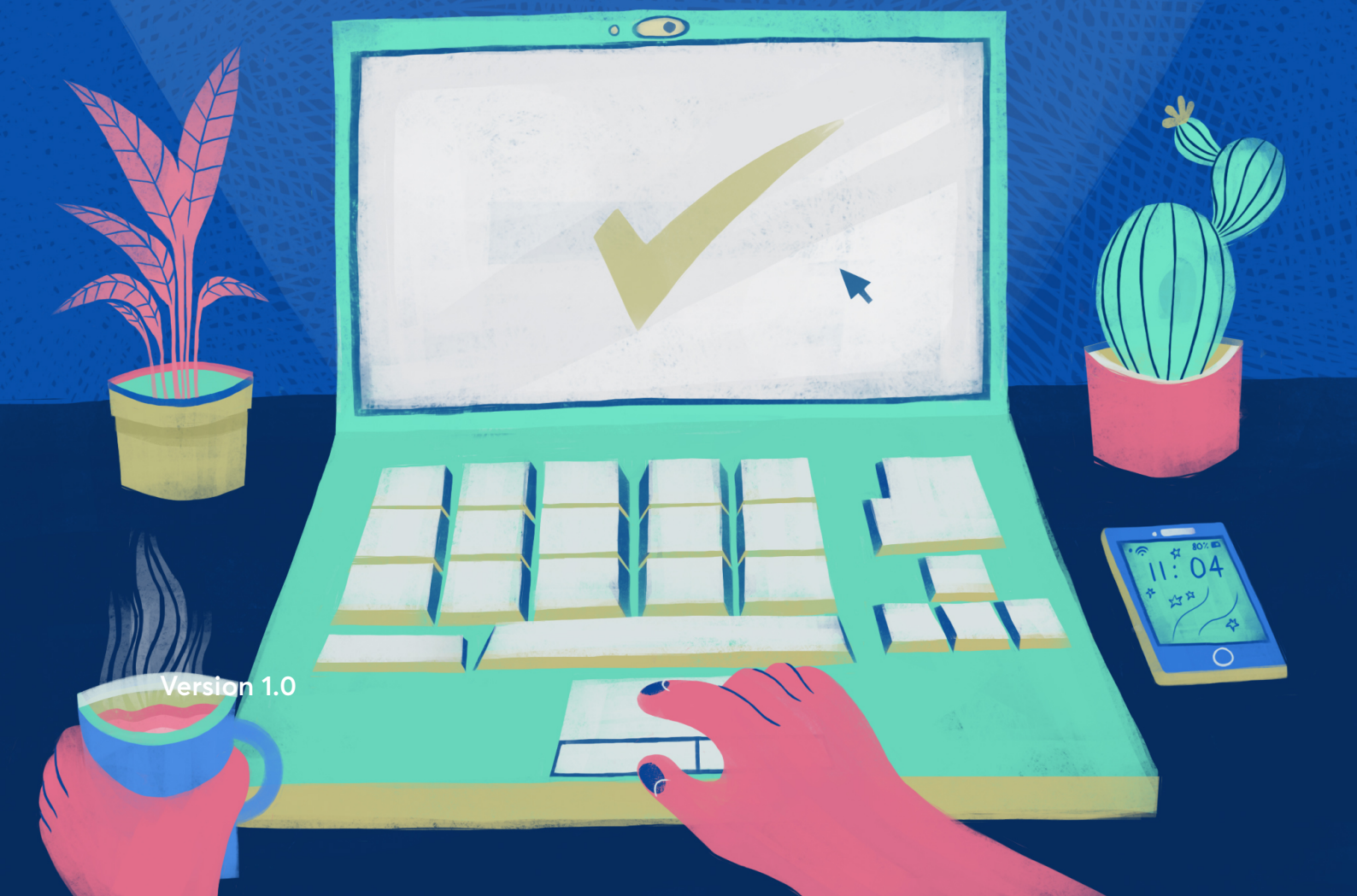
GOCARDLESS

Direct Debit RFP guide



Version 1.0

Contents

Chapter 1 - Overview of the RFP Process

Timeline of the RFP Process

The RFP process involves several important stages and can take around 3 months for a big company. This section walks you through a suggested structure for the process.

A RFP should maximise your chances of picking the right provider. Initially, you'll have a set of requirements that you want to filter providers on. However, once you've filtered out the obviously bad fits, you will still have a couple of providers that could plausibly be the best one for you. Thus, you'll want to look at the shortlist in more detail before coming to your decision.

The RFP Process in detail

The table below provides a suggested structure for your RFP. The timings are suggested on the assumption that you are a large company with multiple stakeholders, which will require a lot of planning and a more drawn-out decision-making process. Using this estimated timing, the process should take just under 3 months; however, this could be significantly shorter for smaller companies so feel free to adjust the timescales accordingly.

