identification and authentication procedures;
- ID/pass…"

> *"Stripe implements policies and procedures for network and operations management. These policies and procedures address hardening, change control, segregation of duties, separation of development and production environments, technical architecture management, network security, malware protection, protection of data in transit and at rest, data integrity, encryption, audit logs and network segregation."*
> — Data Processing Agreement
> *"Each party will maintain commercially reasonable administrative, technical, and physical safeguards designed to protect data in its possession or under its control from unauthorized access, accidental loss, and unauthorized modification."*
> — Stripe Services Agreement - General Terms

> *"Stripe provides the Services in a manner consistent with PCI-DSS requirements that apply to Stripe."*
> — Stripe Services Agreement - Services Terms

Anti-Virus Solution

AI Comment: The playbook item requires confirmation that all authorized computer systems have an anti-virus solution — a specific, scope-bound technical control obligation. Stripe's documents partially address this requirement but do not fully satisfy the acceptable position.

The most directly relevant reference is in the DPA Data Security Exhibit (Document 3), which lists "malware protection" as one of the security areas explicitly addressed by Stripe's network and operations management policies and procedures. Anti-virus software is a principal mechanism for malware protection, so these concepts are closely related. However, "malware protection" is listed as a policy topic among several others — not as a specific technical commitment that anti-virus software is installed on all authorized computer systems. The breadth of the acceptable position ("all authorized computer systems") is not confirmed.

Second, Stripe's PCI DSS Level 1 certification (confirmed annually by a qualified security assessor) provides indirect but meaningful support. PCI DSS Requirement 5 mandates anti-malware controls — including anti-virus — on all systems commonly affected by malicious software within the cardholder data environment. Stripe's maintenance of PCI Level 1 implies systematic anti-malware controls exist. However, the DPA qualifies this coverage "to the extent applicable to the Services," which limits explicit confirmation to in-scope cardholder data environment systems rather than all authorized computer systems enterprise-wide.

Third, the General Terms Section 4.6 commits Stripe to "commercially reasonable administrative, technical, and physical safeguards," which would customarily encompass anti-virus deployment as a baseline industry standard. However, this is a general catch-all obligation and not a specific anti-virus commitment.

Taken together, the documents indicate that Stripe has malware protection controls in place (particularly for PCI-scoped systems) and has general security safeguard obligations, but no provision explicitly confirms anti-virus software deployment across all authorized computer systems. For a High weight item with a specific, scope-broad technical requirement, this partial and inferential coverage warrants a YELLOW classification: the topic is addressed, but with weaker and narrower language than the acceptable position demands.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "To the extent applicable to the Services, Stripe is responsible for providing the Services in a manner that is consistent with the highest certification level (PCI Level 1) provided by the PCI-DSS req…"

> *"These policies and procedures address hardening, change control, segregation of duties, separation of development and production environments, technical architecture management, network security, malware protection, protection of data in transit and at rest, data integrity, encryption, audit logs and network segregation."*
> — Data Processing Agreement
> *"Each party will maintain commercially reasonable administrative, technical, and physical safeguards designed to protect data in its possession or under its control from unauthorized access, accidental loss, and unauthorized modification."*
> — Stripe Services Agreement - General Terms

Restrictions on Use

AI Comment: Overall classification is GREEN. The acceptable position is met: Stripe's use restrictions do not prohibit the stated intended use (processing payments for purchasing the organization's product), and the core restrictions are recognizable acceptable-use policy provisions.

What the restrictions cover:

The principal use-restriction clause is Section 1.2(a) of the General Terms, which establishes nine prohibitions: personal/household use, circumventing technical limits, fraudulent/deceptive/harmful activity, service interference, sublicensing/transfer of rights, redistribution of the Services, account creation for suspended users, acting as a no-value-added pass-through agent, and use for Prohibited or Restricted Businesses. These are textbook AUP provisions. None reaches the intended use (a standard merchant accepting payment from end customers for its own product).

The Section 1.1 business-purpose limitation ("User must use the Services solely for User's Business Purposes") is standard and fully consistent with the stated use case.

The Stripe Payments Terms (§3.1 and §10) affirmatively confirm the intended use: users may "accept payment from Customers using various Payment Methods" and must use the Services "for bona fide commercial transactions … with Customers." This directly describes payment processing for product purchases.

Why the ideal preference is not met (aiPreferenceMet = false):

The ideal preference is "no restrictions beyond a standard acceptable-use policy." Stripe's terms impose three categories of restrictions that go modestly beyond a minimal AUP:

1. **The Prohibited and Restricted Businesses list (Doc 5):** This is an extensive, dynamically-updated catalogue of

prohibited and restricted industry categories that Stripe may modify unilaterally. Even where a business receives approval for a restricted category, that approval "may be modified or revoked by Stripe at any time." Because the intake brief does not specify the exact product or industry being sold, the list's applicability cannot be fully assessed — creating residual uncertainty not present in a typical AUP. This is reflected as YELLOW in PIF 3.

2. **Card network compliance requirements (§3.4 Stripe Payments Terms):** Restrictions on surcharging, minimum/maximum transaction amounts, location disclosure requirements, and card data usage rules are incorporated by reference to third-party Payment Method Rules and Card Network Rules. These are industry-standard obligations for any payment processor (Visa, Mastercard, Amex rules), but they are more operationally specific than what a pure AUP would impose.

3. **Broad suspension/termination triggers:** Section 10.1(b)(i) permits Stripe to terminate the agreement at any time for convenience; suspension rights are triggered by a wide range of risk-based determinations. These are not use restrictions per se but do affect the practical availability of the intended use.

Governing jurisdiction note: Jurisdiction is conditional (CA law for US users; Ireland for EEA; England and Wales for UK/Switzerland/Gibraltar). The restriction analysis does not materially vary across these jurisdictions for this item — the core AUP restrictions and prohibited businesses list apply globally.

Confidence: HIGH. The contract language is explicit and the analysis is well-supported. The one area of moderate uncertainty is the Prohibited/Restricted Businesses list, where full confirmation requires knowledge of the specific product/industry not provided in the intake brief.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "User must not, and must not enable or allow any third party to:

(i) use the Services for personal, family, or household purposes;

(ii) circumvent any technical limitations of the Services or enable …"
2. "User must use the Services solely for User's Business Purposes and in compliance with the Documentation."

> *"You must not use Stripe's services for any illegal activities or for the businesses or product types listed below. The types of businesses listed here are representative of prohibited categories, but this is not an exhaustive list."*
> — Prohibited and Restricted Businesses | Stripe
> *"User may accept payment from Customers using various Payment Methods by submitting Transactions to Stripe through the Stripe Technology. User must comply with Payment Method acceptance and use requirements which may be incorporated into the Stripe API and other Stripe Technology described in the Documentation, or set out in the Payment Method Rules, the Payment Method Terms, or both."*
> — Stripe Services Agreement - Services Terms
> *"User must only use the Payment Methods and Stripe Payments Services for bona fide commercial transactions (which must be free of liens, claims, and encumbrances other than ordinary sales taxes) with Customers."*
> — Stripe Services Agreement - Services Terms

Data Subject Rights Assistance

AI Comment: The playbook item requires two things: (1) Stripe must first notify User when a data subject rights request is received, and (2) Stripe must promptly assist User in fulfilling that request. Both obligations are substantively addressed in the DPA and are reinforced by the incorporated EEA Standard Contractual Clauses (SCCs).

Notification obligation: DPA Section 3.1(c) requires Stripe to "inform User of each request Stripe receives from Data Subjects" exercising DP Law rights across all four standard categories (access, erasure/correction, restriction/objection, portability). This maps directly to the "first notify us" requirement. Critically, the same provision states Stripe "will not respond to these requests unless User instruct Stripe in writing to do so," preserving User's primacy as data controller and ensuring Stripe cannot act on DSRs unilaterally.

Assistance obligation: DPA Section 3.1(c) further requires that "[t]aking into account the nature of the Processing, Stripe will assist User by appropriate technical and organizational measures, insofar as this is possible, to enable User to meet its obligation to respond to a Data Subject Request." This satisfies the "assist in fulfilling" prong. The qualifier "insofar as this is possible" and "appropriate technical and organizational measures" are standard GDPR-aligned language (Art. 28(3)(e)) and do not materially dilute the obligation.

Promptness qualifier: The playbook requires "promptly" assist. DPA Section 3.1(c) does not use "promptly" for the notification trigger, but the incorporated EEA SCCs (Module 2, Clause 10(a)) — which apply when Personal Data is transferred from EEA/UK/Switzerland — explicitly require that Stripe "shall promptly notify the data exporter of any request it has received from a data subject." For US-based Users, the DPA does not contain an explicit promptness qualifier on notification, though the overall framework contemplates timely action. This is a minor gap but does not rise to YELLOW given the comprehensive structure.

Additional support: DPA Section 3.1(e) provides broader assistance obligations for helping User comply with DP Law, including assisting with DPIAs and supervisory authority consultations, further demonstrating the depth of Stripe's processor support role.

Governing jurisdiction note: The applicable obligations differ slightly depending on User's Stripe Account Country. For

EEA users, the EEA SCCs (with "promptly") apply. For US users, DPA Section 3.1(c) applies without an explicit promptness qualifier for notification (though the no-response-without-instruction mechanism effectively achieves the same result). Jurisdiction is not yet confirmed per the intake brief.

