Freshway Media — Lead Posting Specification

Personal Loan Leads · API v1 · Browser-to-server

Specification version	1.0
Last updated	2026-09-15
Audience	Publishers posting personal-loan leads from the consumer's browser
Support	info@freshwaymedia.com

> If you post from your backend, use the server-to-server specification instead. Home-service posting from the browser uses `POST /v1/home-services/leads`.

---

1. Overview

Freshway Media accepts personal-loan leads over a JSON REST API. The consumer's browser submits a single application per request from your form page; we validate it, run compliance and fraud checks, offer it to our buyer network, and return a decision synchronously in the HTTP response.

A request that returns `200 OK` has been **processed**, not necessarily **purchased**. Read the `status` field to determine the outcome.

We do not support a ping/post flow. There is no separate price-quote call: one request submits the lead and returns the decision.

A publishable key is visible to anyone who views your page source. It is not a secret. Its security rests on origin restriction and rate limiting rather than confidentiality.

The body includes SSN and bank account numbers. A browser post puts those values in the page's network panel, which anyone with the consumer's device can open.

Getting started

1. Request sandbox credentials from info@freshwaymedia.com. You will receive a **publishable** key and your campaign names. If you already post home-service leads, the same keys work here — use a **different** `campaignName`.
2. Send us the exact origins you will post from so we can register them. Register `https://www.example.com` and `https://example.com` separately if you use both.
3. Build and post a request against the sandbox base URL using the example in section 5.
4. Confirm your handling of `accepted`, `declined`, and `duplicate` outcomes, and of validation errors. Sandbox outcomes are not deterministic; handle all three `status` values. See section 10.
5. Request production credentials. Sandbox keys do not work in production.

---

2. Endpoints

Environment	Base URL
Sandbox	`https://sandbox-api.freshwayleads.com`
Production	`https://api.freshwayleads.com`

Operation	Method	Path
Submit a personal-loan lead	`POST`	`/v1/personal-loans/leads`
CORS preflight	`OPTIONS`	`/v1/personal-loans/leads`

TLS 1.2 or higher is required. Plain HTTP requests are rejected; they are not redirected.

Vertical is implied by the URL. There is no `vertical` field in the body.

3. Authentication

Present your publishable key as a bearer token:

```
Authorization: Bearer <your-publishable-key>
```

Key type	Prefix	Where it may be used	Secret?
Publishable, production	`fw_live_pk_`	Browser JavaScript, from a registered origin	No
Publishable, sandbox	`fw_test_pk_`	Browser JavaScript, from a registered origin	No

Your account is identified by the key. Do not send an affiliate identifier in the request body; it is ignored. The same publishable key authenticates both `/v1/personal-loans/leads` and `/v1/home-services/leads`. Use a distinct `campaignName` for each product. Reusing a home-service campaign name here would attribute a loan lead to home-service terms.

A publishable key can only submit leads. It cannot read leads, reporting, or account data.

Publishable keys are restricted to the origins you register. A request from an unregistered origin, or with no `Origin` header, is rejected with `403`. Rotate a publishable key if you see traffic you do not recognize.

A missing, malformed, unknown, inactive, or revoked key, or a key belonging to the other environment, is rejected with `401`. Inactive and revoked keys are indistinguishable from an unknown key in the response.

3.1 CORS

We answer the preflight `OPTIONS /v1/personal-loans/leads` request with `204 No Content`. A registered origin receives the headers below. An unregistered origin, or a request with no `Origin` header, is denied. Preflight is not counted against your rate limit.

The browser sends `Origin`. You do not set that header in `fetch`.

Response header	Value
`Access-Control-Allow-Origin`	The single registered origin that sent the request
`Access-Control-Allow-Methods`	`POST, OPTIONS`
`Access-Control-Allow-Headers`	`Authorization, Content-Type, Accept, X-Request-Id`
`Access-Control-Expose-Headers`	`X-Request-Id, X-RateLimit-Limit, X-RateLimit-Remaining, X-RateLimit-Reset, Retry-After`
`Access-Control-Max-Age`	`86400`

We do not send `Access-Control-Allow-Credentials`, and we never reflect an arbitrary origin.

