FIRST UNDERWRITERS INSURANCE BROKERS
Independent Insurance Brokers & Risk Managers

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

SAQ SELECTION GUIDE

Which PCI Self-Assessment Questionnaire Is Right for You?

A Plain-English Guide for Small Business Owners

Retail • Restaurants • E-Commerce • Professional Services • Healthcare

If your business accepts credit cards, debit cards, or any electronic payment, you are required to validate PCI DSS compliance annually. For most small and mid-sized businesses, this means completing a Self-Assessment Questionnaire (SAQ) — a standardized form that documents how you protect cardholder data.

But there are multiple SAQ types, and choosing the wrong one can mean answering hundreds of unnecessary questions — or worse, failing to meet the requirements that actually apply to your business. This guide will help you identify the right SAQ for your payment environment in plain English.

What Is an SAQ?

The Self-Assessment Questionnaire is a validation tool created by the PCI Security Standards Council. It allows businesses to self-certify their compliance with PCI DSS without hiring an external auditor. There are 9 SAQ types (A, A-EP, B, B-IP, C-VT, C, D-Merchant, D-SP, P2PE), each designed for a specific payment processing method. The simpler your payment setup, the simpler your SAQ.

Your acquiring bank or payment processor determines your compliance validation level based on your annual transaction volume. Most small businesses (under 6 million annual transactions) validate via SAQ rather than a formal on-site audit.

PCI REQUIREMENT: Not sure if you need to complete an SAQ? If you accept credit or debit cards in any form — in-store, online, over the phone, or via invoice — the answer is yes. Even if a third-party processor handles everything, you still have compliance obligations. Your acquiring bank can confirm your exact requirements.

© 2026 First Underwriters Insurance Brokers | Independent & Unbiased Guidance

This guide is for educational purposes only. Consult your payment processor or a Qualified Security Assessor (QSA) for formal SAQ determination.

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

SAQ TYPES EXPLAINED

SAQ A — Card-Not-Present — Fully Outsourced

Who It's For: E-commerce, mail-order, or phone-order businesses that have completely outsourced all payment processing to a PCI-compliant third-party provider.

How It Works: You never see, touch, process, or store cardholder data. Your website redirects customers to a hosted payment page (Stripe Checkout, PayPal, Shopify Payments) or you take orders by phone and enter them into the processor's portal.

Complexity: Lowest | **Questions: 22**

SAQ A is the simplest and most common SAQ for small businesses. If your customers enter their card information on someone else's system — not yours — this is likely your SAQ type.

Common Examples of SAQ A Businesses:

- Online store using Shopify, BigCommerce, or WooCommerce with hosted checkout
- Businesses using Stripe Checkout, PayPal, or Square Online (redirect model)
- Mail-order or phone-order businesses entering cards into processor's web portal
- Subscription services using a third-party billing platform (Recurly, Chargebee)
- Invoicing through QuickBooks Online, FreshBooks, or similar with integrated payments

BROKER INSIGHT: If you're currently processing payments on your own website and want to simplify compliance, switching to a hosted payment page (where the customer leaves your site to enter card details) can drop you from SAQ D (326 questions) to SAQ A (22 questions). This is often the single most impactful compliance decision.

This guide is for educational purposes only. Consult your payment processor or a Qualified Security Assessor (QSA) for formal SAQ determination.

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

SAQ A-EP — E-Commerce — Partially Outsourced

Who It's For: E-commerce businesses whose website controls the checkout experience but uses JavaScript or a direct API to send card data to a third-party processor — the card data passes through or is handled by your web server.

How It Works: Your website hosts the payment form, but card data is submitted directly from the customer's browser to the payment processor via embedded JavaScript (Stripe.js, Braintree Drop-in). Your server never receives the full card number.

Complexity: Moderate | **Questions: 191**

SAQ A-EP applies when your website influences the security of the transaction even though card data goes directly from the browser to the processor. A compromised website could inject malicious code to intercept card data.

Common Examples of SAQ A-EP Businesses:

- Online store using Stripe Elements or Braintree hosted fields on your own checkout page
- Custom-built e-commerce site with embedded payment iFrame or JavaScript tokenization
- SaaS platforms with in-app payment forms using direct-post or JavaScript APIs

IMPORTANT: The key difference between SAQ A and SAQ A-EP is whether your website controls the payment page. If the customer stays on YOUR site to enter card details (even if the data goes directly to Stripe), you're SAQ A-EP. If they're redirected to Stripe's hosted page, you're SAQ A. This distinction matters enormously.

Notes:

This guide is for educational purposes only. Consult your payment processor or a Qualified Security Assessor (QSA) for formal SAQ determination.

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

SAQ B — Imprint or Dial-Out Terminal Only

Who It's For: Brick-and-mortar businesses using standalone, dial-out payment terminals that connect directly to the processor via phone line — with no internet connection.