Overall, the provisions collectively meet the acceptable position for a High-weight item: Stripe is obligated to notify User first, refrain from responding without User's written authorization, and assist with appropriate technical and organizational measures to enable User to fulfill DSRs.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "inform User of each request Stripe receives from Data Subjects (including "verifiable consumer requests" as defined under the CCPA) exercising their rights under DP Law to (i) access (e.g., right to k…"

> *"_Clause 10_*
>
> *_**Data subject rights**_*
>
> *(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.*
>
> *(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required."*
> — Data Transfers Addendum

Breach Notification Timeline

AI Comment: The acceptable position requires Stripe to notify User (i) without undue delay, and in any event within 72 hours, of an actual or suspected Data Security Breach, and (ii) of any other actual or potential breach of the DPA. The ideal preference is notification within 24 hours.

Primary Provision — DPA §3.1(f): The core Stripe-to-User notification obligation establishes a tiered approach: "without undue delay, which for Data Incidents affecting Personal Data subject to the GDPR or UK GDPR will be no later than 48 hours." For GDPR/UK GDPR data (applicable to EEA and UK account holders), the 48-hour hard cap is more protective than the acceptable 72-hour threshold — this aspect exceeds the acceptable position. For all other Personal Data (most critically, US-based accounts governed by California law per General Terms §13.1), Stripe commits only to "without undue delay" without any specific hard deadline, failing to satisfy the "in any event within 72 hours" hard cap in the acceptable position.

Gap 1 — Suspected Breaches Not Covered: Stripe's notification obligation triggers only upon an actual "Data Incident," defined as unauthorized or unlawful Processing, use, access, loss, disclosure, destruction, or alteration of Personal Data. The definition does not encompass suspected incidents. The acceptable position explicitly requires notification of "actual or suspected" Data Security Breaches — the missing "suspected" prong is a material gap regardless of jurisdiction.

Gap 2 — Other DPA Breaches Not Covered: The acceptable position's second prong requires notification of "any other actual or potential breach of the DPA." Stripe's DPA notification obligation is confined exclusively to Data Incidents; other categories of DPA non-compliance (e.g., sub-processor failures, instruction violations, confidentiality breaches) carry no notification commitment to User.

Gap 3 — Ideal Preference Not Met: The ideal preference of 24 hours is not met in any scenario. Even the most protective GDPR/UK GDPR provision sets 48 hours, which is double the ideal.

Supplementary Obligations (Data Transfers Addendum): EEA SCCs incorporated via the Data Transfers Addendum (Module 2, Clause 8.6(c)) add a supplementary "without undue delay" notification obligation for EEA transfers processed by Stripe as Data Processor. This is consistent with and additive to DPA §3.1(f) but does not introduce a specific hard timeframe for non-GDPR data, nor does it expand coverage to suspected breaches.

Jurisdiction Dependency: The Stripe Account Country is unresolved (per the pre-computed jurisdiction analysis, it could be California, Ireland, or England/Wales). For California/US-based accounts — a likely scenario for a US-based business using Stripe for payment processing — no specific hard notification deadline exists beyond "without undue delay," leaving the 72-hour cap unmet. This is a material concern for a Critical-weight item.

Positive Elements: Notification content requirements (type of data, categories/number of individuals affected, investigation status) are substantive and consistent with regulatory standards. A follow-up update commitment is also included.

Overall: The DPA substantively addresses breach notification (ruling out silence), and the GDPR/UK GDPR 48-hour provision exceeds the acceptable threshold for EEA/UK scenarios. However, three material gaps — no hard cap for non-GDPR data, no "suspected" breach coverage, and no "other DPA breach" coverage — collectively prevent GREEN classification. YELLOW reflects partial satisfaction with meaningful residual risk, which is significant given the Critical weight of this item.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "if Stripe experiences a Data Incident, notify User without undue delay, which for Data Incidents affecting Personal Data subject to the GDPR or UK GDPR will be no later than 48 hours, in each case aft…"

Retention of Our Rights to Our Property

AI Comment: The Stripe Services Agreement explicitly addresses IP ownership in Section 5.1(b), which states that "Nothing in this Agreement assigns or transfers ownership of any IP Rights to the other party, or contemplates a joint development of intellectual property." This direct prohibition on ownership transfer meets the literal acceptable position of the playbook item on its face — formal title to User's IP is not transferred to Stripe.

However, for a Critical-weight item whose purpose is to protect User's meaningful ownership and control over its own property, three additional provisions collectively prevent a GREEN classification:

1. Content License (§5.1(c)): Stripe is granted a perpetual, worldwide, non-exclusive, irrevocable, royalty-free license over all User-provided Content — broadly defined as all text, images, and other data User provides to Stripe in connection with the Services — not only to deliver services but also "for Stripe's internal business purposes." The irrevocability and perpetual nature mean User cannot retract Stripe's rights post-termination, and the "internal business purposes" scope materially exceeds what service delivery requires.

2. Feedback License (§5.2): Any feedback (ideas, suggestions, observations regarding the Services) is subject to a perpetual, irrevocable license "for any purpose" — an entirely unconstrained scope. Mitigated somewhat by feedback being voluntary and the narrow definition of Feedback, but the combination of perpetual + irrevocable + any purpose is notable.

3. Stripe Data Ownership (§§12, 4.2): Stripe claims ownership of "aggregated information Stripe generates from the Services," restricting User's ability to use derived data products built from User's own transactional activity, and requiring User to use Stripe Data "only as expressly permitted" by the Agreement.

None of these provisions formally transfer IP ownership — legal title and exclusivity remain with User. However, the irrevocable, perpetual character of the Content and Feedback licenses means User permanently loses practical ability to retract Stripe's usage rights. For a Critical-weight item, this departure from ideal terms (a vendor license limited in scope to service delivery and terminable upon agreement termination) warrants YELLOW. A human reviewer should specifically assess whether the Content license scope — particularly "for Stripe's internal business purposes" in perpetuity — is acceptable given the User's business and the types of content likely to be shared with Stripe in the context of payment processing.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "User grants to Stripe, on behalf of itself and its Affiliates, a perpetual, worldwide, non-exclusive, irrevocable, royalty-free license to use the Content to develop, improve, and provide Services and…"
2. "Subject to this Agreement, each party (or its applicable Affiliates) grants to the other party a worldwide, non-exclusive, non-transferable (except as allowed under Section 11.10 (Assignment)), non-su…"
3. ""Stripe Data" means data that User obtains via the Services, including (a) information relating to the Stripe API interactions via the Stripe Technology; (b) information Stripe uses for security or fr…"

> *"Nothing in this Agreement assigns or transfers ownership of any IP Rights to the other party, or contemplates a joint development of intellectual property."*
> — Stripe Services Agreement - General Terms

> *"Except as indicated in Section 1.4, Feedback is voluntary and User grants to Stripe, on behalf of itself and its Affiliates, a perpetual, worldwide, non-exclusive, irrevocable, royalty-free license to use that Feedback for any purpose."*
> — Stripe Services Agreement - General Terms

Regulatory Disclosure Procedure

AI Comment: Multiple provisions across Stripe's documentation address the notification component of this playbook item. DPA §3.1(d) commits to informing User of government authority requests for Personal Data (unless prohibited by law); General Terms §6 commits to advance notification before disclosing Confidential Information to governmental authorities (to the extent legally permitted); and the Data Transfers Addendum (DTA) provides EEA-specific notification obligations. These provisions collectively satisfy the playbook's "forward request to us, unless prohibited by law" element.

However, the playbook's second critical element—that Stripe "await our instructions before acting on the request"—is absent from every provision reviewed. The contrast with DPA §3.1(c) is particularly telling: for data subject requests, Stripe explicitly states it "will not respond to these requests unless User instruct Stripe in writing to do so." No equivalent "await instructions" language appears in DPA §3.1(d) for governmental authority requests. This asymmetry appears deliberate—Stripe retains the right to respond to binding legal demands independently, with notification as the primary user protection mechanism rather than a pause-and-await obligation.

The DTA Module 2, Clause 15.2 provides partial mitigation specifically for EEA Personal Data transfers: Stripe independently reviews legality of government requests, challenges unlawful ones, seeks interim judicial measures (including suspension of disclosure pending a court ruling), and will not disclose while a challenge is pending. This approaches the spirit of "await instructions" for unlawful EEA requests, but falls short for: (a) lawful requests of any kind, (b) transfers outside

the EEA, and (c) the explicit requirement to await User's specific instructions before acting.

Classification is YELLOW: the notification component is robustly addressed across multiple provisions and jurisdictions, but the "await instructions" commitment required by the acceptable position is absent. For a HIGH weight item, this requires documented assessment and may warrant negotiation of a contractual amendment or side letter committing Stripe to a defined notification window during which it would not respond to the authority without User input, except where immediate legal compliance is required.

— Superseding reasoning —
DPA §3.1(d) supersedes General Terms §6 for Personal Data regulatory requests. DPA §7 contains an explicit precedence clause stating that "the provisions of this DPA will prevail" over any conflicting provision of the Agreement regarding Personal Data Processing. Additionally, DPA §3.1(d) is a specific provision addressing Personal Data governmental authority requests, while General Terms §6 is a general confidentiality provision applicable to all Confidential Information. Post-superseding, General Terms §6 continues to govern only for Confidential Information that does not constitute Personal Data. For Personal Data, DPA §3.1(d) governs, supplemented by DTA Module 2 Clause 15 for EEA transfers (the DTA is incorporated into the DPA per DPA §6.1 and the Data Transfers Addendum reference therein). No conflict exists between DPA §3.1(d) and the DTA provisions—they are complementary, with the DTA adding jurisdictional specificity and challenge obligations for EEA transfers.