Stage	Day	Description
Ask providers to sign NDA	0	You will probably share some confidential information with providers about your company (e.g. projected volumes) in order to get pricing information tailored to you; thus, you should ask your providers to sign an NDA to ensure that you are commercially covered.
Distribute RFP to providers	5	Once the provider has signed an NDA, email them the RFP with a schedule and all the information they need to give you a comprehensive set of answers.
Get confirmation & NDAs from providers that intend to participate	10	Some providers may rule themselves out because they cannot meet the requirements laid out in the RFP. Thus, require providers who intend to participate to explicitly opt in by a certain date.

RFP deadline	30	This is the deadline for providers to submit their answers to you. You should allow a 'questions' phase here as well; questions should be submitted to the person leading the RFP process, in a set template, and these questions and answers should be shared with the entire provider list to ensure that everybody has access to the same information.
Internal shortlisting period	50	You will want to run an internal process to shortlist the top 3 providers based on the information you have been given. More detail on this 'evaluation' phase is below.
Notify providers whether they have made the shortlist	52	Email providers informing them if they have been selected for the next stage. For those that have, schedule meetings for the next stage, ensuring that you explain who will be attending and what you will be looking for.
Follow-up meetings with shortlisted providers	73	Conduct follow-up meetings with your shortlisted providers. We explain on this page (gocardless.com/guides/rfp/evaluating-proposals/) what you should be looking for here.
Decision-making	87	Internal scoring and meetings to make the final decision.
Reference-checking, due diligence and further Q&A	101	Get customer references, perform due diligence on the company, and resolve any final questions with your chosen company.
Communicate final decision	115	Communicate the final decision to your shortlist; commence residual legal discussions with your chosen provider.

Download a sample RFP

Our downloadable RFP has a list of suggested questions for your Direct Debit provider. You can edit it or use it as a template.

A comprehensive RFP that clearly spells out your business' requirements is an essential first step in identifying and partnering with the right payments provider. By asking the right questions throughout the RFP process (gocardless.com/guides/rfp/process), you will be able to compare competing providers and identify the best possible solution to fully meet your requirements.

To save you the work, we've made an RFP you can use for your procurement process, covering all of the dimensions you should care about when choosing a direct debit provider.

Please note: the questions suggested in this guide are intended as a starting place for writing your own RFP. They're provided for general information only: they're not intended to be prescriptive or to provide legal advice. We suggest working closely with your management to develop an RFP that is tailored towards the specific requirements of your business.

You'll need Microsoft Excel 2007 or newer to open the sample RFP.

Chapter 2 - What to include in a Direct Debit RFP

Overview

The RFP process should give you a sense of how good each payments provider is for certain functional and non-functional requirements.

A RFP should enable you to decide whether a payments provider meets all the requirements you have. It should also help you to get a sense of how good they are along several dimensions. As a place to start, we've created a sample RFP which can be downloaded here (gocardless.com/guides/rfp/sample-rfp).

In general, you should be assessing companies along the following dimensions:

1. Do they meet your functional requirements?

- Payments-specific requirements
- Technical requirements
- Integration with existing systems

2. Do they meet your non-functional requirements?

- Commercial requirements
- Financial requirements
- Security requirements
- Resilience requirements

We give a high-level overview of what you should be looking for in each of these categories below. For a detailed breakdown of the kind of questions you should be asking, we recommend looking at the sample RFP (gocardless.com/guides/rfp/sample-rfp).

Payments-specific requirements

These are requirements to do with the type of payment method. How you evaluate these answers will depend on how your business takes payments.

For example, whether you prefer a hosted or embedded payment page may depend on the level of control you require over the user experience. A hosted payment solution will enable you to take

payments without needing to touch sensitive financial data. However, it will also mean that you will have less control over the user experience and may need to include the provider's branding in your payment pages. Embedded payment pages let you maintain control but you will need to comply with onerous legal and technical PCI/AUDDIS requirements.

Ideally a provider will offer low failure rates, the ability to take and settle payments as often as you like and regular updates on payment statuses.

For Direct Debit, the types of questions you might want to ask are:

- Does the system allow you to set-up mandates electronically?
- Does the system allow you to take payments on any date?
- Does the system inform you when payments fail or are charged back?
- Can you take variable payments using the system?
- How does signing customers up work? Can this be done over the phone?
- What are the typical failure rates seen for companies that they serve similar to yours?
- Do you own the user experience or does the system require the provider's brand to be featured as well?
- How frequently are funds settled?

See a full list of payment-specific requirements and explanations here.

