
Terms of Service

Bleedpoint Revenue Audit Service

Service Provider: Bleedpoint (a product of CloudSec Global LLC) **Document Version:** 0.9 **Effective Date:** April 26, 2026

1. Service Agreement

1.1 Acceptance of Terms

By signing up for or using Bleedpoint, you agree to these Terms of Service. These terms govern your use of Bleedpoint, including the website, web application, audit reports, and any related services we provide.

If you're agreeing on behalf of a company or other entity, you represent that you have the authority to bind that entity to these terms. In that case, "you" refers to that entity.

1.2 Service Description

Bleedpoint is an automated revenue audit service. When you connect your billing platform (currently Stripe) through a read-only OAuth integration, we analyze your subscription, payment, and customer data to identify potential revenue leakage — including failed payments, involuntary churn, legacy pricing, zombie subscriptions, and discount leakage.

We deliver findings as a downloadable PDF report and, for monitoring subscribers, ongoing audits over time.

Bleedpoint currently supports Stripe. Additional billing platforms may be supported in the future, with notice to existing customers.

1.3 What Bleedpoint Is Not

Bleedpoint provides advisory findings, not financial, legal, accounting, or tax advice. Our reports identify potential revenue recovery opportunities based on automated analysis. The actual recoverable amount depends on your customer relationships, your platform's policies, your business decisions, and other factors outside our control. Findings are estimates only and are not guarantees of recoverable revenue.

You are responsible for deciding what action, if any, to take based on our findings.

2. Subscription and Billing

2.1 Pricing

- **One-Time Audit:** \$149 USD per audit
- **Monthly Monitoring:** \$49 USD per month, available only after purchasing at least one audit

-
- **Currency:** All fees are in US Dollars (USD)
 - **Tax Responsibility:** You are responsible for any applicable taxes on your purchase, except where we are required to collect them

2.2 Payment

- **Payment Method:** Credit card or other methods supported by Stripe Checkout
- **Audit Payment:** One-time charge at the time of purchase
- **Monitoring Payment:** Recurring monthly charge on the same calendar date you subscribed
- **Failed Payments:** If a monthly payment fails, we'll attempt to retry per Stripe's default retry schedule. If recovery fails, monitoring access is suspended until payment is updated.

2.3 Free Preview

We offer a free preview that runs a subset of our audit checks against your connected Stripe account. The preview shows you a summary of potential findings without the full breakdown. There is no charge or commitment for the free preview.

The preview is provided as-is, with no guarantee that the same findings will appear in a full audit (additional checks may surface additional issues).

2.4 Refunds

We offer a money-back guarantee for one-time audits. If the audit finds less than \$745 (5x the audit fee) in identified revenue leakage, you can request a full refund of the \$149 audit fee within 30 days of report delivery.

Refunds are not automatic. To request a refund, you must email guarantee@bleedpoint.com within the 30-day window with your audit ID and a brief reason.

For complete refund details, see our Refund Policy.

Monthly monitoring fees are not refundable. You can cancel at any time per Section 3.2.

3. Service Access and Termination

3.1 Account Access

- **Authentication:** Account access is granted via email-based magic links (no passwords)
- **Account Deletion:** You can delete your account at any time from your dashboard. Deletion removes your audit reports, connected platform credentials, and personal data per the timelines described in our Privacy Policy.
- **Reactivation:** Deleted accounts cannot be reactivated. You can sign up again as a new customer.

3.2 Cancellation Policy

- **No Long-Term Commitments:** Monthly monitoring is month-to-month. There are no contracts.

-
- **Cancel Anytime:** You can cancel monthly monitoring at any time from your dashboard or through Stripe's customer portal. Cancellation takes effect at the end of your current billing period.
 - **No Proration:** We do not prorate partial months. You retain access through the end of the period you've already paid for.
 - **One-Time Audits:** One-time audit purchases cannot be canceled once the audit has run. Refunds are governed by Section 2.4 and the Refund Policy.

3.3 Service Suspension by Bleedpoint

We may suspend or terminate your access if:

- Your payment fails and is not corrected within 14 days
- You violate the Acceptable Use Policy in Section 8
- Required by law, court order, or legitimate regulatory request
- We have reasonable belief that your use poses a security risk to Bleedpoint, our customers, or third parties

When practical, we'll give you notice and a chance to fix the issue before suspending access. For security or legal-compelled actions, suspension may be immediate.