> *"The recipient may disclose Confidential Information if required by Law, subpoena, or court order, or if directed by a Governmental Authority, as long as (if permitted by Law) it notifies the discloser in advance (to the extent legally permitted) and provides reasonable assistance, at the discloser's cost, if the discloser wishes to contest the disclosure."*
> — Stripe Services Agreement - General Terms
>
> *"(d) inform User of each law enforcement request Stripe receives from a Governmental Authority requiring Stripe to disclose Personal Data or participate in an investigation requiring Stripe to disclose Personal Data, unless prohibited by Law;"*
> — Data Processing Agreement
>
> *"The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:*
>
> *(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or*
>
> *(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer."*
> — Data Transfers Addendum
>
> *"The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e)."*
> — Data Transfers Addendum
>
> *"Stripe, LLC will notify User of any binding legal demand for the Personal Data it has received, including national security orders and directives, which will encompass any process issued under Section 702 of FISA, unless prohibited under Law."*
> — Data Transfers Addendum

Data Segregation

AI Comment: The DPA's Data Security Exhibit contains an explicit "Separation Controls" section (indexed at 3-128) committing Stripe to "logical segmentation processes to manage the separation of Personal Data" and "procedures for storage, amendment, deletion, transmission of data for different purposes." This is the principal clause governing this playbook item and directly addresses logical separation. However, the operative framing is separation of "Personal Data collected for different purposes" rather than "data received from different controllers" — a meaningful distinction in a multi-tenant, multi-controller processor environment. Under GDPR and equivalent frameworks, a processor (Stripe) serving many data controllers (User/merchants) has an obligation to prevent one controller's data from being accessible to or commingled with another's. The DPA Separation Controls addresses this tangentially through purpose-based segmentation but does not make an explicit, controller-level isolation commitment. Additionally, no physical separation of different controllers' data is addressed anywhere in the document set. The General Terms §4.6 general safeguards provision provides a broad but non-specific security backdrop (administrative, technical, and physical safeguards against unauthorized access/loss/modification) that does not fill this specific gap. Because the acceptable position requires "physical and/or logical separation of data received from different controllers," and because the contract language: (a) commits to logical segmentation only (not physical); and (b) frames that commitment around purpose rather than controller identity — the contract addresses the topic but with weaker/less precise language than the acceptable position requires. YELLOW is the appropriate classification for this High-weight item. HIERARCHY FLAG: DPA §7 states the DPA prevails over Agreement provisions on Personal Data Processing matters, while General Terms §11.9 places incorporated-by-reference terms (including the DPA) at the lowest precedence level — a competing hierarchy clause. These clauses are not in direct conflict on this topic (they are complementary), but the existence of competing precedence language is flagged for human review per standard playbook methodology.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Stripe implements measures to ensure that Personal Data collected for different purposes can be Processed separately, including:
• "least privilege" limitation of access to data by internal services;
…"

> *"Each party will maintain commercially reasonable administrative, technical, and physical safeguards designed to protect data in its possession or under its control from unauthorized access, accidental loss, and unauthorized modification."*
> — Stripe Services Agreement - General Terms

Vendor's liability

AI Comment: The Stripe Services Agreement addresses the liability cap with a mix of acceptable and deficient protections relative to the playbook's acceptable position (cap "e 12-month fees + four carve-outs: data breaches, confidentiality breaches, IP infringement, indemnification).

Cap Level — MET. Section 8.4 of the General Terms sets the aggregate cap at "the total Fees User paid to Stripe (excluding all pass-through fees levied by Financial Providers) during the 12 month period before the first event giving rise to liability." This meets the minimum acceptable threshold. Note, however, that the cap is based on Stripe service fees only — not total payment volume processed — which could make the cap materially lower than User's exposure depending on Stripe's fee rates.

Carve-out Scorecard:

1. **Data breaches — ABSENT and explicitly excluded.** This is the critical gap. Section 8.4 states the cap applies "(including Data Incident Losses)" — affirmatively placing data breach losses inside the cap. The "Excluded Claims" definition (§12) compounds this adversity: clause (c) carves out confidentiality breaches under §6, but appends "but excluding Data Incident Losses," deliberately ensuring that even when a data breach arises from a confidentiality breach, the cap still applies. This is a deliberate structural choice by Stripe to confine data breach liability within the aggregate cap. For a payment processor handling sensitive financial data (payment card details, bank account information), this is the most commercially significant gap.

2. **Confidentiality breaches — PARTIALLY MET.** General confidentiality breaches under §6 that do not constitute a Data Incident are Excluded Claims (§12, clause c) and therefore uncapped. However, the data breach scenario — the most significant confidentiality breach risk — is expressly kept within the cap.

3. **IP infringement — MET (via indemnification).** The Excluded Claims definition (§12, clause d) carves out "amounts payable under Section 9.1 (Indemnities)." Section 9.1(b) establishes mutual IP indemnities covering claims that Stripe Technology, Services, or Marks infringe third-party IP Rights. Because these indemnification payments are Excluded Claims, IP-related losses recovered through the indemnification mechanism are uncapped.

4. **Indemnification obligations — MET.** Same clause (d) carves out all amounts payable under §9.1, covering both general and IP indemnities. Indemnification payments are uncapped as Excluded Claims.

Beneficial Service-Terms Carve-out (settlement funds). The Stripe Payments Terms §12 explicitly carves out Stripe's liability for failure to transfer settlement funds from the §8.4 cap. For this specific failure, Stripe's liability equals the actual amount owed but not transferred — potentially more favorable than the 12-month fee cap in the operationally most critical payment processing failure scenario. Per §11.9, Service Terms prevail over General Terms.

Preview Services Adverse Cap. Section 1.4 (§1.37) imposes a separate $1,000 aggregate cap for Preview Services, overriding §8.4 via "Notwithstanding anything else in this Agreement." If any Stripe features used by User are designated Preview Services, this cap would be drastically below the acceptable minimum.

Preferred Position — NOT MET. The preferred position (uncapped liability or a super-cap for data breach) is not achieved. Data breach liability is affirmatively included within the standard 12-month fee cap.

Overall: YELLOW — the cap level meets the acceptable threshold and three of four required carve-outs are present, but the absence of a data breach carve-out is deliberate, explicit, and significant given Stripe's role as a payment data processor. For a High weight item, this warrants documented legal assessment.

— Superseding reasoning —
Two superseding relationships exist within this item's scope. First, the Stripe Payments Terms §12 explicitly overrides §8.4 of the General Terms for the specific scenario of Stripe's failure to transfer settlement funds owed to User. The Payments Terms state "The limitation of liability in Section 8.4 of the General Terms will not apply to claims User or User's Affiliates make against the Stripe Parties for failing to transfer any settlement funds." This is a specific-over-general override, reinforced by the Order of Precedence at §11.9 (Service Terms prevail over General Terms). Second, General Terms §1.37 uses "Notwithstanding anything else in this Agreement" to override §8.4 for Preview Services, imposing a $1,000 cap regardless of fees paid. This explicit "notwithstanding" language establishes it as a governing provision for Preview Services scenarios.

— Note —
The AI cited 5 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Except for Excluded Claims, a party's total aggregate liability for damages and Losses for all claims arising out of or relating to the Agreement (including Data Incident Losses) is limited to the tot…"
2. ""Excluded Claims" means: (a) a party's gross negligence, fraud, or willful misconduct, (b) User's breach of Section 1.2 (Restrictions), (c) a party's breach of Section 6 (Confidentiality) but excludin…"
3. ""Data Incident Losses" means Losses arising from a Data Incident to the extent caused by (a) the indemnifying party's material breach of this Agreement; (b) the indemnified party's compliance with any…"
4. "The limitation of liability in Section 8.4 of the General Terms will not apply to claims User or User's Affiliates make against the Stripe Parties for failing to transfer any settlement funds the Stri…"
5. "Notwithstanding anything else in this Agreement, to the maximum extent permitted by Law, Stripe provides no warranty, indemnity, or support for Preview Services and Stripe's aggregate liability for Pr…"

> *"Except for Excluded Claims, to the maximum extent permitted by Law, neither party will have any liability in relation to this Agreement for any indirect, consequential, special, reliance, incidental, or punitive damages, lost revenue, profits, savings or goodwill, business interruption, personal injury, property damage, or loss of data, whether in contract, negligence, strict liability, tort, or other legal or equitable theory, even if these losses, damages, or costs are foreseeable, and whether or not any party has been advised of their possibility."*
> — Stripe Services Agreement - General Terms

Indemnification – Our Company to Vendor

AI Comment: The Stripe Services Agreement imposes indemnification obligations on User that partially align with the acceptable position but exceed it in critical respects. Assessment turns on three dimensions:

1. Third-party claim limitation — Partially met. "Losses" is defined in §12 as amounts arising from "Claims," and "Claim" means proceedings brought by a third party (including government investigations). Because the indemnification obligation in §9.1(a) is for "all Losses," and Losses are tied to third-party Claims, the indemnification is technically limited to third-party claims. This satisfies that limb of the acceptable position.

2. Scope of triggering conduct — Not met. The primary trigger in §9.1(a) is "User's use of the Services or Stripe Technology" — a phrase that on its face is materially broader than the acceptable position's requirement of "misuse of the services." Routine, authorized use that happens to give rise to a third-party claim against Stripe could trigger this obligation. The remaining §9.1(a) triggers — gross negligence, willful misconduct, fraud, material breach — map more closely onto the "misuse" concept in the acceptable position, but the open-ended "use of the Services" language is the principal concern. Separately, the §9.1(b) IP indemnification is tied to User's marks and materials, making it the closest analog to the acceptable position's "content" concept, though it still operates without an explicit content limitation.

3. Uncapped exposure — Not met. The §12 "Excluded Claims" definition expressly excludes "amounts payable under Section 9.1 (Indemnities)" from the §8.4 liability cap. User's entire indemnification exposure is therefore uncapped, with no ceiling tied to fees paid — a significantly worse posture than the acceptable position contemplates.