4. Request headers

Header	Required	Value
`Authorization`	Required	`Bearer <your-publishable-key>` — see section 3
`Content-Type`	Required	`application/json; charset=utf-8`
`Accept`	Recommended	`application/json`
`X-Request-Id`	Optional	Your own correlation id. Echoed back in the response and in our logs.
`Idempotency-Key`	Reserved	Accepted and ignored. Do not rely on it. See section 9.

The browser also sends `Origin`. We use it to enforce your registered origins.

5. Request body

The payload is a flat JSON object using `camelCase` field names.

Do not send `ipAddress` or `userAgent`. We read them from the connection and the request headers.

Conventions

Concern	Rule
Character encoding	UTF-8
Field naming	`camelCase`, case-sensitive
Enumerated values	Lower `camelCase` string values, case-sensitive. Never numeric codes. Never a raw FICO.
Booleans	JSON `true` / `false`. Not `"1"`, `"Y"`, or `"true"`.
Numbers	JSON numbers. Not quoted strings. No currency symbols, thousands separators, or units.
Money	US dollars and cents throughout. Never cents-only, and never with a currency symbol or thousands separator. Amounts you send (`loanAmount`, `monthlyNetIncome`, `debtAmount`) are plain JSON numbers and may include cents: `3500` and `3500.50` are both valid. More than two decimal places is rejected rather than rounded.
Dates	Calendar dates (`dateOfBirth`, `payDate1`, `payDate2`, `employmentHireDate`) are `YYYY-MM-DD` with no time and no timezone. Locale formats such as `04/18/1992` are rejected.
Timestamps	RFC 3339 with a timezone (`submittedAt`, `consentAt`). Prefer UTC with a `Z` suffix and millisecond precision: `2026-09-14T14:32:07.512Z`. A numeric offset (`+00:00`) is also accepted, and fractional seconds are optional.
Empty values	Omit optional fields you have no value for, or send `null`. After trimming, an empty string on an optional field is treated as omitted. An empty string on a required field fails as `required`.
Unknown fields	Ignored, so we can add fields without breaking you. Do not rely on them being stored.
Trimming	Leading and trailing whitespace is trimmed from all string fields before validation.

Field reference

`Required` values: **Required** always; **Recommended** optional but materially improves acceptance rate and price; **Optional** accepted and passed through.

Attribution

Field	Type	Required	Constraints / allowed values	Description
`campaignName`	string	Required	Max 200 chars. Must match one of your active campaign names, which we give you with your keys. Matched ignoring case; surrounding whitespace is trimmed. Do not reuse a home-service campaign name here.	Which of your campaigns this lead belongs to. Determines the commission terms the lead is paid on, so it is required on every request and there is no default, even if you have only one campaign. A name we do not recognize as yours is rejected with `400`; the lead is **not** processed.

`subId`	string	Optional	Max 50 chars	Your own traffic source or sub-affiliate identifier, free-form and not validated. This is for your own reporting breakdowns and does **not** affect attribution or payment: that is `campaignName`.
`submittedAt`	string (date-time)	Recommended	RFC 3339 with a timezone. Must not be more than 24 hours in the past or more than 5 minutes in the future.	When the consumer submitted the form on your property. Defaults to our receipt time if omitted.

Identity and contact

Field	Type	Required	Constraints / allowed values	Description
`firstName`	string	Required	1–50 chars. Letters, spaces, hyphens, and apostrophes.	Consumer's first name.
`middleName`	string	Optional	Max 50 chars. Same character set as `firstName`.	Consumer's middle name.
`lastName`	string	Required	1–50 chars. Letters, spaces, hyphens, and apostrophes.	Consumer's last name.
`email`	string (email)	Required	Max 254 chars. Valid addressable mailbox.	Consumer's email address.
`phone`	string	Required	10-digit NANP (`2051234567`) or E.164 (`+12051234567`). Both forms are accepted.	Consumer's primary contact number. Mobile numbers are strongly preferred.
`homePhone`	string	Optional	Same formats as phone.	A second number when the consumer has one.
`ssn`	string	Required	9 digits (`123456789`) or `NNN-NN-NNNN` (`123-45-6789`). Stored as digits only. All-zero is rejected.	Consumer's Social Security number. Required for this vertical. Visible in the page's network panel.
`dateOfBirth`	string (date)	Required	`YYYY-MM-DD`. The consumer must be at least 18 on the date of the request. Under-18 is `400`, not a decline.	Consumer's date of birth.
`gender`	string (enum)	Required	`male` `female`	Consumer's gender. There is no default.
`driversLicense`	string	Required	Max 20 chars	Driver's license number.
`driversLicenseState`	string	Required	Exactly 2 chars. Uppercase USPS state or territory code, e.g. `TX`.	State that issued the license.
`isMilitary`	boolean	Required	`true` / `false`	Whether the consumer is active-duty military.