How It Works: Your terminal dials the processor over an analog phone line for each transaction. The terminal is not connected to your network or the internet in any way. This includes old-style manual card imprint machines.

Complexity: Low | **Questions: 41**

SAQ B-IP — Standalone IP-Connected Terminal

Who It's For: Brick-and-mortar businesses using standalone, PTS-approved payment terminals that connect to the processor over the internet (IP) — but are not connected to any other systems on your network.

How It Works: Your card terminal connects to the internet to process transactions, but it is isolated — not connected to your POS, computer, or any other system. The terminal is a standalone device on its own network segment.

Complexity: Low-Moderate | **Questions: 82**

NOTE: Most modern card terminals (Verifone, Ingenico, PAX) connect via IP, making SAQ B-IP the more common of these two types. The critical requirement is that the terminal must be standalone and network-segmented — not connected to your computer, POS system, or general business network.

© 2026 First Underwriters Insurance Brokers | Independent & Unbiased Guidance

This guide is for educational purposes only. Consult your payment processor or a Qualified Security Assessor (QSA) for formal SAQ determination.

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

SAQ C-VT — Virtual Terminal Only (Key-Entered)

Who It's For: Businesses that process card-not-present transactions by manually entering card numbers into a web-based virtual terminal provided by their payment processor.

How It Works: You take card numbers over the phone or from paper forms and type them into your processor's virtual terminal (a web page). The computer used for this purpose has no other payment applications or card data storage.

Complexity: Low-Moderate | **Questions: 79**

SAQ C — Payment Application Connected to the Internet

Who It's For: Brick-and-mortar businesses whose POS system or payment application is connected to the internet, but cardholder data is not stored electronically after authorization.

How It Works: Your POS system processes card payments over the internet — this is the typical setup for restaurants, retail stores, and service businesses using systems like Clover, Toast, Square Register, or Lightspeed connected to your network.

Complexity: Moderate | **Questions: 160**

BROKER INSIGHT: SAQ C is the most common SAQ type for brick-and-mortar small businesses with a networked POS system. If your card reader connects to a computer or tablet that also connects to the internet, you are almost certainly SAQ C — not SAQ B or B-IP.

Notes:

This guide is for educational purposes only. Consult your payment processor or a Qualified Security Assessor (QSA) for formal SAQ determination.

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

SAQ D — All Other Merchants

Who It's For: Any merchant that does not qualify for any of the above SAQ types. This includes businesses that store cardholder data electronically, process cards on their own servers, or have complex multi-channel payment environments.

How It Works: You store, process, or transmit cardholder data in ways not covered by simpler SAQ types. This is the most comprehensive and rigorous self-assessment, covering all PCI DSS requirements in full detail.

Complexity: Highest | **Questions: 326**

SAQ D is the "catch-all" — if you don't clearly fit another SAQ type, you default to SAQ D. Many businesses end up here unnecessarily because they haven't optimized their payment architecture.

SAQ P2PE — Point-to-Point Encryption (Validated)

Who It's For: Merchants using a PCI-validated Point-to-Point Encryption (P2PE) solution where card data is encrypted at the terminal and cannot be decrypted in your environment.

How It Works: Your P2PE-validated terminal encrypts card data immediately upon swipe, dip, or tap. The encrypted data passes through your network but cannot be read — decryption only happens at the processor. You must use a PCI-listed P2PE solution.

Complexity: Low | **Questions: 33**

RISK FACTOR: P2PE is a powerful compliance simplifier. By encrypting card data at the point of interaction, it removes your network from PCI scope almost entirely. If your processor offers a validated P2PE solution, it may be worth the investment to dramatically reduce your compliance burden and cyber risk exposure.

© 2026 First Underwriters Insurance Brokers | Independent & Unbiased Guidance

This guide is for educational purposes only. Consult your payment processor or a Qualified Security Assessor (QSA) for formal SAQ determination.

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

FIND YOUR SAQ: DECISION GUIDE

Answer each question below based on how your business actually processes card payments. Follow the path to determine your most likely SAQ type.

Q1: Do you accept card payments in-person (card present)?

YES → Go to Q3 (in-person path)	**NO →** Go to Q2 (card-not-present path)

Q2: Does the customer enter card details on YOUR website (not a redirect)?

YES → SAQ A-EP (191 questions)	**NO →** SAQ A (22 questions)

Q3: Is your card terminal standalone (not connected to POS, computer, or network)?

YES → SAQ B or B-IP (41-82 questions)	**NO →** Go to Q4

Q4: Does your POS system or payment app connect to the internet?

YES → SAQ C (160 questions)	**NO →** SAQ B (41 questions)

Q5: Do you use a PCI-validated P2PE encryption solution?

YES → SAQ P2PE (33 questions)	**NO →** SAQ C or SAQ D (160-326 questions)

Q6: Do you store cardholder data electronically after authorization?