Technical requirements

These are requirements that determine how efficient and effective the provider is from a technical point of view. Ideally, you will want to find a provider with a simple modern REST API, helpful client libraries, clear documentation and great technical support. If you love your developers, it might even be worth checking out some of the more particular features of the API; such as versioning, pagination and URL structure.

In particular, you will want to know things like:

- Does the provider have a REST API that you can connect with?
- How does the API work?
- Does the API provide real-time information, or does it work in batch?
- Does the API provide webhooks on events such as payment failures?
- Is the API rate limited?

See a list of technical requirements and explanations here.

Integration with existing systems

This will vary depending on what systems you use, but generally speaking, you will want to find a solution which integrates with your current internal systems. This will save you time upfront as well as on an ongoing basis.

The types of questions you might want to ask are:

- Does the provider integrate with any of our current internal systems? (e.g. Zuora, Salesforce). This includes:
    - Billing
    - CRM
- If not, does the provider have a REST API that your partners can use to develop an integration?
- What can the provider do to make processes more efficient where an integration is not possible? e.g. can it support agents using a dashboard to perform reconciliation? How will the process work?

Commercial requirements

Here, you will want to know the pricing of the service. Some providers may offer low transaction costs but charge additional fees for hidden extras. Ideally you'll want to find a provider with a superior service at the lowest cost. Make sure you compare fully-loaded costs not just transaction fees by asking questions like:

- How does the pricing vary as your number of transactions scale?
- How much will the cost be, all-in, per year?
- What does the provider charge for:
    - Set-up
    - Monthly/yearly fees
    - Per transaction
    - Per new payer
    - Per failed payment
    - Per chargeback
    - Per file submission (if applicable)
    - For training / installation
- Are there any other charges?
- Does the provider pay out all funds to you or do they retain any in case of chargebacks?

See a list of pricing and commercial questions here

Financial requirements

Financially, you will want to understand how funds will flow to you. This will vary depending on whether your provider offers "facilities management" or "managed administration".
With facilities management, you will have your own SUN (gocardless.com/direct-debit/service-user-numbers) therefore the funds will typically flow directly to you.

With managed administration, the bureau will submit and manage payments on your behalf through their SUN. Payments will therefore go via the bureau's bank account and will usually take a few days to reach your account.

Which of these options is right for you will depend on your business - managed administration will work out significantly cheaper, however, if you need to have full control over the payment process and user experience you may want to consider a provider which offers facilities management. Either way make sure you understand the flow of funds and consider how this will work with your business.

- How often does the provider pay out funds to you?
- What is the flow of funds, end-to-end?
- Does the provider hold funds at any point, and if so, why?
- How does reconciliation work? i.e. walk through the money flows for a payment failure from end to end.

See a suggested list of finance questions here.

Security requirements

Security is of paramount importance when picking a provider, particularly when it comes to payments. You'll want to find a provider who can offer a proven high level of security. Broadly speaking, you'll want to know:

- Has the provider been penetration tested in the last 6 months?
- What were the results of that report?
- How often is a penetration test performed?
- Does the provider use HTTPS? SSL encryption?
- Has the provider had any security breaches in the past, and if so can they detail them?
- How does the provider's physical security work? i.e. guards, access control etc..

The sample RFP we provide has a full list of questions vetted by our security and technical team.

Resilience requirements

Resilience refers to the availability of the service electronically as well as the ability of the service to stay up in the event of an adverse event e.g. a failure at a data centre. Ideally a provider will have over 99.99% uptime and will have back-up systems in place to ensure this doesn't worsen.

You will want to ask about:

- Uptime records in the last year.
- How the provider ensures uptime in the event that one of its centres fails, e.g. having an alternate site.
- What the uptime SLA is.
- What the event resolution time SLA is, and who your contact will be.
- Does the provider use cloud hosting or host locally? If the latter, ask them to explain how physical security works.
- If cloud hosted, explain who the provider is and why that one was chosen.

See our suggested list of questions regarding the Service Level Agreement (SLA) and business continuity

Functional Requirements

A list of functional requirements and questions for your Direct Debit provider.

A RFP should include questions relating to how your business wants to collect payments.

Suggested questions for a Direct Debit provider include:

	Question	Explanation
1.	Does your service allow us to create Direct Debit mandates (gocardless.com/direct-debit/mandates) electronically?	It's important that mandates can be created electronically, and not just via paper.
2.	Does your service allow us to create DD payments electronically?	It's important that mandates can be created electronically, and not just via paper.
3.	Describe how the customer flow would work and specify whether you provide a whitelabel option and/or a hosted option for online payment pages.	You should know how the customer flow works from end-to-end. This will be any of the below three options; which one you prefer depends on how much control you require over the customer experience. • A 'hosted' option - Like Paypal, the customer is redirected to the payment provider's site and then ends up back at your site. • A 'whitelabel' option - The customer stays on your site the whole time, allowing your brand to be front and centre. • A mixture - e.g. an iFrame that stays on your site, but is actually a 'window' to the payment provider's site.