`bestTimeToCall`	string (enum)	Recommended	`morning`
			`afternoon`
			`evening`
			`anytime`
				Preferred contact window.

Address

Field	Type	Required	Constraints / allowed values	Description
`address1`	string	Required	1–100 chars	Street address.
`address2`	string	Optional	Max 100 chars	Unit, suite, or apartment.
`city`	string	Required	1–50 chars	City.

`state`	string	Required	Exactly 2 chars. Uppercase USPS state or territory code, e.g. TX.	State.
`postalCode`	string	Required	`^[0-9]{5}$`	5-digit ZIP code. ZIP+4 is not accepted; send the first five digits only.
`residenceType`	string (enum)	Required	`own` `rent`	Whether the consumer owns or rents.
`monthsAtResidence`	integer	Required	0–1000	Months at the current address.

Loan request

Field	Type	Required	Constraints / allowed values	Description
`loanAmount`	number	Required	100–50000 USD. Cents allowed, max 2 decimal places.	Requested loan amount.

`loanPurpose`	string (enum)	Required	`other`
			`autoPurchase`
			`homeImprovement`
			`creditCardConsolidation`
			`medical`
			`debtConsolidation`
			`emergency`
			`autoRepair`
				Purpose of the loan. String tokens, not numeric codes.

`creditRating`	string (enum)	Required	`excellent`
			`good`
			`fair`
			`poor`
				Self-reported credit quality. Never a raw FICO and never `0`–`4`.

`debtAmount`	number	Optional	0–99999999 USD. Cents allowed, max 2 decimal places.	Self-reported outstanding debt.
`ownVehicle`	boolean	Required	`true` / `false`	Whether the consumer owns a vehicle.
`hasCosigner`	boolean	Optional	`true` / `false`	Whether a cosigner is available. Defaults to `false` if omitted.

Employment and income

Field	Type	Required	Constraints / allowed values	Description
`employerName`	string	Required	1–100 chars	Employer name.
`employmentPosition`	string	Required	1–50 chars	Job title.
`monthsEmployed`	integer	Required	1–1000	Months in the current role.
`employmentHireDate`	string (date)	Optional	`YYYY-MM-DD`	Hire date.
`workPhone`	string	Required	Same formats as phone.	Work phone number.
`workPhoneExtension`	string	Optional	Max 10 chars	Work phone extension.

`employerAddress`	string	Optional	Max 100 chars	Employer street address.
`employerCity`	string	Optional	Max 50 chars	Employer city.
`employerState`	string	Optional	Uppercase USPS code.	Employer state.
`employerPostalCode`	string	Optional	5-digit ZIP.	Employer postal code.

`incomeSource`	string (enum)	Required	`fullTime`
			`partTime`
			`selfEmployed`
			`benefits`
			`pension`
			`socialSecurity`
			`unemployed`
			`other`
				Source of the reported income.

`monthlyNetIncome`	number	Required	1–999999 USD per month. Cents allowed, max 2 decimal places.	Take-home monthly income. Do not send annual income.

`payFrequency`	string (enum)	Required	`weekly`
			`biweekly`
			`twiceMonthly`
			`monthly`
				How often the consumer is paid.

`payDate1`	string (date)	Required	`YYYY-MM-DD`. Today or a future date.	Next pay date.
`payDate2`	string (date)	Required	`YYYY-MM-DD`. Must be after `payDate1`.	Pay date after `payDate1`.

Banking

Field	Type	Required	Constraints / allowed values	Description
`bankName`	string	Required	1–50 chars	Name of the consumer's bank.
`bankAccount`	string	Required	4–17 digits.	Account number. Visible in the page's network panel.
`routingNumber`	string	Required	9 digits that pass the ABA check digit.	ABA routing number.
`accountType`	string (enum)	Required	`checking` `savings`	Account type.
`directDeposit`	boolean	Required	`true` / `false`	Whether income is direct-deposited.
`monthsAtBank`	integer	Required	1–1000	Months the account has been open.

