[Your firm name and logo]

[CPA firm name]
[Firm address]
[Date]
[Service organization legal name]
Attention: [CISO or CEO name, title]
[Address]
Re: SOC 2 [type 1 / type 2] examination of [system name]

Dear [Name],

The engagement
You have engaged [CPA firm name] to examine management's description of [Service organization legal name]'s [system name] system and the suitability of the design [and operating effectiveness] of its controls, based on the description criteria and the trust services criteria for [security / availability / confidentiality / processing integrity / privacy]. We will perform the examination under the attestation standards established by the AICPA.

Scope
The scope is set out in the attached table: the system and its boundaries, infrastructure and locations, the trust services categories, the report type, the [as-of date (type 1) / examination period from (start date) to (end date) (type 2)], and each subservice organization with the carve-out or inclusive method. Changes to scope require a written amendment and may change our fee.

Our responsibilities and the limits of an examination
We will plan and perform the examination to obtain reasonable assurance and express an opinion. Because of their nature, controls may not prevent or detect every error or breach, and projections of our conclusions to future periods are subject to the risk that controls change or fail.

Management's responsibilities
Management is responsible for: preparing the system description; selecting the criteria; identifying the risks that threaten the service commitments and system requirements; designing, implementing and operating controls to address them; and giving us access to all relevant information and to the people we need.

Written assertion
Management will give us a written assertion about the fairness of the description and the suitability of design [and operating effectiveness] of the controls, in draft by [date] and in final form with our report. If management will not provide it, we will withdraw from the engagement where the law allows.

Subservice organizations and user entity controls
For each carved-out vendor, management will give us its most recent SOC report by [date]. The description will list the complementary user entity controls and complementary subservice organization controls that the system relies on.

Evidence calendar
Management will deliver policies and procedures by [date]; populations of new hires, terminations, system changes and incidents for the period by [date]; and evidence for each sample we select within [number] business days of the request. Late evidence may move the report date and add fees.

Independence and readiness work (optional)
We will not design, implement, operate or monitor any control in scope. [Our earlier readiness assessment was limited to observations and recommendations; management made all decisions about controls and designated (name) to oversee that work.]

Exceptions and the opinion
Deviations we find will be described in the tests of controls. Depending on their nature, our opinion may be qualified or adverse, and we may withdraw if we cannot obtain enough evidence.

Representation letter
At the end of fieldwork, management will sign a representation letter dated as of our report date.

Use of the report
The report is intended for management, user entities of the system during the period, and their auditors, and for prospective customers who receive it under a confidentiality agreement. You will not post it publicly. Any bridge letter covering the time after the period is management's own statement; we will not issue or sign it.

Fees and schedule
Our fee is [amount] for a [type 1 / type 2] report covering [categories]. Added categories, scope changes or retesting after remediation are billed at [rates]. Fieldwork is planned for [dates], with the report expected by [date].

Signatures
Please sign and return this letter, with the scope table initialled, to confirm these terms.

Sincerely,
[CPA firm name]
[Partner name], CPA, Partner
Signature: _____ Date: _____
Agreed for [Service organization legal name]:
[Officer name], [Title] Signature: _____ Date: _____