3.4 Termination by Bleedpoint for Convenience

We may terminate your account with 30 days' written notice for any reason. If we do, we'll refund any prepaid monthly monitoring fees for periods after the termination date.

4. Your Account and Data

4.1 Connected Platform Access

To run audits, you'll authorize Bleedpoint to access your billing platform (currently Stripe) using read-only OAuth tokens. Specifically:

- We request read-only access — we cannot modify, create, or delete anything in your account
- We never see or store your credit card numbers, your customers' card numbers, or any payment credentials
- You can revoke our access at any time from your dashboard or directly from your billing platform's settings
- Disconnecting from the platform deletes the OAuth token from our systems within 24 hours

4.2 Your Data Stays Yours

- **Your Data:** All data we receive from your connected billing platform — your customer records, transactions, subscriptions, and so on — remains yours. We process it on your behalf to deliver the audit; we don't claim ownership of it.

-
- **Audit Reports:** The PDF reports we generate contain your data combined with our analysis. You own the underlying data and the findings. We retain ownership of the report format, templates, and the analytical methodology that produced them.
 - **Findings:** Specific revenue leak findings about your account belong to you. The check definitions and detection logic that produced them belong to us.

4.3 Confidentiality

We treat all data we receive from your billing platform as confidential. We don't share your data with third parties, don't use it for marketing, and don't access it manually except where strictly necessary for support, debugging, or as required by law.

4.4 Privacy and Data Processing

Our handling of personal data — including data about your customers that flows through our service — is governed by our Privacy Policy and Data Processing Agreement (DPA). Both documents are part of these Terms by reference.

5. Intellectual Property

5.1 Our Property

Bleedpoint owns all rights to:

- The Bleedpoint software, web application, and underlying systems
- Audit check definitions, detection logic, and analytical methodology
- Report templates, design, and presentation format
- The Bleedpoint name, logo, branding, and marketing materials
- Documentation, including these Terms and our other policies

5.2 Your Property

You own:

- All data flowing in from your connected billing platform
- The factual findings about your specific account contained in audit reports
- Anything you produce using our reports — your remediation plans, customer outreach, and so on

5.3 Limited License to Use Bleedpoint

We grant you a non-exclusive, non-transferable, revocable license to use Bleedpoint for your business purposes during your active subscription. This license ends when your account is canceled or terminated.

5.4 Feedback

If you send us suggestions, feature requests, or feedback, we can use it freely to improve Bleedpoint without owing you anything. You're not required to send feedback, but if you do, you're not putting any conditions on how we use it.

6. Limitation of Liability

6.1 No Warranty on Recoverable Revenue

Audit findings are estimates based on automated analysis of your billing platform data. We do not warrant that:

- Any specific dollar amount of leaked revenue will be recovered
- Any finding will translate into actual recovered revenue
- Our analysis will identify every revenue leak in your account
- Recommended remediation actions will succeed

The actual recoverable amount depends on factors outside our control, including customer relationships, billing platform policies, regulatory considerations, and your business decisions.

6.2 Liability Cap

To the maximum extent permitted by law, Bleedpoint's total cumulative liability for any claim arising out of or related to these Terms or your use of the service is limited to the fees you paid us in the 12 months before the claim arose.

6.3 Excluded Damages

To the maximum extent permitted by law, Bleedpoint is not liable for:

- Indirect, consequential, special, incidental, exemplary, or punitive damages
- Lost profits, lost revenue, lost business opportunities, or lost goodwill
- Cost of substitute services
- Loss or corruption of data caused by your billing platform, your infrastructure, or third parties
- Damages caused by your action (or inaction) on our findings
- Damages caused by your billing platform's outages, errors, or policy changes

This applies regardless of the legal theory of the claim (contract, tort, strict liability, or anything else) and even if we knew or should have known the damage was possible.

6.4 Exceptions

Some jurisdictions don't allow certain liability limitations. Where the law overrides our liability cap or excluded damages list, our liability is limited to the maximum amount permitted by that law.

7. Warranties and Disclaimers

7.1 What We Warrant

- We will perform the service with reasonable care and skill
- The service will function substantially as described in our marketing and documentation
- We will use commercially reasonable efforts to maintain availability of the service

7.2 Disclaimers

EXCEPT AS EXPRESSLY STATED IN SECTION 7.1, BLEEDPOINT IS PROVIDED "AS IS" AND "AS AVAILABLE." WE DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

We don't warrant that:

- The service will be uninterrupted or error-free
- Audit findings will be 100% accurate or comprehensive
- Recommendations will fit your specific business situation
- The service will meet every regulatory or compliance requirement that applies to you

The service depends on third parties (your billing platform, our cloud infrastructure provider, payment processors). We're not liable for their outages, errors, policy changes, or terms updates.