Opt-ins

Optional booleans, default `false` if omitted.

Field	Type	Required	Description
`debtOptIn`	boolean	Optional	Consumer opted in to debt-relief offers.
`creditScoreOptIn`	boolean	Optional	Consumer opted in to credit-score offers.
`creditRepairOptIn`	boolean	Optional	Consumer opted in to credit-repair offers.
`creditReportOptIn`	boolean	Optional	Consumer opted in to credit-report offers.

Consent and provenance

Field	Type	Required	Constraints / allowed values	Description
`consent`	boolean	Required	Must be `true`. A lead the consumer did not consent to is rejected with `400`.	The consumer gave express written consent to be contacted about this request, including by phone and SMS.
`consentLanguage`	string	Required	1–1000 chars	The verbatim disclosure text displayed to the consumer at the point of submission. Retained as your compliance record.
`consentAt`	string (date-time)	Recommended	RFC 3339 with a timezone. Must not be later than `submittedAt`.	When the consumer accepted the disclosure.
`trustedFormCertificateUrl`	string (url)	Optional	Max 255 chars. When present: absolute `https` URL on `cert.trustedform.com`, with a non-empty path.	TrustedForm certificate for this submission. Omit if you do not have one. When present, must be a well-formed `https://cert.trustedform.com/...` URL. `consentNotVerified` may be returned in a later revision; see section 6.
`landingPageUrl`	string (url)	Required	Max 2048 chars. Absolute `https` URL. A page that collects consumer PII must be served over TLS.	The page on which the consumer submitted the form. Must be the actual form page, not your domain root.

Validation strictness

Beyond the constraints above we apply additional screening to `email`, `phone`, and `trustedFormCertificateUrl` — for example rejecting undeliverable mailboxes, disposable and role-based email domains, and non-dialable number ranges. This screening tightens over time within `v1` and is not exhaustively enumerated here. Do not build logic that depends on a malformed value being accepted today.

Example request

```
POST /v1/personal-loans/leads HTTP/1.1
Host: sandbox-api.freshwayleads.com
Origin: https://yourlandingpage.com
Authorization: Bearer fw_test_pk_1a2b3c4d5e6f7890
Content-Type: application/json; charset=utf-8
Accept: application/json
```

```
{
  "campaignName": "PL-ACME-01",
  "subId": "spring-promo-42",
  "submittedAt": "2026-09-14T14:32:07.512Z",
  "firstName": "Test",
  "lastName": "McTester",
  "email": "test@notarealemailaddress.com",
  "phone": "+12051234567",
  "ssn": "123-45-6789",
  "dateOfBirth": "1992-04-18",
  "gender": "female",
  "driversLicense": "DL123456",
  "driversLicenseState": "TX",
  "isMilitary": false,
  "bestTimeToCall": "evening",
  "address1": "123 Main St",
  "address2": "Apt 4B",
  "city": "Dallas",
  "state": "TX",
```

```
  "postalCode": "75201",
  "residenceType": "rent",
  "monthsAtResidence": 18,
  "loanAmount": 3500.50,
  "loanPurpose": "debtConsolidation",
  "creditRating": "good",
  "ownVehicle": true,
  "employerName": "Test Inc",
  "employmentPosition": "QA Analyst",
  "monthsEmployed": 24,
  "workPhone": "2145550199",
  "incomeSource": "fullTime",
  "monthlyNetIncome": 4200.50,
  "payFrequency": "biweekly",
  "payDate1": "2026-10-01",
  "payDate2": "2026-10-15",
  "bankName": "Example Bank",
  "bankAccount": "123456789",
  "routingNumber": "021000021",
  "accountType": "checking",
  "directDeposit": true,
  "monthsAtBank": 36,
  "debtOptIn": false,
  "consent": true,
  "consentLanguage": "By clicking Submit I agree to be contacted by lenders at the phone number provided, including by automated technology and SMS, about this loan request. Consent is not a condition of purchase.",
  "consentAt": "2026-09-14T14:32:05.980Z",
  "trustedFormCertificateUrl": "https://cert.trustedform.com/0f7a5c1e9b3d4a628f10c2e5b7d9a3f18c604e2b",
  "landingPageUrl": "https://yourlandingpage.com/personal-loans/apply"
}
```


6. Successful response

A processed lead returns `200 OK` with `Content-Type: application/json`.