Mitigating factors. Section 9.2 is meaningful: the indemnification obligation does not apply where the Claim/Losses arise from Stripe's own negligence, fraud, willful misconduct, or breach. This carve-out protects User from indemnifying Stripe for Stripe's own wrongdoing. Additionally, §9.3 procedural protections (notice, control of defense, no settlement without User consent for non-monetary terms) provide further guardrails.

Additional obligation in Stripe Payments Terms. Section 11 of the Stripe Payments Terms creates an additional, separately uncapped responsibility for losses, damages, and costs Stripe incurs from fraudulent Transactions, as well as Financial Provider audit and forensic investigation costs arising from User's use of the Stripe Payments Services. This operates alongside §9.1 of the General Terms.

Ideal preference (no indemnification obligation on User) is clearly not met.

Overall: YELLOW. The Losses/Claim definitions satisfy the third-party requirement, and §9.2 provides meaningful fault-based protection, but the "use of the Services" trigger exceeds the acceptable position's "misuse" standard, no content limitation is present, and the indemnification is entirely uncapped. The gap between the acceptable position and the contract language is real but not absolute — the bulk of scenarios under which indemnification could be triggered (negligence, misconduct, fraud, breach) do map onto "misuse."

— Note —
The AI cited 5 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Subject to Section 9.2 (Limitations on Indemnity), User will indemnify Stripe, its Affiliates, and their directors, employees, and agents for all Losses arising from User's use of the Services or Stri…"
2. "An indemnifying party's obligations under Section 9.1 do not apply to the extent that the Claim or Losses arise out of an indemnified party's negligence, fraud, willful misconduct, or breach of this A…"
3. ""Claim" means any claim, demand, government investigation, or legal proceeding that a third party makes or brings against any indemnified party."
4. ""Excluded Claims" means: (a) a party's gross negligence, fraud, or willful misconduct, (b) User's breach of Section 1.2 (Restrictions), (c) a party's breach of Section 6 (Confidentiality) but excludin…"

5. "As between the parties, User is responsible for all (a) losses, damages, and costs Stripe and its Affiliates incur due to fraudulent Transactions, and the limitations on liability in Sections 8.3 and …"

> *"Subject to Section 9.2 (Limitations on Indemnity), each party will indemnify the other party, its Affiliates, and their directors, employees, and agents for all Losses, to the extent they arise from an IP Claim, except that this indemnification obligation does not apply if the indemnified party uses the Materials in combination with other materials not provided by the indemnifying party (if the Materials the indemnifying party provided would not infringe absent the combination)."*
> — Stripe Services Agreement - General Terms

Automatic Renewal

AI Comment: The acceptable position requires (1) at least 30 days' notice before the renewal date and (2) the right to cancel before renewal. The Stripe SSA partially — but not fully — satisfies this standard.

Right to cancel before renewal (condition 2): SATISFIED. Section 10.1(a)(i) provides an unrestricted, unconditional Termination for Convenience right: User may close its Stripe Account via the Dashboard at any time, with no penalty and no minimum notice period. This is a strong and clear cancellation right that exceeds the acceptable position on this prong.

Notice before renewal date (condition 1): PARTIALLY SATISFIED, with two gaps.

First, the SSA is structured as an evergreen agreement (§1.8) — it runs indefinitely until terminated by either party — rather than as a fixed-term contract that "auto-renews." This means many of the classic auto-renewal concerns (e.g., a 12-month commitment silently rolling into another 12-month commitment) do not arise at the Agreement level.

Second, for Subscription Plans specifically, Section 7.1(c) provides 30 days' advance notice of any *increase* in fees or any *materially adverse change* to a Subscription Plan. This partially satisfies the notice prong: if a subscription is renewing at a higher rate or under worse terms, User gets 30 days' warning. However, this clause is expressly limited to *changes*; it does not require Stripe to provide advance notice before a subscription auto-renews at the *same* terms and rate. An unchanged auto-renewal could occur without affirmative prior notice beyond what was disclosed at plan enrollment.

Third, Section 7.1(e) expressly provides for automatic conversion of free trials to paid subscriptions upon expiry, but specifies no minimum advance notice before that conversion occurs. This is a gap against the acceptable position's 30-day notice requirement applied to the trial-to-paid renewal event.

Fourth, Section 7.1(b) expressly defers the governing renewal terms to "the applicable Subscription Plan," the specific terms of which are not in the provided document set. The content of those Subscription Plans — including whether they contain renewal-specific notices — cannot be assessed from the materials provided.

Aggregate assessment: YELLOW. The right to cancel is fully satisfied. The notice obligation is partially addressed (changes trigger 30-day notice; §7.1(c)) but not fully (unchanged renewals and free trial conversions lack explicit advance notice). Renewal mechanics for Subscription Plans are also deferred to terms not in evidence. Given the "Acceptable to Deviate" weight, this finding is informational and does not require formal escalation, but practitioners should confirm Subscription Plan terms contain adequate renewal notice provisions and should note the free trial auto-conversion gap.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "This Agreement is effective when User first accesses or uses the Services or Stripe Technology (the "Effective Date") and continues until User or Stripe terminates it (the "Term")."

> *"Subscription Services are governed by the terms of the applicable Subscription Plan. If User exceeds the entitlement scope in the Subscription Plan, then except as stated otherwise in the Subscription Plan or agreed in writing between the parties, Stripe will charge User for the increased scope of use according to the Fees stated on the Stripe Pricing Page."*
> — Stripe Services Agreement - General Terms
> *"Subject to the requirements of Law, Stripe may revise the Fees and Subscription Plans at any time. Stripe will provide User with at least 30 days notice (or longer period if Law requires) of any increase in a Fee or any new Fees for any Service provided to User, or any materially adverse change in a Subscription Plan."*
> — Stripe Services Agreement - General Terms
> *"Stripe may make certain Services available to User on a trial basis free of charge until (i) the expiration or termination of the free trial, at which point the Fees stated on the Stripe Pricing Page will apply, or (ii) the start of any Subscription Plan that User has purchased, at which point that Subscription Plan will automatically commence."*
> — Stripe Services Agreement - General Terms
> *"User may terminate this Agreement at any time by closing its Stripe Account via the Stripe Dashboard."*
> — Stripe Services Agreement - General Terms

Security Training

AI Comment: The playbook item requires that vendor employees who access data attend security training at least annually. The Stripe Data Processing Agreement (DPA), incorporated by reference into the General Terms via Section 4.1, directly and explicitly satisfies this requirement through two complementary provisions in its Data Security Exhibit.

First, the "Training and Awareness" sub-section confirms the required annual cadence: "Stripe's employees complete an annual Security and Privacy awareness training on Stripe's data security and confidentiality policies and practices." This expressly meets the "at least annually" threshold.

Second, the "Personnel Education and Controls" sub-section establishes the scope of coverage: the training obligation applies to all Stripe employees AND independent contractors "who may have access to data, including those who Process Personal Data," with the explicit obligation to "conduct security and privacy training." This aligns precisely with the playbook's trigger — "employees that access data."

Together, these provisions confirm: (a) the correct population (all personnel with data access), (b) the correct activity (security training), and (c) the correct frequency (annual). All three elements of the acceptable position are satisfied. Classification: GREEN.

Note: No ideal preference was specified in the playbook item, so aiPreferenceMet is false — GREEN reflects that the acceptable threshold is met, not that an unstated higher standard is exceeded. Confidence is HIGH given that the contract language is unambiguous and directly maps to each element of the requirement.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Annual Security and Privacy Training. Stripe's employees complete an annual Security and Privacy awareness training on Stripe's data security and confidentiality policies and practices."
2. "All (a) Stripe employees; and (b) Stripe independent contractors who may have access to data, including those who Process Personal Data ((a) and (b), collectively "Personnel") acknowledge their data s…"

Compliance Monitoring

AI Comment: The playbook item requires the vendor to proactively review, and where necessary adapt, its compliance with the DPA and applicable data protection and privacy laws at least annually. Stripe's documents address compliance monitoring in several related but distinct ways, none of which precisely satisfies this requirement.

The closest language appears in the DPA Data Security Exhibit, where Stripe commits to maintaining a security program that includes "documented policies that Stripe formally approves, internally publishes, communicates to appropriate personnel and reviews at least annually." This provides an annual review cycle, but it is explicitly scoped to security policies — not to DPA compliance or data protection law compliance broadly. Similarly, SOC 1 and 2 reports are produced annually and periodic vulnerability assessments and risk assessments are conducted, but these are security-assurance mechanisms rather than a formal commitment to review and adapt DPA/data protection law compliance.

The DPA Section 3.1(g) contemplates audit support — but only upon User's written request (no more than once annually). This is user-triggered and reactive, not Stripe's own proactive annual compliance review. The Privacy Policy also commits to updating the policy to reflect changes in privacy practices or applicable laws, but this too is reactive and lacks an explicit periodic cadence.

Critically, no provision in any document obligates Stripe to proactively and periodically (at least annually) assess its own compliance posture against the DPA and applicable data protection laws and make any necessary adaptations. The obligation runs from User to Stripe (via audit requests) rather than from Stripe as an internal, self-initiated annual review.

Given the High weight of this item and the absence of explicit language satisfying the annual compliance review and adaptation obligation — despite the existence of meaningful but insufficient adjacent provisions — this item is classified YELLOW. The contract addresses the topic area in part, but provides weaker and narrower coverage than the acceptable position requires.