8. Acceptable Use

8.1 Permitted Use

You agree to:

- Use Bleedpoint only on billing platform accounts you own or have authorization to audit
- Provide accurate signup and billing information
- Maintain reasonable security on your own systems and credentials
- Comply with your billing platform's terms of service and acceptable use policies
- Use the service for legitimate business purposes

8.2 Prohibited Use

You agree not to:

- Connect a billing platform account you don't own or aren't authorized to audit
- Reverse engineer, decompile, disassemble, or attempt to extract our source code or detection logic
- Share your account credentials with anyone outside your organization
- Attempt to access another customer's data or systems

-
- Use the service to compete with Bleedpoint or build a competing product
 - Use the service for unlawful purposes
 - Probe, scan, test, or attack the security of our infrastructure (other than authorized security research per Section 8.3)
 - Use the service to harass any individual or violate anyone's privacy
 - Send spam, malware, or other unwanted content through any feature of the service

8.3 Authorized Security Research

If you're a security researcher and find a vulnerability, please report it to security@bleedpoint.com. We won't pursue legal action against good-faith researchers who follow responsible disclosure practices and don't access customer data beyond what's necessary to demonstrate the issue.

9. Modifications to Terms

9.1 When We Update

We may update these Terms from time to time. When we do:

- For minor changes (typos, clarifications), we'll update the document and effective date without separate notice
- For material changes (pricing, scope of service, liability), we'll give you at least 30 days' advance notice via email or in-app notice

9.2 Your Options

If you don't agree to material changes, you can cancel your subscription before they take effect. Continued use after the effective date constitutes acceptance.

10. Governing Law and Disputes

10.1 Governing Law

These Terms are governed by the laws of the State of Nevada, United States, without regard to conflict-of-law principles.

10.2 Informal Resolution First

Before filing a formal dispute, both parties agree to attempt good-faith resolution by direct communication. Email legal@bleedpoint.com to start the conversation. We'll do the same if we have an issue with you.

10.3 Jurisdiction

Any dispute that can't be resolved informally is subject to the exclusive jurisdiction of the state and federal courts located in Clark County, Nevada. Both parties consent to personal jurisdiction in those courts.

10.4 Arbitration Option

For disputes seeking less than \$50,000 USD, either party may elect binding arbitration under the rules of the American Arbitration Association (AAA), conducted by a single arbitrator. The arbitrator's decision is final and enforceable in any court.

10.5 Class Action Waiver

To the extent permitted by law, both parties agree to resolve disputes individually, not as part of any class, collective, or representative action.

11. General Terms

11.1 Entire Agreement

These Terms, together with our Privacy Policy, Data Processing Agreement, Refund Policy, Security disclosures, and any order forms or pricing pages, are the entire agreement between you and Bleedpoint regarding the service.

11.2 No Assignment by You

You can't assign or transfer your rights under these Terms without our written consent. We may assign these Terms in connection with a merger, acquisition, sale of assets, or similar transaction, with notice to you.

11.3 Force Majeure

Neither party is liable for delays or failures caused by events beyond reasonable control, including natural disasters, war, terrorism, civil disorder, pandemic, government action, or major infrastructure outages. The affected party will notify the other promptly and use reasonable efforts to mitigate.

11.4 Severability

If any provision of these Terms is held invalid or unenforceable, the rest of the Terms remain in effect. Where possible, the invalid provision is reinterpreted to come as close as possible to its original meaning while staying enforceable.

11.5 No Waiver

Our failure to enforce any right or provision is not a waiver of that right.

11.6 Survival

Sections that by their nature should survive termination (including IP, liability limits, indemnification, dispute resolution, and confidentiality) survive termination of these Terms.

11.7 Contact

For questions about these Terms: legal@bleedpoint.com For general support: support@bleedpoint.com
For refund requests: guarantee@bleedpoint.com For security disclosures: security@bleedpoint.com

Bleedpoint is a product of **CloudSec Global LLC**, a Nevada limited liability company.

These Terms are effective as of the date you first sign up for the service or April 26, 2026, whichever is later.