This response is delivered into the consumer's browser and is visible in developer tools. It does not include a payout figure.

Response headers

Header	Description
`X-Request-Id`	Correlation id for this request. Echoes your value if you supplied one. Quote it in support requests.
`X-RateLimit-Limit`	Your request ceiling for the current window.
`X-RateLimit-Remaining`	Requests left in the current window.
`X-RateLimit-Reset`	Unix epoch seconds at which the window resets.

Response body

Field	Type	Always present	Description
`leadId`	string	Yes	Freshway's identifier for this lead. An opaque string, at most 32 characters. Store it and quote it in support requests. Do not parse it or infer anything from its format, which may change.
`status`	string (enum)	Yes	`accepted` — a buyer purchased the lead. `declined` — processed but not purchased. `duplicate` — reserved; not currently returned. See section 9.

`receivedAt`	string (date-time)	Yes	When we received the request. RFC 3339 UTC.
`completedAt`	string (date-time)	Yes	When we finished processing. RFC 3339 UTC.
`redirectUrl`	string (url)	Only when `status` is `accepted`	Buyer-supplied URL for the consumer. Absent, not empty, when there is nothing to redirect to. See below.
`declineReason`	string (enum)	Only when `status` is `declined`	Machine-readable reason. See table below.
`declineMessage`	string	Only when `status` is `declined`	Always `The lead was not purchased.` For your logs. Do not branch on this text.
`originalLeadId`	string	Only when `status` is `duplicate`	The `leadId` of the earlier submission.

Successful responses carry no `errors` field. Errors appear only on `4xx` and `5xx` responses, in the format described in section 7.

Using `redirectUrl`

Navigate the consumer to this URL in the page. This is the buyer's own confirmation or offer page and is the intended consumer experience.

When the field is present, always send the consumer. Buyers treat redirect rate as a quality signal; a low rate costs you coverage even though the lead already sold.

Decline reasons

`declineReason`	Meaning	Should you retry?
`noBuyerMatch`	No buyer in the network purchased the lead. This is the general case.	No.
`failedFraudChecks`	The lead did not pass our fraud screening.	No.
`consentNotVerified`	The TrustedForm certificate could not be claimed or did not match the submission.	No. Fix your certificate capture.
`belowMinimumPrice`	No buyer bid at or above the floor price for this lead.	No.

`consentNotVerified` and `belowMinimumPrice` are not currently returned. We return `noBuyerMatch` instead. Handle all four so you do not need to change anything when they start appearing.

Example — accepted

```
{
  "leadId": "01K4A7XJ2P8Q3R5S6T7V8W9XYZ",
  "status": "accepted",
  "redirectUrl": "https://buyer.example.com/offers/12345",
  "receivedAt": "2026-09-14T14:32:08.104Z",
  "completedAt": "2026-09-14T14:32:09.016Z"
}
```

Example — declined


```
{
  "leadId": "01K4A7XJ7C2D4E6F8G0H1J2K3M",
  "status": "declined",
  "declineReason": "noBuyerMatch",
  "declineMessage": "The lead was not purchased.",
  "receivedAt": "2026-09-14T14:32:08.104Z",
  "completedAt": "2026-09-14T14:32:08.755Z"
}
```


Example — duplicate


```
{
  "leadId": "01K4A7XKB5N6P7Q8R9S0T1U2V3",
  "status": "duplicate",
  "originalLeadId": "01K4A7XJ2P8Q3R5S6T7V8W9XYZ",
  "receivedAt": "2026-09-14T14:35:11.220Z",
  "completedAt": "2026-09-14T14:35:11.298Z"
}
```


---

7. Error responses

Errors return `Content-Type: application/problem+json` and follow RFC 9457 Problem Details.

