FAQ

SecurityMetrics PCI Compliance

FULLSTEAM | securityMETRICS®

Table of Contents

General Questions

Monthly Fee for PCI Service

Q: *Why the monthly charge for PCI Service?*
A: Your software's payment solution, in partnership with Security Metrics, ensures your Payment Card Industry security. This involves necessary forms and vulnerability scans to safeguard card data. The fee covers these services.

Monthly Fee for PCI Non-Compliance and How to Avoid It

Q: *Why the monthly fee for PCI Non-Compliance? How to avoid it?*
A: The presence of a monthly fee for PCI Non-Compliance is connected to the requirements set forth by card brands like Visa, Mastercard, and others. When you partner with your software's payment solution, the responsibility falls on us to ensure that your payment processing adheres to these security standards. The fee emerges when either evidence of compliance is lacking or certain mandated measures aren't in place. This fee, in turn, gets passed on to you as a merchant. To prevent incurring this fee, it's crucial to furnish the necessary proof of compliance through Security Metrics. This attestation demonstrates your commitment to meeting the required PCI standards.

Understanding PCI Participation and Requirements

Q: *What is PCI and why am I being asked to participate in this questionnaire? Is participation mandatory?*
A: PCI, or Payment Card Industry, includes major card brands like Visa, Mastercard, Discover, American Express, and JCB. They've set up comprehensive security rules, the PCI Data Security Standards (PCI DSS), to protect card info in transactions. Your participation is crucial as your software's payment solution, partnered with Fullsteam, helps gather and report compliance to these brands. As a card data handler, annual validation of adherence is necessary. You can choose Security Metrics for this, but it's not obligatory. Regardless, you need to submit an Attestation of Compliance and complete a Self-Assessment Questionnaire. Quarterly scans are essential too, finding and addressing security gaps.

Buying Security Metrics' Products for Compliance

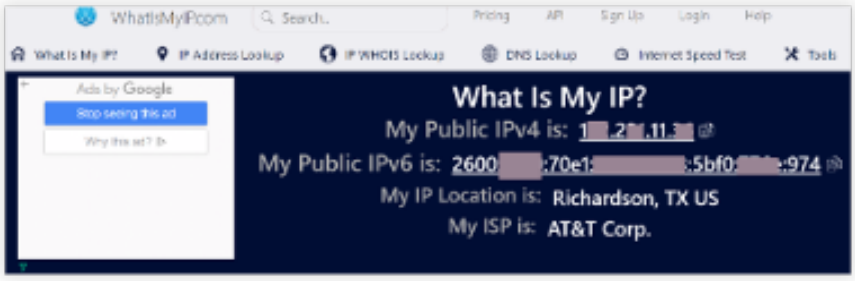
Q: *I'm being asked to buy extra products from Security Metrics to be compliant. Do I have to buy them?*
A: You might be advised to buy extra products from Security Metrics for compliance. Note that your software's payment solution, powered by Fullsteam, already covers many required PCI services: support, Self-Assessment Questionnaire documentation, and quarterly vulnerability scans. If specific security controls are lacking, Security Metrics could offer additional products to fill those gaps. Remember, these purchases aren't mandatory. The key is having necessary security controls in place. You can achieve this through Security Metrics, your own methods, or other providers.

See the table below for more products they might suggest.

Item	Cost	Optional
Security Metrics PCI Program	Included	No
Premium Service Warranty (Breach Protection)	Included	No
PCI Policies	Included	No
PANScan	Extra	Yes
MobileScan	Extra	Yes
Trainings	Extra	Yes
PII Scan	Extra	Yes
Vision	Extra	Yes
HIPAA	Extra	Yes
GDPR Defence	Extra	Yes
Shopping Cart Inspect	Extra	Yes
PCI Advisor	Extra	Yes
AntiVirus Essentials	Extra	Yes

Providing Your IP Address for Security Metrics Questionnaire

Q: *Security Metrics is requesting my IP address. What is that, and how can I locate it?*
A: Your IP address functions as your computer's distinct label on the Internet, allowing communication with your systems. Security Metrics requires this to configure scans and bolster protection against unauthorized access. To find it, open a web browser (e.g., Internet Explorer, Chrome, Firefox) and visit www.whatismyip.com. The page will display a sequence of four numbers separated by periods (like ###.###.###.###). This entire set is your IP address. A masked example is provided below.



Already Having a Security Metrics Account - Next Steps

Q: *If I already have a Security Metrics account, what's the procedure?*
A: If your Security Metrics account is established with the same credentials (Merchant Identifier, contact info), it's probable Fullsteam couldn't onboard you. Contact Fullsteam support at 801.705.5700 or support@securitymetrics.com. We'll request Security Metrics to shift you under our partnership for compliance data transfer.If your account holds different boarding details, Fullsteam likely boarded you with our info. Reach out to Fullsteam support. We'll ask Security Metrics to transfer compliance data to the new account and close the old one.

