Scaleit USA Supplemental FAQ

Scaleit USA and Fullsteam have provided the following supplemental instruction to help merchants complete their PCI compliance program with Security Metrics. Neither Scaleit USA nor Fullsteam can attest to compliance for merchants. However, we have provided the following guidance based on the Scaleit USA payment software alone. We caution that if the merchant uses any other payment solution, handles data separately, uses a terminal or e-commerce, then their answers may differ.

I. Scoping Questions:

- Assuming the merchant is only using Scaleit USA as their payment solution, that they do not use a terminal or swiper (i.e. uDynamo, iDynamo) and the merchant does not process or store transactions itself, Scaleit USA accepts payments using an iFrame from Fullsteam.

Figure 1: Scoping Questions for Scaleit USA

- Scaleit USA does not store cardholder data, so if the merchant does not store cardholder data or use another payment solution, they can answer, "No".

Figure 2: Storing Cardholder Data

- Neither Scaleit USA or Fullsteam are in the drop down list for Security Metrics. Therefore merchants using Scaleit USA can type in "Scaleit USA" and select "Add" on the right hand side. The warning in orange will appear, but it will not prevent the merchant from becoming compliant.
- Nothing is required in the Co-Location section.

Figure 3: Web Host & Co-Location

II.　Expected SAQ

- If the merchant only uses ScaleitPay, does not store data, process online payments themselves, and only uses the iFrame, we expect the merchant to most likely be routed to SAQ A with no scan required.
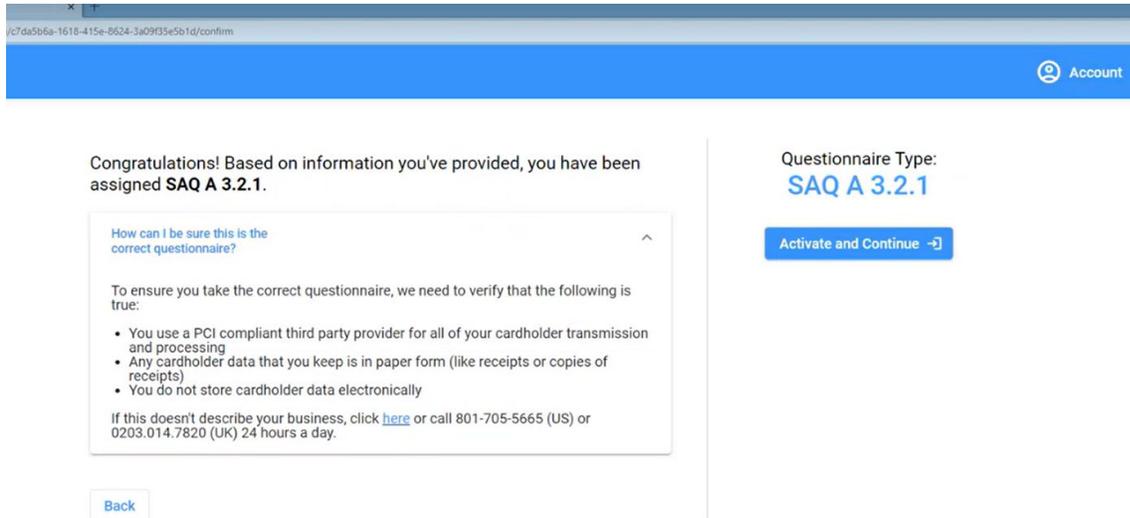
Figure 4: SAQ A for Scaleit USA

III.　Compliance Complete

- If the merchant uses only Scaleit USA as their payment solution, no swipers or online payments, and no terminals, the merchant was most likely routed to SAQ A and is not required to complete a scan. Therefore, once completing the SAQ A the merchant should see "Passing" compliance on their dashboard.
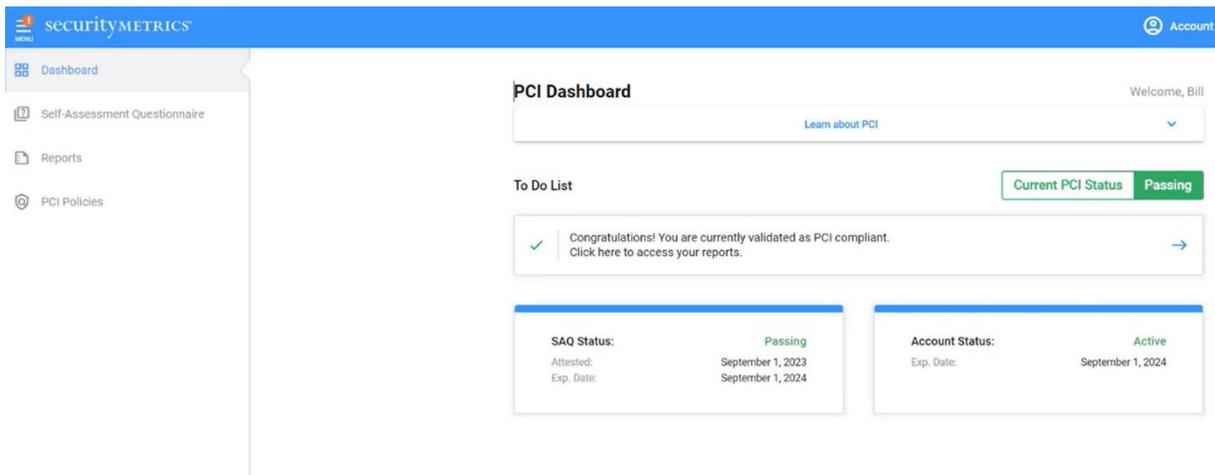
Figure 5: Compliance Complete