Field	Type	Description
`type`	string (uri)	Stable identifier for the error class. **Branch on this**, not on `status`, `title`, or `detail`.
`title`	string	Short human-readable summary of the error class.
`status`	integer	HTTP status code, repeated for convenience.
`detail`	string	Human-readable explanation specific to this occurrence.
`instance`	string	Path of the request that failed, e.g. `/v1/personal-loans/leads`.
`requestId`	string	Correlation id. Matches the `X-Request-Id` response header.
`errors`	array	Field-level failures. Present on validation errors only.
`errors[].field`	string	Name of the offending request field.
`errors[].code`	string	Machine-readable failure code: `required`, `invalidFormat`, `tooLong`, `notAllowedValue`, `outOfRange`.
`errors[].message`	string	Human-readable description of the field failure.

Status codes

Six codes, each with distinct handling. Where two conditions call for the same action from you, they share a status code and are distinguished by `type`.

Status	type	When	Retry?
`200 OK`	—	Lead processed. Read `status` for the outcome.	n/a
`400 Bad Request`	`.../malformed-request`	Body is not valid JSON, or `Content-Type` is wrong.	No — fix the request.

`400 Bad Request`	`.../validation-failed`	Body is valid JSON but one or more fields fail validation. `errors` is populated.	No — fix the fields.
`401 Unauthorized`	`.../unauthenticated`	Missing, malformed, unknown, inactive, or revoked key, or a key that belongs to the other environment.	No — fix credentials.
`403 Forbidden`	`.../forbidden`	The request came from an unregistered origin or with no `Origin` header.	No — contact us.
`429 Too Many Requests`	`.../rate-limited`	Rate limit exceeded. Honor `Retry-After`.	Yes, after the delay.
`500 Internal Server Error`	`.../internal-error`	Unexpected failure on our side.	Yes, with backoff.

Any `4xx` means the lead was not processed and never will be. Do not resubmit the same payload unchanged. A `429` is the exception: the payload was never looked at, so resubmit it after the delay.

Example — validation failure

```
HTTP/1.1 400 Bad Request
Content-Type: application/problem+json
X-Request-Id: 9c1f4b7a-5d2e-4a83-b6c9-70e1f2a3d4b5
```

```
{
  "type": "https://docs.freshwayleads.com/errors/validation-failed",
  "title": "One or more fields failed validation.",
  "status": 400,
  "detail": "The lead was not processed. Correct the fields listed in 'errors' and submit a new request.",
  "instance": "/v1/personal-loans/leads",
  "requestId": "9c1f4b7a-5d2e-4a83-b6c9-70e1f2a3d4b5",
  "errors": [
    {
      "field": "ssn",
      "code": "invalidFormat",
      "message": "ssn must be 9 digits or NNN-NN-NNNN."
    },
    {
      "field": "loanAmount",
      "code": "outOfRange",
      "message": "loanAmount must be between 100 and 50000."
    },
    {
      "field": "consent",
      "code": "notAllowedValue",
      "message": "consent must be true. Leads without express written consent are not accepted."
    }
  ]
}
```

Example — rate limited

```
HTTP/1.1 429 Too Many Requests
Content-Type: application/problem+json
Retry-After: 24
X-RateLimit-Limit: 100
```

```
X-RateLimit-Remaining: 0
X-RateLimit-Reset: 1788192000
```


```
{
  "type": "https://docs.freshwayleads.com/errors/rate-limited",
  "title": "Rate limit exceeded.",
  "status": 429,
  "detail": "Your account is limited to 100 requests per minute. Retry after 24 seconds.",
  "instance": "/v1/personal-loans/leads",
  "requestId": "1b2c3d4e-5f60-4718-9a2b-3c4d5e6f7081"
}
```


8. Rate limiting

The default limit is **100 requests per minute per key**, measured in a fixed one-minute window.

Browser traffic is additionally limited to **5 requests per minute per consumer IP address**, to absorb a single misbehaving client without consuming your whole key allowance. A real consumer submits once, so this ceiling is not reachable by legitimate use. A consumer who trips the per-IP limit receives a `429`; your key allowance is unaffected.

Every `POST /v1/personal-loans/leads` response, successful or not, carries the current state. CORS preflight (`OPTIONS`) is not counted and does not carry these headers.