— Note —
The AI cited 7 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Stripe maintains and enforces a security program that addresses how Stripe manages security, including its security controls. The security program includes:
- documented policies that Stripe formally…"
2. "following User's written request, contribute to audits or inspections by making audit reports available to User. Following this request, and no more frequently than once annually, Stripe will promptly…"
3. "Stripe performs risk assessments, and implements and maintains controls for risk identification, analysis, monitoring, reporting and corrective action.
Stripe maintains and enforces an asset managemen…"
4. "Stripe maintains Service Organization Controls ("SOC") auditing standards for service organizations issued under the AICPA. SOC 1 and 2 reports are produced annually and will be provided upon request."
5. "Stripe performs periodic vulnerability assessments and penetration testing on its systems and applications, including those that Process Personal Data. Vulnerabilities are managed and remediated in ac…"

6. "Upon written request, and no more frequently than annually, Stripe will complete a written data security questionnaire of reasonable scope and duration regarding Stripe's business practices and data t…"
7. "We may change this Policy from time to time to reflect new services or changes in our privacy practices or relevant laws. The "Last updated" legend at the top of this Policy indicates when this Policy…"

> *"Stripe implements and maintains data retention policies and procedures related to Personal Data and reviews these policies and procedures as appropriate."*
> — Data Processing Agreement

Indemnification – Vendor to Our Company

AI Comment: This playbook item requires Stripe (vendor) to indemnify User for two distinct categories: (1) intellectual property infringement claims and (2) data breaches. The Agreement addresses these two requirements very differently, and only the IP component is satisfied.

IP Infringement Indemnification — Present (with meaningful limitations): Section 9.1(b)(i) of the General Terms provides bilateral IP indemnification. Where Stripe is the indemnifying party, it covers third-party IP Claims arising from User's use of Stripe Technology, Services, Stripe Marks, or any other Material Stripe provided — a broad and appropriate scope for a payment-processing vendor. This satisfies the IP component of the playbook requirement. Three limitations weaken the indemnity compared to an unconstrained IP warranty: (a) Stripe retains the sole discretion to terminate User's access to infringing Materials on 30 days' notice rather than being obligated to remediate the infringement (§9.1(b)(ii)); (b) Section 9.1(b) constitutes User's sole and exclusive remedy for IP Claims, foreclosing any supplemental contractual or tort claims (§9.1(b)(iii)); and (c) a combination carve-out excludes the indemnity where infringement arises only from combining Stripe's Materials with non-Stripe materials — a standard but notable carve-out.

Data Breach Indemnification — Absent: The Agreement contains no indemnification provision from Stripe to User for data breaches or Data Incidents. Instead, Data Incident Losses (as defined in §12) are governed by the general fee-based liability cap (§8.4), which limits Stripe's aggregate liability to fees paid in the prior 12 months. The Excluded Claims definition expressly confirms that Data Incident Losses do NOT fall outside the liability cap (they remain capped). The DPA adds a data incident notification obligation (§3.1(f)) requiring notice without undue delay and within 48 hours for GDPR-scope incidents, but this is a procedural obligation, not indemnification. The DPA further disclaims liability for Data Subject claims where Stripe was acting per User's Instructions (§3.4). Collectively, these provisions replace indemnification with a capped-direct-liability framework — a materially weaker posture given that Stripe processes payment card data and substantial Customer Personal Data, creating meaningful third-party exposure for User (regulatory fines, customer claims, card network assessments) if Stripe's breach causes a data incident.

Overall Assessment: The acceptable position — indemnification for both IP infringement claims and data breaches — is only half-met. IP indemnification is present (albeit with limiting terms reducing its practical value), while data breach indemnification is entirely absent. At Medium weight, documented justification is required. Negotiation focus should target explicit indemnification from Stripe covering third-party claims (regulatory actions, data subject claims, card network assessments) causally attributable to a Data Incident arising from Stripe's material breach of the Agreement or DPA. Note that governing jurisdiction is not yet confirmed (California, Ireland, or England and Wales depending on User's Stripe Account Country), which may affect enforceability analysis of any indemnification terms obtained.

— Note —
The AI cited 7 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "" **IP Claim**" means:

(a) where Stripe is the indemnifying party, a Claim by a third party that the indemnified party's use of the Stripe Technology, Services, Stripe Marks, or any other Material th…"
2. "If an IP Claim arises, the indemnifying party may, at its sole discretion and expense (i) modify the Materials it provided to be non-infringing, replace them with non-infringing alternatives, or obtai…"
3. "This Section 9.1(b) states the indemnifying party's entire liability to the indemnified parties, and the indemnified parties' sole and exclusive rights and remedies, with respect to an IP Claim."
4. "An indemnifying party's obligations under Section 9.1 do not apply to the extent that the Claim or Losses arise out of an indemnified party's negligence, fraud, willful misconduct, or breach of this A…"
5. "Except for Excluded Claims, a party's total aggregate liability for damages and Losses for all claims arising out of or relating to the Agreement (including Data Incident Losses) is limited to the tot…"
6. "" **Excluded Claims**" means: (a) a party's gross negligence, fraud, or willful misconduct, (b) User's breach of Section 1.2 (Restrictions), (c) a party's breach of Section 6 (Confidentiality) but exc…"
7. "Notwithstanding anything to the contrary in the Agreement, including this DPA, Stripe and its Affiliates will not be liable for any claim made by a Data Subject arising from or related to Stripe's or …"

> *"Subject to Section 9.2 (Limitations on Indemnity), each party will indemnify the other party, its Affiliates, and their directors, employees, and agents for all Losses, to the extent they arise from an IP Claim, except that this indemnification obligation does not apply if the indemnified party uses the Materials in combination with other materials not provided by the indemnifying party (if the Materials the indemnifying party provided would not infringe absent the combination)."*
> — Stripe Services Agreement - General Terms

> *"if Stripe experiences a Data Incident, notify User without undue delay, which for Data Incidents affecting Personal Data subject to the GDPR or UK GDPR will be no later than 48 hours, in each case after becoming aware of the Data Incident."*
> — Data Processing Agreement

Ownership of Custom Deliverables

AI Comment: The playbook requires that Stripe assign ownership of custom deliverables to the user. The Agreement does not meet this acceptable position — in fact, it affirmatively and explicitly contradicts it across multiple provisions.

Section 5.1(a) broadly asserts Stripe's ownership of all IP Rights in the Services, Stripe Technology, and Documentation. Section 5.1(b) then delivers an explicit, categorical negation: "Nothing in this Agreement assigns or transfers ownership of any IP Rights to the other party, or contemplates a joint development of intellectual property." This language leaves no ambiguity — there is no pathway for a user to receive assigned ownership of any Stripe-created deliverable under the standard Agreement.

The Professional Services Terms, which govern Stripe's advisory and consulting engagements, are the most relevant context for "custom deliverables." However, rather than carving out an ownership assignment for work product, those terms classify deliverables — specifically, Sample Codes — as "Documentation for purposes of this Agreement." Documentation is squarely within Stripe's IP ownership under §5.1(a). The Professional Services Terms thus reinforce (not relax) Stripe's IP retention.

Additionally, Section 5.1(c) runs in the opposite direction from the playbook requirement: the Agreement grants Stripe a perpetual, irrevocable, royalty-free license to use user-provided Content for Stripe's own development and business purposes — with no reciprocal assignment of Stripe-created outputs to the user.

The absence of any custom deliverable assignment provision, combined with the explicit "nothing in this Agreement assigns…IP Rights" language, constitutes a direct conflict with the acceptable position. This is RED on a High-weight item, presenting high risk requiring senior legal justification or negotiated amendment. In practice, if the user requires assignment of custom deliverables (e.g., bespoke integrations, custom-built tooling), this would need to be addressed in a separately negotiated Professional Services Order Form or a specific IP ownership addendum — neither of which is present in the reviewed documents.

— Superseding reasoning —
The Professional Services Terms (Service Terms) take precedence over the General Terms per §11.9 (Order of Precedence). However, no conflict exists between these layers on the IP ownership question — both are consistent. The Professional Services Terms classify deliverables as "Documentation," and the General Terms confirm Stripe owns the Documentation. The Service Terms do not create an IP assignment carve-out; they reinforce Stripe's retention of ownership. No superseding determination is required.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "User grants to Stripe, on behalf of itself and its Affiliates, a perpetual, worldwide, non-exclusive, irrevocable, royalty-free license to use the Content to develop, improve, and provide Services and…"
2. "Stripe may, as part of Stripe Professional Services, provide sample codes, snippets, and programming examples illustrating various features of the Stripe Technology (collectively, "Sample Codes"). Str…"

> *"As between the parties, Stripe, its Affiliates, and its third party licensors own all IP Rights in the Services, the Stripe Technology, Stripe Data, the Stripe Marks, the Documentation, and the Stripe Website."*
> — Stripe Services Agreement - General Terms

> *"Nothing in this Agreement assigns or transfers ownership of any IP Rights to the other party, or contemplates a joint development of intellectual property."*
> — Stripe Services Agreement - General Terms

Processing Limitation

AI Comment: The acceptable position requires that processing be limited to fulfilling contractual obligations and written instructions. Stripe's terms address this requirement in a dual-role framework — satisfying it for the Data Processor role, but explicitly departing from it in the Data Controller role and via the Content license.

Processor Role — Requirement Met:
DPA §3.1(a) expressly commits Stripe to "Process Personal Data on User's behalf and according to User's Instructions," with an obligation to flag non-compliant instructions. The Data Transfers Addendum §8.3 reinforces this, declaring the DPA and Agreement are "User's complete and final instructions at the time of execution of the DPA for the Processing of Personal Data." The CCPA-specific provision (DPA §3.3) adds a further constraint: Stripe will not "retain, use or disclose Personal Data outside of its direct business relationship with User other than to provide Stripe's products and services and as required to comply with Law." Together, these provisions satisfy the acceptable position for the Processor role.