No Response from Security Metrics Support

Q: *I raised a support ticket with Security Metrics, but I haven't received any response. What should I do now?*
A: It's important to note that Security Metrics doesn't send confirmation upon ticket receipt. They strive to address all tickets within 48 hours, Monday through Friday. If this period lapses without a response, contact their support line and provide your merchant identifier to request an update. If the situation requires escalation, get in touch with Fullsteam support. We'll directly contact Security Metrics on your behalf to elevate the matter and ensure resolution.

Having Compliance with Another Vendor

Q: *I've achieved compliance through a different vendor. What's my next step?*
A: After your transition to Security Metrics, confirm the active and updated status of your Attestation of Compliance (AOC), which encompasses the Self-Assessment Questionnaire (SAQ) and scans, if applicable. Subsequently, email saq@securitymetrics.com, outlining the need to refresh your compliance data in the merchant portal. Make sure to include your merchant identifier ([portfolio company].[company name].[number]).

Opting Out of Security Metrics Compliance Program

Q: *I've chosen not to participate in the Security Metrics compliance program. Do I need to take any additional steps?*
A: Every organization handling cardholder data is responsible for maintaining relevant controls and validating them annually. Opting out removes the monthly fee and disengages you from using Security Metrics' platform for annual validation documentation. While Fullsteam, in partnership with Security Metrics, oversees compliance monitoring and reporting, you aren't obligated to use their platform for completing a Self-Assessment Questionnaire (SAQ) or ASV scan.

For the SAQ, you can access the appropriate form from the PCI SSC's document library (https://www.pcisecuritystandards.org/document_library/) and populate it as needed. If an ASV scan is required, you can choose a vendor that aligns with your business needs. Even if you've opted out, Fullsteam is still responsible for reporting each merchant's compliance status. If you've opted out, kindly send your compliance documents to saq@securitymetrics.com, including quarterly scans and the annual Attestation of Compliance (AOC), if applicable. This allows us to fulfill our reporting obligations effectively.

Contacted by Another Vendor for PCI Compliance

Q: *A different vendor contacted me regarding PCI compliance. How should I respond?*
A: Security Metrics is the sole authorized PCI vendor for our merchants. Avoid sharing sensitive details with other parties to safeguard your information.

Cardholder Environment Scoping Questions

Understanding Cardholder Data Processing Questions

Q: *While completing my responses, I'm encountering a series of questions about processing cardholder data. Could you clarify the distinctions between them?*
A: These questions are tailored to your specific cardholder data handling. Given the extensive 400+ questions in the full PCI DSS, not all are relevant to everyone. Responding to each helps remove irrelevant queries, expediting your response time. Below, you'll find the questioned area and available choices. Our guidance, indicated by a ~ in italics, accompanies each choice.
In your annual validation's initial phase, you can select up to four payment data methods: Terminal, Computer, eCommerce, Mobile Device. You can choose more than one method. Our guidance, marked with ~ in italics, will assist you.

Terminal
~This is referring to the type of payment terminal that you use, which usually sits next to your point-of-sale system machine and connected to the internet and/or your computer system or via a phone line. Select all that apply to your interaction with cardholder data

- My terminal(s) use an Internet connection.
- My Internet connection is used for multiple business purposes.
- My Internet connection is only used for the terminal(s).
- My terminal is connected to an analog phone line.
- My terminal is wireless and connects to a cell tower.
- I use an imprint machine (knuckle buster) or manually enter credit card data.
- I use my acquirer's touch-tone system to process cards.
- My terminal features validated P2PE(point-to-point encrypted) hardware

Computer
~This is referring to an actual computer or laptop. In these cases you will either have a dedicated system that ONLY processes cardholder data, a computer that runs an application, OR a computer that you would use to connect to an external web page to take payments for services and goods.
Virtual Terminal (VT) is a method you would use if you navigate to a web browser and are presented with a method to enter card data which is virtual. If you close the browser window or computer, the VT is gone. Note, this is different than an e-commerce.

I use a Virtual Terminal

- I use a single VT for processing and have no other devices using that internet connection
- *~This means that the computer which runs the VT is isolated on the network and there is nothing else on it. If there are other devices on the SAME network this choice should not be used.*

- My VT is on a shared network with multiple computers.
- *~This should be selected if you have more than JUST Point of sale devices connected to the SAME network.*

- I have a USB swipe device or card reader attached to my VT.
- *~If you have a terminal that you use for collection of cardholder data and it feeds the data into the VT, this should be selected as well as all other applicable responses.*

I use a Point-of-Sale on a computer or a separate integrated-register (touch-screen) system.

