PCI DSS 3.0 - FAQs

Please note that the below information is for guidance only and is based on our current understanding of the PCI DSS regulations and recent changes. The information is subject to change at any time and ultimately it is you (the merchant) that is responsible for specifying and maintaining the correct PCI DSS policy and documentation for your own circumstances and organisation. We recommend that if you are unsure' you consult a PCI DSS Qualified Security Assessor (QSA).

1. Who is affected by the new Payment Card Industry Data Security Standard (PCI DSS) 3.0 changes?
They will affect all merchants that are regulated by PCI DSS. If you process, store, or transmit payment information you are affected by the changes.

2. When does PCI DSS 3.0 come into effect?
The PCI DSS 3.0 regulations apply from January 1st 2014, however PCI DSS 2.0 compliant merchants have until January 1st 2015 to transition to the new standard.

3. What will happen if I am not compliant with PCI 3.0 in January 1st, 2015?
If you haven't complied with PCI 3.0 by January 1st 2015, you will technically be in violation of PCI DSS. If you are compromised, you may face heavy fines.

4. How does PCI 3.0 affect e-commerce merchants?
Originally e-commerce merchants were validated by the completion of PCI SAQ (Self-Assessment Questionnaire) A, but many merchants will now have to move to the new PCI SAQ A-EP which includes further requirements.

5. Which SAQ will I need to complete?

SAQ A: You would still complete this if your website is entirely hosted and managed by a PCI-compliant third-party payment processor (all payment processing functions fully outsourced) or if your website provides an iframe or URL that entirely redirects a customer to a PCI-compliant third-party payment processor, where no elements of the page originate from the your website.

SAQ A-EP: You would need to complete this if your website creates a payment form and posts payment data to PCI-compliant third-party payment processor or your website provides an iframe or a URL that redirects a customer to a PCI-compliant third-party payment processor but some elements of the payment page originate from your website. These elements could be JavaScript, CSS, or anything else that supports how the payment page is created.

6. Why have the regulations changed?
The SAQ A-EP was developed to address potential instances where an attacker takes over a merchant site and maliciously redirects the unsuspecting customer to a false payment page. The controls within the new SAQ A-EP ensure that a merchant's website (one which actually controls or manages the payment transaction) is secured and cannot impact the overall security of the payment process.

7. What are the key differences between SAQ A and SAQ A-EP?
For SAQ A-EP:

- A firewall has to be in place for each internet connection, the configuration of which has to be regularly reviewed (1.x).
- Configuration standards that are consistent with industry accepted system hardening practices have to be developed for all system components (2.2).
- Processes to identify security vulnerabilities need to be in place (6.1) and all system components and software need to be protected from all known vulnerabilities by installing appropriate vendor supplied security patches (6.2).
- Documented control procedures for implementing security patches and software modifications have to be in place (6.4.x/6.5.x).
- System audit trails (logs) need to be in place for all in-scope system components and actions (10.2).
- An external PCI ASV (Approved Scanning Vendor) scan has to be completed quarterly (11.2.2).
- An internal vulnerability scan must also be run quarterly and also after any significant changes in the network environment (11.2.3).
- An external penetration test must be completed at least annually (11.3).

8. Who should I contact for further information or advice regarding these changes?
You should contact your acquirer (who currently direct you to complete your annual PCI SAQ), or a PCI-DSS certified QSA (Qualified Security Assessor).

9. Useful links
Self-Assessment Questionnaire A-EP and Attestation of Compliance:
https://www.pcisecuritystandards.org/documents/SAQ_A-EP_v3.pdf

Understanding the SAQs for PCI DSS v3.0:
https://www.pcisecuritystandards.org/documents/Understanding_SAQs_PCI_DSS_v3.pdf

Processing e-commerce payments, a guide to security and PCI DSS requirements:
http://www.visaeurope.com/media/images/processing%20e-commerce%20payments%20guide-73-17337.pdf

Summary of Changes from PCI DSS Version 2.0 to 3.0:
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_Summary_of_Changes.pdf

Self-Assessment Questionnaire A-EP and Attestation of Compliance:
https://www.pcisecuritystandards.org/documents/SAQ_A-EP_v3.pdf