4.	Who stores the bank details collected from the customer?	You ideally don't want to store bank details yourself for security reasons.
5.	Describe how the service provides information on the status of mandates, payments etc.	Providers will either send you files with reports (a more manual option) or send them to you via their API in the form of 'webhooks' which allows full automation to take place. If you want full automation, you should look for the latter.
6.	Describe the flow if a payment fails.	The key here is to know how you're informed of a payment failure; you want to know whether this requires a manual process or is fully automated, and you should ensure that nothing can go wrong with a customer e.g. a payment fails 'silently'. A fully automated solution is preferable as it minimises human error.
7.	Does your service allow sign-ups (a) online (b) by phone (c) in person?	Depending on your requirements, you may need to sign up customers through multiple channels. Some providers don't support all of these.
8.	How long does a payment take from creation to being taken from the customer's account to being paid out to us? Describe in as much detail as possible.	This is more for your information than anything else, and allows you to plan out billing cycles i.e. if you want the customer to be charged on day X, on what day do you need to send a payment request to the provider? You may also have requirements around timings.

9.	How soon are we notified of any failures that occur? Is this in real-time or batched? How are we notified?	The key here is to know how you're informed of a payment failure; you want to know whether this requires a manual process or is fully automated, and you should ensure that nothing can go wrong with a customer e.g. a payment fails 'silently'. A fully automated solution is preferable as it minimises human error.
10.	Do you manage the interactions with Bacs on our behalf?	Some providers provide lightweight software that still requires you to deal with Bacs yourself, including complicated report processing and submission protocols. Other providers will abstract this away using an API or file submission processes. Generally speaking, you are better off saving time on payment processing by letting the provider take care of this for you.
11.	What happens if the customer cancels the mandate (gocardless.com/guides/posts/cancelling-direct-debit) with their bank? How are we informed?	You should make sure the provider will inform you automatically if the customer cancels a mandate, so you can take appropriate action.
14.	Does the dashboard allow export of relevant data? Explain in detail.	For reporting and for customer service purposes.
15.	Does the dashboard report on money due vs. money paid out?	This is for financial reconciliation, i.e. so that you know where your money is at all times and how much you're due.
16.	Can we search for specific customers using the dashboard?	

17.	Does the dashboard show the payment timeline (gocardless.com/direct-debit/timings) for a specific payment? i.e. date submitted, date collected, date paid out etc.	So that you know what the next action on a payment is and when you will be paid.
18.	Does your service support refunds? Can these be done via the dashboard? Can they be done via an API?	The service should ideally support refunds so that you don't have to develop a separate system for these.
19.	Does your service support partial refunds?	In case the customer was overcharged, for example, and you don't want to refund the whole payment.
20.	What validation do you perform of Direct Debit details?	Look for modulus checking (gocardless.com/guides/posts/modulus-checking), which checks that a bank account and sort code number could be valid. You want these to be done instantly so that any errors are caught in the sign-up form, making for the best customer experience.
21.	Do you support variable payments (gocardless.com/guides/posts/variable-payments)? One-off payments? Recurring subscription payments?	The service should support all types of payments; Direct Debit is a flexible payment method and can support payments taken only once, for example. (Although it is best used for recurring payments).
22.	How do we retry a payment?	You may need to retry a payment if it fails, e.g. because the customer didn't have enough money in their account at the time.

23.	Is your software integrated with any accounting platforms? Specify three.	You want a service that is integrated with software providers, both because it increases convenience and saves you time (e.g. a Zuora integration) and because it signals that the provider has an API that is easy to integrate against, which saves you development time down the road.
24.	What happens if we want to change provider? Is this supported?	Many providers don't help you switch provider or lock you in for a certain amount of time. Ideally, the provider doesn't force you to stay with them for any amount of time and they should help you move off the platform if need be - which is easy with Direct Debits, since they can be transferred between banks (gocardless.com/direct-debit/transferring) without the customer having to do anything.
25.	What steps do you take to minimise payment failures?	The best providers have lower failure rates because of their experience and specialism in Direct Debit. They should be able to give you specifics on how they minimise failures e.g. by optimising submission cycles, gracefully dealing with common bank errors (gocardless.com/direct-debit/receiving-messages), etc.
26.	Does your system enable upgrades/ downgrades of subscriptions without additional customer input?	For the best customer experience, you want the ability to change payment amounts without requiring any more input from the customer.