Controller Role — Material Gap:
DPA §2 explicitly carves out a separate Data Controller role in which Stripe "has the sole and exclusive authority to determine the purposes and means of Processing Personal Data it receives from or through User." The enumerated Controller purposes include, critically, "analyze, improve and develop Stripe's products and services." This is independent processing that is not directed by, or limited to, User's contractual obligations or written instructions. While the other listed Controller purposes — fraud detection, AML/KYC compliance, Financial Provider obligations — represent expected and largely unavoidable processing for a regulated payment processor, the product development/improvement purpose is a direct deviation from the acceptable position.

Content License — Additional Gap:

General Terms §5.1(c) grants Stripe a "perpetual, worldwide, non-exclusive, irrevocable, royalty-free license to use the Content to develop, improve, and provide Services and Stripe Technology and for Stripe's internal business purposes." Content is defined to exclude Personal Data, but it encompasses other business data User provides (text, images, operational data). The "internal business purposes" formulation is unrestricted and extends well beyond fulfilling User's contractual obligations. This license is irrevocable and survives the contract term.

Precedence:
DPA §7 establishes that the DPA prevails over General Terms for Personal Data processing conflicts. However, the Controller-role gap originates within the DPA itself (§2) — not from a conflict between the DPA and General Terms — so DPA's supremacy clause does not remedy it. The Content license (General Terms §5.1(c)) applies to non-Personal Data Content and is not addressed by the DPA, so it stands.

Classification Rationale (YELLOW, not RED):
The Processor-role commitment is explicit and comprehensive. The Controller purposes, while broader than the acceptable position, are in large part institutionally expected for a regulated payment processor (fraud, compliance, AML/KYC). The product development/improvement purpose and the irrevocable Content license are the primary departures from the acceptable position. The overall framework is structured and contractually documented rather than absent — but for a Critical-weight item, these gaps warrant significant legal attention, negotiation, or a documented exception with risk justification. Jurisdiction-specific note: the finalized governing jurisdiction for this review is unconfirmed (US/California, Ireland/EEA, or England/Wales depending on User's Stripe Account Country), but this gap is structural across all regional variants of the DPA.

— Superseding reasoning —
DPA §7 establishes that DPA provisions prevail over General Terms for Personal Data processing conflicts. This makes the DPA's Processor instruction obligation (§3.1(a)) authoritative for that dimension. However, the Controller-role carve-out (DPA §2) is itself a DPA provision, not a General Terms provision, so no inter-document superseding applies to the Controller gap. The Content license (General Terms §5.1(c)) applies to non-Personal Data Content and is not addressed by the DPA, so no superseding applies there either. No intra-item superseding among PIFs is required — the Processor (GREEN) and Controller (YELLOW) findings address distinct processing tracks that co-exist within the DPA's framework.

— Note —
The AI cited 4 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "When Stripe Processes Personal Data as a Data Controller it:
- has the sole and exclusive authority to determine the purposes and means of Processing Personal Data it receives from or through User; a…"
2. "The purposes of Stripe's Processing of Personal Data in its capacity as a Data Controller when providing Stripe's products and services are to:
- determine and utilize third parties (banks and payment…"
3. "User grants to Stripe, on behalf of itself and its Affiliates, a perpetual, worldwide, non-exclusive, irrevocable, royalty-free license to use the Content to develop, improve, and provide Services and…"
4. "To the extent the CCPA applies and Stripe is acting as a Data Processor, Stripe will not (except to provide Stripe's services as permitted by Law): (a) sell or share (as defined under the CCPA) Person…"

> *"When Stripe is acting as a Data Processor for User, Stripe will, to the extent required by DP Law:*
>
> *(a) Process Personal Data on User's behalf and according to User's Instructions. Stripe will inform User if, in its opinion, Instructions violate or infringe DP Law"*
> — Data Processing Agreement
> *"The DPA and the Agreement are User's complete and final instructions at the time of execution of the DPA for the Processing of Personal Data. Any additional or alternate instructions must be agreed separately in writing by User and Stripe."*
> — Data Transfers Addendum
> *"Stripe will use Third Party Data as this Agreement describes and to (a) secure, provide, and update the Stripe services, (b) comply with Law and Financial Provider requirements, and (c) prevent and mitigate fraud, financial loss, and other harm."*
> — Stripe Services Agreement - General Terms

Data Backup & Restoration

AI Comment: The playbook requirement has two distinct obligations: (1) creating backups of data, and (2) regularly conducting restoration tests of backups, at a minimum annually.

Prong 1 — Backup Creation: The DPA Data Security Exhibit (Availability Controls) explicitly confirms Stripe maintains "backup procedures" and "measures to ensure the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident." This satisfies the first prong of the requirement.

Prong 2 — Restoration Testing (Minimum Annual): No document in the reviewed set explicitly commits to (a) performing restoration tests of backups, or (b) doing so at any defined frequency (annual or otherwise). The DPA Security Programs section references "regular testing of the key controls, systems and procedures," but this language is too generic to be read as a specific commitment to backup restoration testing. PCI DSS Level 1 certification (confirmed annually by a QSA) and annual SOC 1/2 reports may implicitly encompass backup recovery testing through their respective control frameworks, but Stripe makes no contractual commitment to restoration testing in the reviewed terms—and in any event, PCI DSS scope is limited to the cardholder data environment rather than all data Stripe processes.

Conclusion: The topic is addressed, but with materially weaker coverage than the acceptable position requires. Backup creation is confirmed; restoration testing cadence is not contractually committed to. This is a YELLOW finding under the functional-equivalence standard: the contract addresses the same subject matter (backups and restoration) but provides narrower protection (no explicit testing obligation or minimum annual frequency). At HIGH weight, this requires documented legal review. A contract supplement or security addendum explicitly requiring periodic restoration testing (minimum annual) would be recommended.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Stripe implements measures to ensure the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, including:
- database repl…"
2. "The security program includes:
- documented policies that Stripe formally approves, internally publishes, communicates to appropriate personnel and reviews at least annually;
- documented, clear ass…"
3. "To the extent applicable to the Services, Stripe is responsible for providing the Services in a manner that is consistent with the highest certification level (PCI Level 1) provided by the PCI-DSS req…"

> *"Each party will maintain commercially reasonable administrative, technical, and physical safeguards designed to protect data in its possession or under its control from unauthorized access, accidental loss, and unauthorized modification."*
> — Stripe Services Agreement - General Terms

Breach Indemnification

AI Comment: The Stripe Services Agreement and DPA do not contain an explicit indemnification obligation from Stripe to User for Stripe's own data breaches, security incidents, or the breaches of Stripe's subprocessors. Instead, Stripe provides a general liability framework that falls materially short of the playbook's acceptable position of "indemnification."

Indemnification is asymmetric and limited to IP Claims. Section 9.1(a) requires User to indemnify Stripe for User's own breaches and misconduct. Section 9.1(b) is the only provision that runs indemnification obligations from Stripe to User, and it is expressly limited to IP Claims — it does not cover data breaches, security incidents, or operational breaches. There is no general breach indemnification from Stripe to User anywhere in the Agreement or DPA.

Data Incident Losses are explicitly included within the aggregate liability cap. Section 8.4 caps a party's total aggregate liability — "including Data Incident Losses" — at fees paid in the 12 months preceding the first triggering event. The "Excluded Claims" definition (which carves out gross negligence, fraud, willful misconduct, and confidentiality breaches from the cap) does NOT carve out Data Incident Losses. This means losses from data breaches caused by Stripe's ordinary negligence are capped at a potentially modest amount, rather than being subject to an uncapped indemnification obligation. The explicit bracketing of Data Incident Losses within the cap — not the carve-outs — is a deliberate and significant structural choice.

Subprocessor accountability exists as capped liability, not indemnification. DPA §3.2(b) provides that if a Sub-processor fails to fulfill its data protection obligations, "Stripe will remain liable to User for the acts and omissions of its Sub-processor to the same extent Stripe would be liable if performing the relevant Services directly under this DPA." This is meaningful — Stripe accepts full accountability for subprocessor failures without limiting liability to the subprocessor's direct breach — but it is liability language, not indemnification. Stripe would be responsible for the same damages as if it performed the services directly, subject to the same aggregate cap that applies to Stripe's own conduct.

DPA Disclaimer further limits Stripe's exposure. DPA §3.4 disclaims Stripe's (and its Affiliates') liability for any claim made by a Data Subject arising from Stripe's acts or omissions to the extent Stripe was acting in accordance with User's Instructions. This reduces Stripe's overall exposure in instruction-following breach scenarios.

EEA SCC liability provisions apply conditionally but remain capped. For EEA-originating transfers, the Data Transfers Addendum Module 2 (Clause 12) provides that each party is liable to the other for damages caused by any breach of the EEA SCCs. However, DTA §8.6 expressly provides that the Agreement's "limitations and exclusions of liability" apply to the EEA SCCs to the greatest extent permitted by law, preserving the aggregate cap even for SCC-governed transfers.

Conclusion. The acceptable position — indemnification from Stripe for its own breaches and subprocessor breaches — is not met. Stripe provides: (i) no explicit breach indemnification to User; (ii) capped general liability for data incidents (subject to the 12-month fees cap); (iii) pass-through subprocessor accountability (as capped liability); and (iv) carve-outs from the cap only for gross negligence, fraud, willful misconduct, and confidentiality breaches (explicitly excluding Data Incident Losses from those carve-outs). A true indemnification would include defense obligations, hold-harmless protection, and potentially uncapped recovery. This High weight gap requires review and documented senior legal justification before proceeding.

