



ADVANCED SECURITY PACKAGE (ASP)



STEP 1:

During the WRF boarding process, you will receive an email from Trustwave® inviting you to the TrustKeeper web portal to complete the compliance validation process. Click on the link in the email to take you to the portal, then click on the big "Get Started" button.

STEP 2:

Follow directions in the TrustKeeper web portal to be placed in the proper version of the Self-Assessment Questionnaire (SAQ), complete the SAQ, and set up vulnerability scans if appropriate (the portal will help you with this).

STEP 3:

Once you have successfully completed the SAQ and you have successfully passed your first scan (if applicable), you will have validated PCI-DSS compliance. Wind River Financial will have visibility to your compliance status.

Depending on the complexity of your credit card processing solution, the SAQ may become very technical. If so, we recommend that technical resources be utilized. The Trustwave® Support Center is available 24 hrs/day at (800) 441-1762 to help answer questions. In addition, Wind River Financial has resources available at (800) 704-7253. Note that some businesses may need to contact an IT vendor to reach PCI-DSS compliance.

INDUSTRY STATISTICS INVOLVING COMPUTER BREACHES AND COMPROMISED DATA

20%

of merchants fail after a credit card data compromise

87%

of breaches were avoidable with simple/intermediate measures

96%

of breaches are to small merchants

FREQUENTLY ASKED QUESTIONS

Q: Is participation mandatory?

A: Yes. The payment brands require that all entities that accept payment cards be PCI compliant.

Q: What if I am already enrolled with a different security vendor?

A: If you choose to stay with a different security vendor, you will be required to provide proof of compliance through the Trustwave portal in order to avoid monthly non-compliance fees.

Q: If I only use a terminal, am I still required to be compliant? What if I don't store credit card data?

A: Yes. Terminal only merchants will have a lesser validation type, but must still complete it. Data can be intercepted while being transmitted, which means that you still must validate compliance, even if you do not store credit card data.

Q: If I am already compliant, should I still have Breach Protection?

A: Being compliant is not a guarantee against a breach. It only means that you are practicing the minimum information security best practices required by the industry. Breaches normally result in significant costs which Breach Protection is designed to help cover. At Wind River Financial, we are proud to offer \$100,000 coverage per individually-affected merchant ID number.