27.	Who handles notifications for customers? How does this work in terms of the flow?	Depending on how you want the branding to work, you should look for a provider that's flexible here, i.e. helps you set up your own emails to notify customers of payments, or provides an option where the provider does it for you.

Our sample RFP includes all of the questions above and more. You can download it here (gocardless.com/guides/rfp/sample-rfp) and use it as a template for creating your own.

Note: The questions suggested on this page are intended as a starting place for writing your own RFP. They're provided for general information only: they're not intended to be prescriptive or to provide legal advice. We suggest working closely with your management to develop an RFP that is tailored towards the specific requirements of your business.

Technical Requirements

A list of technical criteria to include in a RFP for determining how efficient and effective a payments provider is.

A RFP should list your technical requirements from a payments provider. Ideally, you'll want to find a provider with a modern REST API, helpful client libraries, clear documentation and great technical support.

Suggested questions to ask your Direct Debit provider include:

Question	Explanation	
1.	Do you have an API?	An API allows you to automate the Direct Debit process, and is particularly helpful if you collect DD details from a website. Without the API, you'd have to get those details into the direct debit system manually, which is labour-intensive.
2.	What protocol is the API based on? (i.e. SOAP, REST)	REST and SOAP are different ways of designing an API that follow established conventions. RESTful APIs are generally considered easier and quicker to integrate against.
3.	What data format does the API transact in? (i.e. JSON, XML)	JSON and XML are different formats for transmitting data. This information helps determine how well the provider fits with your current technology stack.

4.	Is the API rate limited? Specify the limit. Does the API return the remaining number of request tokens with each request?	A rate limit is a way of ensuring that someone doesn't overload an API - it limits the number of requests to an endpoint. Having one generally ensures that an API is robust and is unlikely to be brought down by too many requests. Specifying the number of remaining tokens allows you to know how many 'requests' you have remaining.
5.	Does the API enforce HTTPS/TLS or does it accept unsecured HTTP requests?	Enforcing HTTPS/TLS is preferred for security reasons.
6.	What authentication protocol does the API use?	Worth knowing for security reasons.
7.	How is version control / backwards compatibility enforced in the API? How does a customer communicate the version they are using to you? (e.g. using the 'Accepts' header)	Breaking changes should be minimised and handled gracefully (e.g. by using headers and versioning). This ensures your integration will function at all times.
8.	How does the API inform us of events, e.g. a payment failure? Is it webhook-based or does it use batched file transfers?	Webhooks are preferred because they are real time, whereas batched file transfers mean you will be less responsive to e.g. payment failures.
9.	Do you enable modulus check (gocardless.com/guides/posts/modulus-checking) via the API?	The provider should allow you to modulus check details you collect on your site to prevent false details from being submitted. (A modulus check is a numerical check against the bank account number & sort code to make sure the combination is possible. It reduces the error rate on checkout pages)

10.	Where a mandate or payment fails, does the API provide us notification of the reason why? Describe how this is done.	The API should provide reason codes to allow you to program the appropriate response, e.g. for insufficient funds you'll want to contact the customer rather than automatically retrying the payment.
11.	Are your list/index endpoints paginated?	This feature means that for large numbers of payments or customers, you get data in a graceful way that's easy to work with.
12.	Is your API documented online? Please provide a link.	APIs should be documented, ideally online, and the quality of documentation is important to ensure a smooth and quick developer integration with your website.
13.	Can we store custom IDs against mandate objects?	This facilitates integration into other systems e.g. Salesforce by allowing you to match objects in one system to another.
14.	Does your API enable the set-up of recurring subscriptions? (i.e. where you handle the timing logic)	This feature is desirable in case you want to 'set it and forget it' for e.g. annual recurring subscriptions.
15.	Does your API support the use of dynamic descriptors on the customer's statement? Is this on a per mandate basis only, or do you also allow this on a per payment basis?	For various reasons you may want to set different references per payment and/or per mandate; you should check that the API allows you to do this if you have this requirement.
16.	Do you return HTTP status codes with each response?	This allows graceful error handling.

Our sample RFP includes all of the questions above and more. You can download it here (gocardless.com/guides/rfp/sample-rfp) and use it as a template for creating your own.

Note: The questions suggested on this page are intended as a starting place for writing your own RFP. They're provided for general information only: they're not intended to be prescriptive or to provide legal advice. We suggest working closely with your management to develop an RFP that is tailored towards the specific requirements of your business.

Pricing & commercials

A list of pricing-related questions to include in your RFP.