— Superseding reasoning —
No superseding determination applies between the identified PIFs. The DPA §7(a) establishes that the DPA prevails over the Agreement for Personal Data Processing conflicts, which means DPA §3.2(b)'s subprocessor accountability framework governs over any conflicting Agreement provision for personal data scenarios. However, there is no direct conflict to resolve:

the Agreement sets the general liability cap (including Data Incident Losses), and the DPA adds subprocessor accountability without specifying a different cap. The provisions are complementary, not conflicting. DPA §3.2(b) is the more specific governing provision on subprocessor liability for personal data and is applied as the governing text on that sub-topic.

— Note —
The AI cited 5 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Subject to Section 9.2 (Limitations on Indemnity), User will indemnify Stripe, its Affiliates, and their directors, employees, and agents for all Losses arising from User's use of the Services or Stri…"
2. "(b) IP Indemnities.

(i) Indemnity. Subject to Section 9.2 (Limitations on Indemnity), each party will indemnify the other party, its Affiliates, and their directors, employees, and agents for all Los…"
3. "Except for Excluded Claims, a party's total aggregate liability for damages and Losses for all claims arising out of or relating to the Agreement (including Data Incident Losses) is limited to the tot…"
4. ""Excluded Claims" means: (a) a party's gross negligence, fraud, or willful misconduct, (b) User's breach of Section 1.2 (Restrictions), (c) a party's breach of Section 6 (Confidentiality) but excludin…"
5. "Notwithstanding anything to the contrary in the Agreement, including this DPA, Stripe and its Affiliates will not be liable for any claim made by a Data Subject arising from or related to Stripe's or …"

> *"If a Sub-processor fails to fulfill its data protection obligations under that agreement, Stripe will remain liable to User for the acts and omissions of its Sub-processor to the same extent Stripe would be liable if performing the relevant Services directly under this DPA."*
> — Data Processing Agreement

Arbitration or other dispute resolution process

AI Comment: The Stripe Services Agreement comprehensively restricts the method of dispute resolution across all identified jurisdictions, directly conflicting with the acceptable position of "no limitation as to method of dispute resolution."

Under § 11.4(a)(i) of the General Terms, binding arbitration before a single arbitrator is the exclusive mechanism for virtually all disputes—statutory, common law, and contractual alike. The sole carve-out is for IP Rights claims (§ 11.4(a)(ii)), which are channeled to specific designated courts, not left to free choice of method.

Regional Terms supersede § 11.4(a)(i) for specific jurisdictions per the contract's own hierarchy provision (§ 13), but substitute equally or more restrictive mandatory mechanisms:

• United States (§ 13.2.1 / § 13.2.4): Mandatory AAA arbitration in San Francisco, California; Federal Arbitration Act governs; class action waiver applies—individual basis only.
• European Economic Area (§ 13.2.1 / § 13.2.3): Mandatory ICC arbitration in Dublin, Ireland; class action waiver from preamble does NOT apply—a relative improvement, but mandatory arbitration remains.
• United Kingdom / Switzerland / Gibraltar (§ 13.2.1 / § 13.2.3): Mandatory ICC arbitration in London, England; class action waiver from preamble does NOT apply.
• Brazil (§ 13.2): Section 11.4 is explicitly superseded; exclusive court jurisdiction in the Judicial District of São Paulo—the most favorable provision in that it restores court access, but still mandates a single exclusive forum.
• All other regions (Canada, Hong Kong, India, Indonesia, Japan, Malaysia, Mexico, Singapore, Thailand, UAE, etc.): Each prescribes mandatory arbitration under region-specific rules and forums.

In no identified jurisdiction does the Agreement leave the method of dispute resolution open to User's selection. Even the Brazil provision, the most favorable, merely substitutes one mandatory mechanism (exclusive court jurisdiction) for another (arbitration). The applicable jurisdiction cannot be definitively confirmed without knowing User's Stripe Account Country, which introduces uncertainty about which specific mandatory forum and rules govern—but all possibilities fail the acceptable position.

Classification: RED at Medium weight, requiring documented justification. Practical impact: User cannot freely choose arbitration, mediation, litigation, or other ADR methods; the specific forum, rules, and location are all pre-determined by Stripe's Agreement.

— Superseding reasoning —
The Agreement's hierarchy provision (§ 13 of the General Terms) explicitly states that Regional Terms prevail over General Terms in cases of conflict. Accordingly, the general binding-arbitration clause in § 11.4(a)(i) is displaced for users in specific jurisdictions by their respective Regional Terms. For Brazil, § 13.2 goes further and explicitly states "This provision supersedes Section 11.4," removing arbitration entirely and substituting exclusive court jurisdiction in São Paulo. For US, EEA, and UK/CH/GI users, the applicable regional arbitration terms supplant the general clause with jurisdiction-specific arbitral forums and rules. None of these regional substitutions, however, relieves the fundamental limitation: in every case, a single mandatory method (and specific forum) is imposed without User having any choice.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "All disputes, claims, and controversies principally related to a party's IP Rights will be resolved by litigation."

> *"Disputes between User and Stripe are subject to a class action waiver and will be resolved by individual binding arbitration, except as stated otherwise in this Agreement."*

— Stripe Services Agreement - General Terms
"Except as stated otherwise in Section 11.4(a)(ii) or the Regional Terms, all disputes, claims, and controversies, whether based on past, present, or future events, including those arising out of or relating to statutory or common law and the breach, termination, enforcement, interpretation, or validity of any provision of this Agreement, will be determined by binding arbitration by a single arbitrator."
— Stripe Services Agreement - General Terms
"(a) Arbitration will be held in San Francisco, California."
— Stripe Services Agreement - General Terms
"To the extent Law permits, any dispute arising out of or relating to this Agreement, whether in arbitration or in court, will be conducted only on an individual basis and not in a class, consolidated or representative action."
— Stripe Services Agreement - General Terms
"(a) Arbitration will be held in Dublin, Ireland."
— Stripe Services Agreement - General Terms
"(a) Arbitration will be held in London, England."
— Stripe Services Agreement - General Terms
"This provision supersedes Section 11.4. Each party irrevocably submits to the exclusive personal jurisdiction of, and agrees that any dispute, claim, or controversy will be brought before, the Judicial District of São Paulo, State of São Paulo, disregarding any other competent court or authority to settle the dispute, and each party waives all objections to that jurisdiction and venue."
— Stripe Services Agreement - General Terms

Subprocessor Audit Rights

AI Comment: The acceptable position for this playbook item requires User to have the right to audit Subprocessor's systems and their compliance with the DPA. The Stripe DPA and Data Transfers Addendum address the broader topic of Subprocessor oversight, but fall materially short of granting User any direct audit right over Subprocessors' systems or a direct compliance assessment mechanism.

What is provided: DPA §3.1(g) grants User the right to request audit reports or a written security questionnaire regarding Stripe's and its Affiliates' processing — limited to once per year and satisfied in documentation/questionnaire format only. Stripe retains sole control over how this right is fulfilled and may satisfy it by providing documentation rather than permitting inspection. Notably, the scope covers "Stripe's and its Affiliates' Processing" — this does not clearly extend to non-Affiliate third-party Subprocessors. DPA §3.2(b) requires Stripe to contract with each Subprocessor to impose comparable DPA obligations, and renders Stripe fully liable for Subprocessor failures, providing an indirect liability backstop. The DPA Exhibit confirms the questionnaire-based audit mechanism is confined to Stripe's own systems and practices. DTA §8.3 explicitly channels the EEA SCC audit right (Clause 8.9, Module 2) through the DPA mechanism — confirming that even under the SCCs, User's audit rights are exercised through Stripe's documentation/questionnaire approach, not through direct access to Subprocessors' systems. DTA Module 2, Clause 9(c) allows User to request copies of Subprocessor agreements (which Stripe may redact for business confidentiality), providing limited contractual visibility but not audit access to Subprocessors' systems.

The gap: No provision in any document grants User the direct right to audit Subprocessors' systems or independently verify Subprocessors' DPA compliance. User's audit right runs only against Stripe. Visibility into Subprocessors is limited to: (i) Stripe's contractual liability backstop; (ii) a Stripe-issued questionnaire about Stripe's own practices (not Subprocessors' systems); and (iii) possibly redacted copies of Subprocessor agreements. The General Terms §11.16 further confirms Stripe remains responsible for subcontractors but does not extend any audit right to User.

Classification rationale — YELLOW: The topic of Subprocessor compliance assurance is addressed through Stripe's contractual obligations to Subprocessors and its liability backstop, but the protection provided is materially weaker than the acceptable position. The playbook requires a direct right to audit Subprocessor's systems; what exists is an indirect model (Stripe audits or holds Subprocessors contractually, User audits Stripe via questionnaire). For a Medium-weight item, this finding warrants documented justification if the indirect model is acceptable to the organization.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "following User's written request, contribute to audits or inspections by making audit reports available to User. Following this request, and no more frequently than once annually, Stripe will promptly…"
2. "Upon written request, and no more frequently than annually, Stripe will complete a written data security questionnaire of reasonable scope and duration regarding Stripe's business practices and data t…"

"(b) Stripe will enter into a written agreement with each Sub-processor that imposes on that Sub-processor obligations comparable to those imposed on Stripe under this DPA, including the obligation to implement appropriate Data Security Measures. If a Sub-processor fails to fulfill its data protection obligations under that agreement, Stripe will remain liable to User for the acts and omissions of its Sub-processor to the same extent Stripe would be liable if performing the relevant Services directly under this DPA.