Header	Meaning
`X-RateLimit-Limit`	Your ceiling for the window.
`X-RateLimit-Remaining`	Requests left in the window.
`X-RateLimit-Reset`	Unix epoch seconds at which the window resets and `Remaining` returns to `Limit`.

Exceeding the limit returns `429` with a `Retry-After` header in seconds. Honor it; it overrides your own backoff schedule.

Contact us before a campaign launch if you expect to exceed 100 requests per minute.

9. Duplicates, timeouts, and retries

Duplicate detection

Repeated submissions are still processed and can still be sold. A consumer double-clicking submit, or a retry after a timeout where the first request succeeded, can produce a second purchased lead.

`status: "duplicate"` and `originalLeadId` are reserved and not currently returned. Handle them if they appear.

The `Idempotency-Key` header is accepted and ignored. Do not rely on it.

Timeouts and retries

Processing involves live calls to buyers, so latency is normal.

Setting	Recommendation
Connect timeout	5 seconds
Read timeout	30 seconds — do not set this lower, or you will abandon leads we are actively selling
Retry on	`429`, `500`, connection failures, read timeouts

Do not retry on	`400`, `401`, `403`
Backoff	Exponential with jitter, e.g. 1s, 2s, 4s
Max attempts	3 total

A read timeout does not mean the lead was not processed. Retry it, knowing that a successful first attempt plus a retry can sell the consumer twice.

---

10. Sandbox testing

Sandbox credentials (`fw_test_pk_`) are refused by production, and production credentials (`fw_live_pk_`) are refused by sandbox. Validation, rate limits, CORS, authentication, error shapes, and response fields are the same in both environments.

Sandbox outcomes are not deterministic. A given payload is not guaranteed to return `accepted`, `declined`, or `duplicate`. Handle all three `status` values, treat an unrecognised `status` as not accepted, and treat an unrecognised `declineReason` as a generic decline.

Do not post real consumer data to sandbox. Use synthetic SSNs, bank accounts, and contact details.

If `trustedFormCertificateUrl` is sent, it is checked for URL shape. A well-formed `https://cert.trustedform.com/...` URL passes. Omitting the field is accepted. `consentNotVerified` may be returned in a later revision.

Before requesting production credentials, confirm you parse `leadId` and `X-Request-Id`, treat `4xx` other than `429` as terminal, honor `Retry-After` on `429`, and tolerate the three `status` values and the four `declineReason` codes.

---

11. Compliance and security

- **SSN and bank details.** Personal-loan buyers require SSN and bank account data. Send them on every request. They appear in the page's network panel.
- **Transport.** TLS 1.2 or higher, HTTPS only.
- **Consent.** Only post leads where the consumer gave express written consent covering contact by phone and SMS. Send the exact disclosure text in `consentLanguage`. Falsified consent is grounds for immediate termination and chargeback of all affected leads.
- **TrustedForm.** Send a well-formed certificate URL on `cert.trustedform.com` when you have one. Omitting the field is accepted. When present, the URL is checked for shape. `consentNotVerified` may be returned in a later revision.
- **Logging.** Do not log full request bodies containing SSN, bank account, or other consumer PII in systems that are not access-controlled. Log `leadId`, `X-Request-Id`, `status`, and `declineReason` instead.
- **Credentials.** One publishable key per environment, covering your whole account rather than one per campaign: a key says who you are, and `campaignName` on each request says which of your campaigns the lead belongs to. The same publishable keys authenticate home-service posting. Use a distinct `campaignName` for each product. Publishable keys may appear in browser JavaScript but only work from the origins you register with us.
- **Rotation.** Ask us for a replacement key before retiring the one you hold. Both work at the same time, so you can cut over at your own pace and tell us to revoke the old key afterwards. There is no window where posting fails.

---

12. Versioning policy

The major version is in the URL path. Within `v1` we make only backward-compatible changes:

- New optional request fields.
- New response fields.
- New enum values on existing fields, including new `declineReason` codes.
- New `type` values on existing status codes.

- Tightened validation on fields already documented as constrained.

Build your integration to tolerate these. Ignore response fields you do not recognize, treat an unrecognized `declineReason` as a generic decline rather than a parse failure, treat an unrecognized `status` as "not accepted", and branch on `type` rather than on the numeric status code alone.

Breaking changes ship as a new path version with a written deprecation window for the previous one.