- My POS system batches (stores) cardholder data.
- My POS system tokenizes (does not store) cardholder data.
- *~In both cases provided, you will need to contact your point-of-sale vendor to obtain if the point-of-sale application you use stores cardholder data, stores a payment token, or stores either. It may be possible that none of these are applicable to your POS solution.*

eCommerce

~This payment method denotes that you employ the use of a web page for taking payments. The website is either hosted by you or a third party.

I have an eCommerce website.

- I accept payments through my own website
- My website uses Direct Post/Transparent Re-Direct.
- *~When a user connects to your webpage for payment, their browser is sent to a third party for processing of the payment functions*

- I accept payments using an I-Frame from a 3rd party source
- *~When a customer connects to your website for payment, their browser is still connected to your site, however there is an iFrames embedded into your payment page that accepts the cardholder data.*

- I accept payments through a 3rd Party Store (Amazon, Etsy, etc.)
- I accept payments through a 3rd Party Link (Paypal Button, etc.)
- I accept payments through a 3rd Party Re-Direct (Payment page on another website e.g. authorize.net, sagepay.co.uk, etc.)
- *~The preceding 3 are unlikely used for processing of payments with Fullsteam.*

Mobile Device

- I process cardholder data using a smartphone or tablet.
- ~This payment method is typically a device that plugs into your phone or tablet such as the Square solution.

- The swipe equipment I have encrypts at point-of-swipe.
- The swipe equipment I have does not encrypt at point-of-swipe.

Responding to the Security Metrics PCI provided questions.

Getting Assistance with Question Responses and Your Responsibility

Q: *While completing my responses, I'm encountering a series of questions about processing cardholder data. Could you clarify the distinctions between them?*
A: Throughout the assessment, a series of questions will be posed, allowing you to respond with Yes, No, or Not Applicable (N/A).

- Yes: Indicates compliance, confirming the control is in place.
- No: Signifies non-compliance, indicating the requirement hasn't been met.
- N/A: Denotes inapplicability to your organization. For instance, if certain controls relate to software development and you're not involved, they aren't relevant.

Your responsibility includes answering these questions accurately based on your organization's situation. If you need assistance, you can refer to the provided guidance or reach out to the designated support channels.

Here's a concise breakdown of the responsibilities for each section:

Policy

- Merchants: Develop and maintain policies to address all relevant PCI DSS requirements.

Stored Data

- Merchants: Provide data based on methods and processes.
- Your software's payment solution: Provide data storage details to the merchant.

Transmission

- Merchants: Answer questions about end user messaging protocols.
- Fullsteam: Manages encryption of cardholder data during processing.

Data Access

- Merchants: Responsible for access to data, unless POS provider handles usernames and passwords.

Physical Access

- Merchants: Control physical access to cardholder data environment.

Anti-virus

- Merchants: Responsible for POS and computer devices, unless POS provider manages.

Stored Data

- Merchants: Responsible for all stored data.
- Your software's payment solution: Can provide data about POS and cardholder data storage.

Firewall

- Merchants: Set up and configure firewalls, unless POS provider handles.

Unique ID

- Merchants: Responsible for usernames and account setup.

Vendor Defaults

- POS Provider: Direct who changes vendor defaults.

Development

- POS Provider: Advise on POS system patch management.
- Merchants: Responsible for secure software development if applicable.

Testing

- Merchants: Responsible for security testing.

Logging

- POS Provider: Can provide logging attribute details.
- Merchants: Responsible for logging, unless POS provider handles.

These responsibilities guide compliance with PCI DSS requirements.

Third Party Service Providers

Guidance on Answering Questions About Third Parties

Q: *I'm required to provide details about third parties I use. Can you guide me on how to answer these questions?*
A: Toward the end of your assessment, you'll encounter questions about third parties involved in collecting payment card data. Our guidance is indicated by a ~ in italic font to assist you in responding effectively.

Guidance for Providing Third-Party Information

Payment Gateway
~Your response should be Fullsteam.

Web Host
~If you utilize a third party to host your web-based payment application, list their name(s) here.

Shopping Cart
~If a third party provides your shopping cart services for payment and customer info collection, list their name(s) here.

Co-Location
~If you use an off-site third-party location for hosting payment processing and website, list their name(s) here.

Point-of-Sale Terminal
~List all types of POS terminals you use here.

Payment Application
~Specify your point-of-sale software's name here.

These details help ensure accurate representation of third-party involvement in your payment processes.