"
— Data Processing Agreement
"_Clause 8.9 of the EEA SCCs, Module 2 (Transfer: Controller to Processor) and Module 3 (Transfer: Processor to Processor): Audit_. User acknowledges and agrees that User exercises User's audit right under Clause 8.9 of Module 2 (Transfer: Controller to Processor) and/or Module 3 (Transfer: Processor to Processor) of the EEA SCCs by instructing Stripe, LLC to comply with the audit measures described in the DPA.

"

— Data Transfers Addendum

"(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

"

— Data Transfers Addendum

Cybersecurity Prevention Systems

AI Comment: The playbook item requires Stripe to maintain adequate systems and processes preventing unauthorized access to, disclosure of, or loss of User data. Stripe addresses all three dimensions of this requirement explicitly and comprehensively across multiple documents. No exception documentation is required for this HIGH weight item.

UNAUTHORIZED ACCESS: The DPA Data Security Exhibit mandates technical access controls including MFA per NIST 800-63B, role-based access rights with differentiated profiles, access monitoring and logging, automatic lockout, and break-in-attempt monitoring. Physical controls at third-party data centers include 24x7 Security Operations Center monitoring, CCTV, electronic access systems, and trained security staff. Personnel controls include pre-employment background checks, annual security training, and prompt access revocation upon termination.

UNAUTHORIZED DISCLOSURE: Encryption is applied at multiple points — TLS 1.2 for all external connections, mTLS for internal production networks, and AES-256 for all production data at rest — with cryptographic key access restricted to a limited number of authorized personnel. Disclosure controls ensure Personal Data cannot be read, copied, modified, or transmitted without authorization, with full audit logging of access and changes.

LOSS OF DATA: Availability controls include database replication, backup procedures, hardware redundancy, and a formal disaster recovery plan, designed to restore availability and access in a timely manner following a physical or technical incident.

GOVERNING FRAMEWORK: The DPA Data Security Exhibit — incorporated by reference into the Agreement per General Terms §4.1, and referenced directly in General Terms §4.6(b) as Stripe's specific obligation ("Stripe will comply with its obligations in the Data Security Exhibit to the DPA") — provides the detailed governing statement of security requirements. It supersedes the General Terms §4.6 "commercially reasonable safeguards" baseline under the specific-over-general principle. The DPA §7 further confirms DPA provisions prevail over the Agreement for Personal Data processing matters.

INDEPENDENT VERIFICATION: Annual PCI Level 1 QSA certification and SOC 1 & 2 reports provide independent third-party verification that stated controls are implemented and effective — substantially strengthening confidence in adequacy. The Stripe Payments Services Terms §3.7 separately commits to PCI-DSS compliance in the payment processing context.

JURISDICTION NOTE: The governing security provisions in the DPA Exhibit apply regardless of the User's Stripe Account Country. The unresolved jurisdictional question (California / Ireland / England and Wales) does not materially affect this item's classification.

The security framework substantially exceeds the "adequate" threshold — it is comprehensive, specifically documented, independently certified annually by qualified third parties, and addresses all three components of the playbook item. Classification: GREEN. High-weight item. No exception required.

— Superseding reasoning —
The DPA Data Security Exhibit provides specific, detailed security measures that supersede the General Terms §4.6 "commercially reasonable safeguards" general baseline under the specific-over-general principle. Critically, General Terms §4.6(b) itself directs to the DPA Exhibit as Stripe's specific obligation ("Stripe will comply with its obligations in the Data Security Exhibit to the DPA"), confirming the Exhibit as the governing standard for security controls. The DPA §7 further establishes that DPA provisions prevail over the Agreement for Personal Data processing matters. The Exhibit and §4.6 are complementary rather than conflicting — §4.6 provides the general contractual baseline while the Exhibit provides the specific, measurable implementation — and the Exhibit governs as the more specific and authoritative statement of security requirements.

— Note —
The AI cited 6 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Stripe maintains and enforces a security program that addresses how Stripe manages security, including its security controls. The security program includes:
- documented policies that Stripe formally…"
2. "Stripe implements measures to prevent data processing systems from being used by unauthorized persons, including the following measures:
- user identification and authentication procedures;
- ID/pass…"
3. "Stripe applies data encryption mechanisms at multiple points in Stripe's service to mitigate the risk of unauthorized access to Stripe data at rest and in transit. Access to Stripe cryptographic key m…"
4. "Stripe implements measures to ensure the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, including:

- database repl…"
5. "To the extent applicable to the Services, Stripe is responsible for providing the Services in a manner that is consistent with the highest certification level (PCI Level 1) provided by the PCI-DSS req…"
6. "Stripe performs periodic vulnerability assessments and penetration testing on its systems and applications, including those that Process Personal Data. Vulnerabilities are managed and remediated in ac…"

> *"Each party will maintain commercially reasonable administrative, technical, and physical safeguards designed to protect data in its possession or under its control from unauthorized access, accidental loss, and unauthorized modification. Stripe will comply with its obligations in the Data Security Exhibit to the DPA."*
> — Stripe Services Agreement - General Terms
> *"Stripe will implement and maintain a written information security program with the Data Security Measures stated in the Exhibit of this DPA."*
> — Data Processing Agreement
> *"Stripe provides the Services in a manner consistent with PCI-DSS requirements that apply to Stripe."*
> — Stripe Services Agreement - Services Terms

Documents

Title	URL	Type	Scraped At	Replaced
Stripe Services Agreement - General Terms	https://stripe.com/legal/ssa	text/markdown	2026-07-11T19:57:31.620Z	No
Stripe Services Agreement - Services Terms	https://stripe.com/legal/ssa-services-terms	text/markdown	2026-07-11T19:57:44.518Z	No
Data Processing Agreement	https://stripe.com/legal/dpa	text/markdown	2026-07-11T19:58:03.111Z	No
Data Transfers Addendum	https://stripe.com/legal/dta	text/markdown	2026-07-11T19:58:10.503Z	No
Prohibited and Restricted Businesses | Stripe	https://stripe.com/legal/restricted-businesses	text/markdown	2026-07-11T19:58:20.211Z	No
Privacy Policy	https://stripe.com/privacy	text/markdown	2026-07-11T20:01:52.007Z	No

Beyond-Playbook Findings

Pre-Emptive Waiver of All Claims Arising from Terminated Merchant List Placement [HIGH] — § 3.6 (Data Sharing) — Stripe Payments Terms

Section 3.6 of the Stripe Payments Terms requires User to pre-emptively waive any claim against Stripe arising from Stripe's sharing of User information with Payment Method Providers and Payment Method Acquirers — explicitly including placement on a 'terminated merchant list.' Being placed on a terminated merchant list (such as Mastercard's MATCH list) is one of the most severe commercial consequences a merchant can suffer: MATCH-listed merchants are typically unable to obtain payment processing from any Mastercard or Visa acquirer for up to five years, potentially crippling their business. By signing this Agreement, User prospectively surrenders the right to challenge even an erroneous or unjustified MATCH listing resulting from Stripe's sharing practices. This is an asymmetric risk allocation with potentially existential business consequences. Litigation around MATCH listings and merchant termination has been an active area in US courts, reinforcing that this waiver has real-world significance. Reviewers should assess whether User's risk profile makes this pre-waiver acceptable, and whether insurance or contractual remedies elsewhere (e.g., indemnification for Stripe's negligent sharing) could serve as mitigants.

Financial Provider Terms (Visa, Mastercard, etc.) Automatically Supersede Negotiated Agreement [MEDIUM] — § 2.4 (Financial Providers) — Stripe Financial Services Terms

The Stripe Financial Services Terms provide that where any provision of the Agreement conflicts with Financial Provider Terms — defined to include card network rules (Visa Rules, Mastercard Rules, American Express Operating Guide, PCI Standards, and Payment Method Terms) — the Financial Provider Terms will prevail. This is a blanket dynamic incorporation clause: Visa, Mastercard, and other card networks can and do modify their rules unilaterally and without advance notice to merchants (see also § 3.4(a) of Stripe Payments Terms: 'Each Card Network may amend its Card Network Rules at any time without notice to User'). The combined effect is that a material portion of User's legal obligations under this Agreement can change unilaterally, without User's knowledge or consent, at any time. This is structurally distinct from standard SaaS modification clauses — the modifying party (Visa, Mastercard) has no direct contractual relationship with User and no accountability to User. Users in the payments space must accept some degree of card network rule compliance, but the blanket supersession provision without any floor of protection for User is notably broad.

Stripe May Unilaterally Demand a Personal or Parent Company Guarantee [MEDIUM] — § 3.5 (Credit Support Requirement) — Stripe Financial Services Terms

Section 3.5 of the Financial Services Terms authorizes Stripe to require User to provide a guarantee — including a personal guarantee, parent company guarantee, or bank letter of credit — in a form and substance that satisfies Stripe. Stripe's sole discretion governs both the trigger and the form. If User is unable to satisfy the requirement on demand, Stripe may suspend or terminate access to the Services. This provision is structurally unusual in SaaS payment processing agreements: the ability to demand personal guarantees is typically found in lending and credit agreements, not operational vendor contracts. For any organization that is a subsidiary, the prospect of a parent guarantee demand should be escalated to parent company counsel and treasury. For founders or sole proprietors, personal guarantee exposure is existential. There is no defined trigger — Stripe can demand the guarantee at any time at its discretion — and no cap on the guarantee amount, creating open-ended financial exposure. Negotiating a cap tied to historical transaction volume or a sunset on the demand right would be a market-reasonable mitigation.

Reviewers

Name	Current Step
Acme Tenant Admin	ANALYSIS