When writing a RFP, it's important to ask detailed questions about the pricing of a service. Some providers could offer low transaction costs but may charge additional fees for hidden extras. To compare fully-loaded costs, you'll want to ask questions like the following:

	Question	Explanation
1.	What setup fee do you charge?	All of these questions are designed to ensure you get the maximum commercial information to make an informed decision with. In particular, some providers do not quote the bank fees as part of their bid, which is a misleading picture of cost.
2.	What monthly fee do you charge?	
3.	What fee do you charge per transaction? Does this change as our transaction numbers scale?	Transaction fees should ideally decrease as you scale to take account of this.
4.	What fee is there per DDI setup (gocardless.com/direct-debit/submitting)?	
5.	What fees do you charge for: (a) Chargebacks (gocardless.com/direct-debit/guarantee) (b) Failures (gocardless.com/direct-debit/receiving-messages)?	
6.	What fee do you charge for file submission?	File submission' is the cost of submitting a DD file.
7.	What fee do you charge for training?	

8.	What fee do you charge for ongoing support?	
9.	What fee do you charge for refunds?	
10.	Are there any additional fees charged apart from the types specified in questions 1-8? (Including fees charged by the bank, one-off consulting fees that we are likely to incur, etc.)	Bank fees are the fees you pay to your bank if you choose to become a DD originator yourself and use someone's software to submit yourself. You should ensure you account for the cost of these when comparing the total cost of different providers.
11.	Given the volumes we specify, what is the all-in monthly cost of the service? Annual cost?	

Our sample RFP includes all of the questions above and more. You can download it here (gocardless.com/guides/rfp/sample-rfp) and use it as a template for creating your own.

Note: The questions suggested on this page are intended as a starting place for writing your own RFP. They're provided for general information only: they're not intended to be prescriptive or to provide legal advice. We suggest working closely with your management to develop an RFP that is tailored towards the specific requirements of your business.

Service Level Agreement & Support

A list of questions to ask your Direct Debit provider about the Service Level Agreement (SLA) and customer support.

Suggested questions to ask your Direct Debit provider include:

	Explanation	Question
1.	Will we be given a dedicated account manager?	Self-explanatory.
2.	What hours will the account manager be reachable?	You should ensure that you can reach someone in an emergency and/or if the service goes down.
3.	Do you provide UK-based support?	Preferable so that they keep the same hours as you.
4.	What hours is your support desk available?	Self-explanatory.
5.	What is the SLA for response time if your service goes down or there is an issue with any of our Direct Debits?	The provider should commit to informing you of issues within a certain window. You should aim for the same day at least. A resolution plan should also follow.
6.	Describe your response protocols to both minor and major incidents and explain how we will be informed of the incident, resolution steps and preventative actions for future incidents.	You should look for detailed response protocols in both cases and clear resolution and information mechanisms.
7.	What is the target resolution time for minor incidents? Major incidents?	Minor incidents should be resolved within a few hours; major incidents may take longer.

8.	When will maintenance of the website take place? How much notice will we receive when scheduled maintenance takes place?	You should receive at least a week's notice of planned maintenance to allow you to plan around this. Maintenance should always be scheduled.
9.	What is the maximum amount of scheduled maintenance that will take place in a month, in hours?	This should not be more than a few hours per month.
10.	What is the SLA for uptime of your service?	You want at least 'three nines' of availability. A good explanation can be found here.
11.	How do you define/calculate 'uptime' and are there any exceptions e.g. scheduled maintenance?	Scheduled maintenance can be excluded from 'uptime' definition for clarity's sake.
12.	Through what channels can we expect support? (e.g. phone, email, web chat etc.)	Self-explanatory.
13.	What is the process if we wish to move away from your service? What support will be given?	Some providers lock you in for a certain number of years and/or will not provide you with support if you wish to move away. You should look for a provider that helps with this process (known as a 'bulk change').

Our sample RFP includes all of the questions above and more. You can download it here (gocardless.com/guides/rfp/sample-rfp) and use it as a template for creating your own.

Note: The questions suggested on this page are intended as a starting place for writing your own RFP. They're provided for general information only: they're not intended to be prescriptive or to provide legal advice. We suggest working closely with your management to develop an RFP that is tailored towards the specific requirements of your business.

Finance

A suggested list of financial questions to include on a RFP.

Financially, you'll want to understand how funds will flow to you. This can vary depending on whether your provider offers "facilities management" or "managed administration".

Suggested questions to ask your Direct Debit provider include:

	Question	Explanation
1.	Describe how long your organisation has been in operation.	Most of these questions are for due diligence purposes.
2.	Please attach a copy of your latest audited accounts.	For due diligence.
3.	What is your annual turnover?	For due diligence.
4.	What approximate percentage of your turnover is contributed by your two largest customers?	For due diligence.
5.	Has your company taken on any external investment? If so, describe from whom and how much.	For due diligence.
6.	How often do you pay out our funds to us?	You should ensure that this matches your cash flow requirements - a provider that pays out every day is ideal. This question is not relevant if you own the originator number (i.e. because the money will flow straight from customer to you - an arrangement known as 'managed administration'.)