YES → SAQ D (326 questions)	**NO →** Review Q1-Q5 for best fit

NOTE: This is a simplified decision guide. Many businesses have mixed payment environments (e.g., in-store + online). If you accept payments through multiple channels, you may need to complete the SAQ type that covers your most complex channel — or separate SAQs for each. Consult your payment processor for guidance.

This guide is for educational purposes only. Consult your payment processor or a Qualified Security Assessor (QSA) for formal SAQ determination.

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

SAQ COMPARISON AT A GLANCE

SAQ	Payment Method	Questions	Complexity	Best For
A	Fully outsourced (redirect)	**22**	Lowest	E-com w/ hosted checkout
A-EP	E-com w/ JS/API integration	**191**	Moderate	E-com w/ embedded forms
B	Dial-out terminal (phone line)	**41**	Low	Imprint / analog terminal
B-IP	Standalone IP terminal	**82**	Low-Mod	IP terminal, no POS
C-VT	Virtual terminal (key-entered)	**79**	Low-Mod	Phone orders, manual entry
C	POS connected to internet	**160**	Moderate	Retail, restaurant POS
D	All other merchants	**326**	Highest	Complex / storing card data
P2PE	Validated P2PE terminal	**33**	Low	Encrypted at terminal

The number of questions directly correlates with your compliance burden. Every question requires a documented answer — either "Yes" (with evidence), "No" (with a remediation plan), or "N/A" (with justification). Fewer questions means less effort, less cost, and faster compliance.

BROKER INSIGHT: Your SAQ type directly impacts your cyber insurance. Carriers assess your PCI compliance posture during underwriting. Businesses on SAQ A or P2PE present lower risk profiles and may qualify for better terms. Businesses on SAQ D face more scrutiny and may encounter coverage restrictions or higher premiums.

IMPORTANT: If you are currently SAQ D and processing fewer than 6 million transactions annually, there is almost certainly a way to simplify your payment environment to qualify for a less complex SAQ. This should be a priority conversation with your payment processor and IT team.

© 2026 First Underwriters Insurance Brokers | Independent & Unbiased Guidance

This guide is for educational purposes only. Consult your payment processor or a Qualified Security Assessor (QSA) for formal SAQ determination.

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

COMMON SAQ MISTAKES TO AVOID

✕ Choosing SAQ A when you host your own payment form

If customers enter card details on YOUR website — even if Stripe.js sends them directly to Stripe — you are SAQ A-EP, not SAQ A.

✕ Assuming your POS vendor handles compliance for you

Your POS vendor's PCI compliance covers THEIR systems, not yours. You are still responsible for your own network, access controls, and security practices.

✕ Ignoring e-commerce because your primary business is in-store

If you sell online AND in-store, you need to address both channels. Your SAQ is determined by your most complex payment channel.

✕ Completing the wrong SAQ and submitting it to your acquiring bank

An incorrect SAQ can result in a false sense of compliance and leave you liable in the event of a breach. Worse, your acquiring bank may reject it.

✕ Treating PCI compliance as a one-time event

PCI compliance requires ongoing effort: quarterly scans, annual SAQ resubmission, continuous security monitoring, and employee training.

NEXT STEPS

1. Identify how your business accepts card payments (in-store, online, phone, all three)
2. Use the decision guide on Page 7 to determine your likely SAQ type
3. Confirm your SAQ type with your payment processor or acquiring bank
4. Complete the appropriate SAQ and submit by your annual deadline
5. Schedule quarterly ASV vulnerability scans (required for most SAQ types)
6. Share your PCI compliance status with your insurance broker at renewal

© 2026 First Underwriters Insurance Brokers | Independent & Unbiased Guidance

This guide is for educational purposes only. Consult your payment processor or a Qualified Security Assessor (QSA) for formal SAQ determination.

(425) 242-5357 | www.firstunderwriters.com
4055 Lake Washington Blvd NE, Suite 100
Kirkland, WA 98033

> **BROKER INSIGHT:** PCI compliance and cyber insurance are two sides of the same coin. A documented PCI compliance program — with the correct SAQ, quarterly scans, and employee training — demonstrates to carriers that you take data security seriously. This directly impacts your eligibility, coverage breadth, and premium.

Notes:

REVIEW SIGN-OFF

By signing below, the business owner confirms they have reviewed this guide and understand their obligation to determine and complete the correct SAQ for their payment environment.

Business Owner Signature: _____ **Date:** _____

SAQ Type Determined: _____ **Processor:** _____

Need Help with PCI Compliance?

As independent brokers, we help you understand how PCI compliance impacts your cyber insurance, ensure your policy covers PCI fines and penalties, and connect you with resources to simplify your compliance.

Call (425) 242-5357 | Visit www.firstunderwriters.com

© 2026 First Underwriters Insurance Brokers | Independent & Unbiased Guidance

This guide is for educational purposes only. Consult your payment processor or a Qualified Security Assessor (QSA) for formal SAQ determination.