7.	Describe the insurance on (a) client funds (b) the business that you have in place.	For due diligence.
8.	How are client funds stored (if applicable?)	These should be kept separate from the provider's operational funds and ideally the account is fully backed/insured by the sponsor bank to ensure security of funds.
9.	Who is your sponsor bank for access to the DD scheme?	For due diligence.
10.	Describe your Bacs status and regulatory status (e.g. Authorised Payment Institution, Bacs Approved Bureau, etc) along with dates that these were awarded.	For due diligence.
11.	Describe the flow of funds from the customer to us in as much detail as possible, including payment timings.	For due diligence.
12.	Are any of our funds withheld from us e.g. for chargeback and/or failure protection?	Some providers hold a certain % of your funds as a deposit; this should be avoided if possible.
13.	Are you Direct Debit specialists or do you provide a variety of payment methods?	Direct Debit specialists are preferred, particularly for SEPA (gocardless.com/guides/sepa), where the scheme is complex. This will ensure you get low failure rates for payments and expert advice when you need it.
14.	Describe how reporting works with your system i.e. how reports can be generated, in what formats, and what types of data are available.	Reporting should be flexible to enable a full match to your requirements. You should ideally have standard reports that are exportable from an online dashboard/portal and also the ability to construct custom reports either online or via the API.

15.	How do we find out, at a given point in time, how much money is due to be paid out to us?	For financial reconciliation purposes.
16.	How do we match a Direct Debit payout to the transactions included within it?	For financial reconciliation purposes.

Our sample RFP includes all of the questions above and more. You can download it here (gocardless.com/guides/rfp/sample-rfp) and use it as a template for creating your own.

Note: The questions suggested on this page are intended as a starting place for writing your own RFP. They're provided for general information only: they're not intended to be prescriptive or to provide legal advice. We suggest working closely with your management to develop an RFP that is tailored towards the specific requirements of your business.

IT & Data Security

A list of suggested questions to ask your Direct Debit provider about IT and data security.

Security is of paramount importance when picking a provider, particularly when it comes to payments. You'll want to find a provider who can offer a proven high level of security.

The following list of suggested questions have been vetted by our security and technical team:

	Question	Explanation
1.	Describe how access to payments data is controlled (i.e. who can access it, how accessing it works, details of encryption etc.)	In general, these questions are around ensuring that the provider has established practices to ensure the security of payments data. Payments data should be encrypted and difficult to get access to.
2.	Describe your password security guidelines and how these are enforced.	For due diligence.
3.	Has your system been externally penetration tested? If so, please attach a copy of the report (or at least the summary).	A penetration test should be done by an external provider and should be done semi-annually at least; these ensure that any security vulnerabilities are discovered and resolved.
4.	When was your system last externally penetration tested?	For due diligence.
5.	How often is your system externally penetration tested?	For due diligence.

6.	Describe how your application and its associated data is hosted (i.e. cloud, bare metal, local vs. remote, etc.). If you use any external providers, specify them and explain why they were chosen.	For due diligence.
7.	Are your data centres located in the EU? Specify where.	For due diligence.
8.	What software is used to generate Bacs submissions and how is access to these controlled?	For due diligence.
9.	How is physical security ensured? i.e. employee access, designated rooms for servers, etc.	For due diligence.
10.	Describe how the encryption of payment details works, including web-based encryption (e.g. HTTPS).	Ensuring that the data is encrypted from end to end is crucial; transmission over the web should be TLS/HTTPS only, and SSL keys should be used internally and stored securely.

Our sample RFP includes all of the questions above and more. You can download it here (gocardless.com/guides/rfp/sample-rfp) and use it as a template for creating your own.

Note: The questions suggested on this page are intended as a starting place for writing your own RFP. They're provided for general information only: they're not intended to be prescriptive or to provide legal advice. We suggest working closely with your management to develop an RFP that is tailored towards the specific requirements of your business.

Business Continuity

A list of suggested questions to ask your Direct Debit provider about their Business Continuity Plan (BCP).

You should include a section in your RFP asking your payments provider about their Business Continuity Plan (BCP).

Suggested questions to ask include:

	Question	Explanation
1	Do you have a Business Continuity Plan (BCP)? If so, please attach to this RFP. If not, please explain your processes around Business Continuity, i.e. procedures for recovery from a partial or total loss of your services due to a technical failure.	A BCP is a step-by-step explanation of what the process is for restoring data and availability of the service after any adverse event, both major and minor. It should explain the exact steps taken, resolution times, and key risks - in particular, how much data would be lost in a major event.
2	How frequently do you create data backups?	These should be as close to real-time as possible to minimise potential data loss.
3	For how long are these backups retained?	
4	Where are these backups stored?	
5	How are backups secured?	
6	In a disaster event, how long would it take you to restore the system from these backups? Would any data be lost, and if so, how much?	Naturally, you should be looking for an answer as soon as possible and no data loss. 2-4 hours is a good answer here.
7	How are employees kept aware of the BCP?	This should be a quarterly/semi-annual review with the person in charge.

8	How frequently is the BCP reviewed and how do you ensure that it is kept up to date?	This should be quarterly/semi-annually reviewed by a senior team member.
9	Who has responsibility for deciding to invoke the BCP?	This is usually the Head of IT/ Engineering or Security.
10	When was your BCP last tested? Describe how testing took place.	The organisation should have simulated a disaster event to ensure all steps of the process work.
11	Describe your review process in the event of a disaster that required the BCP to be invoked.	The organisation should perform a retrospective and take specific actions to improve the process in case of future adverse events.

Our sample RFP includes all of the questions above and more. You can download it here (gocardless.com/guides/rfp/sample-rfp) and use it as a template for creating your own.

Note: The questions suggested on this page are intended as a starting place for writing your own RFP. They're provided for general information only: they're not intended to be prescriptive or to provide legal advice. We suggest working closely with your management to develop an RFP that is tailored towards the specific requirements of your business.

Chapter 3 - Distributing your RFP

List of Direct Debit providers

Typically, your company will be looking for credit card or Direct Debit payments. We list the relevant providers for Direct Debit below.

Direct Debit specialists

A Direct Debit specialist is a company that only provides Direct Debit (and no other payment method.) It is often worth picking a specialist Direct Debit provider because they are more likely to be experts in the payment method and be able to maximise your conversion, minimise failure rates, and act as trusted advisors. It may also be that they are integrated into other software that you are already using (e.g. Zuora, Salesforce), which argues for using them over a full-service provider.

Direct Debit specialists serving the UK:

Bureaus

- GoCardless
- Fastpay
- Eazipay
- Rapidata
- First Capital Cashflow
- AccessPay
- Eazy Collect
- Smartdebit
- London & Zurich

Management software

- Bottomline
- Fundtech

Full-service providers

The advantage of full-service providers is that they often cover all of your payment needs in one integration. The downside, however, is that you typically have to do more yourself (e.g. to use Direct Debit, you may also need to register with your bank, a process that takes months and can be expensive). Moreover, they often have outdated APIs and may not integrate with your chosen solution, which can cause huge amounts of work and problems further down the line.

Full-service providers serving the UK:

- Adyen
- GlobalCollect
- WorldPay

Evaluating Your Proposals

This section will walk you through how to use the information you've been given to choose the right payments provider for your business.

1. Make a shortlist

Once RFPs have been submitted, you will want to run an internal process to shortlist the top three providers based on the information you have been given. You should rank the providers based on the ideal answers given in the sample RFP - one simple way of doing this would be to assign a rank from 1-5 for each answer, sum up the scores and rank the providers by score.

2. Invite the top three to a round of meetings

You should pick the top three providers and invite them for a round of meetings to make your final decision.

3. Hold stakeholder meetings to evaluate the top three

Set up meetings with the key stakeholders (typically representatives from finance, product, support, IT, and business) and outline to the providers that they should prepare slides explaining why their solution should be chosen, what the key advantages are vis-a-vis other providers, and who will be attending the meeting from your side.

From each RFP, you should have made a list of:

a) Key advantages of using the provider Use the meeting to validate these and ensure that they are true, going into more detail e.g. for particular integrations, are they feature-complete?

b) Key concerns with the provider If they are weak on certain dimensions, use the meeting to probe more into these and find out whether the weakness can be mitigated or additional useful information can be provided on these.
Each provider should be scored using a similar system to before, along several dimensinons. Once the meetings are complete, each attendee should submit their personal evaluations and recommendations on behalf of their part of the business.

4. Make your decision

The leader of the procurement process should make a choice based on these evaluations and then sit down with each of the stakeholders to propose the solution that the business will choose and hear out any objections/concerns which may need to be considered.

Once this process has been completed, you should have a good idea of which provider you wish to go with. There is still a round of due diligence and referencing to be done.

5. Carry out due diligence and referencing

We recommend speaking to at least three customers of comparable size to you and getting references on the business to ensure that they do what they say they can do, and in particular, act with integrity and with the interests of the customer in mind (rather than their own). The usual due diligence process should also be followed, i.e. check that the business is financially stable, do reference checks on the directors, and ensure that the claims they have made with regard to regulation and sponsorship are legitimate.