QSA & PA-QSA Revocation
Frequently Asked Questions

Purpose of document: The Council recently revoked the status of a PA-QSA and QSA. The purpose of this document is to answer questions about the impact that action may have on customers of the QSA and PA-QSA in question.

Q What is the Council announcing?

A *Effective immediately, the Council is announcing the revocation of CSO's status as a Council Qualified Security Assessor (QSA) and Payment-Application Qualified Security Assessor (PA QSA).*

Q When is this revocation effective?

A *This revocation is effective immediately, August 03, 2011.*

Q Why is this revocation happening?

A *CSO's status as QSA and PA-QSA is being revoked due to the company's failure to meet the high standards demanded of QSAs and PA-QSAs.*

CSO's status as a QSA and PA-QSA was revoked only after careful review of reports and evidence submitted as part of the quality assurance program, and only after determining that no intermediate steps would accomplish the twin purposes of maintaining the high standards of the Council's QSA and PA-QSA lists and maintaining the integrity of its certification and validation programs. It accompanies CSO's inability to demonstrate sufficient improvement through a prior remediation process.

With this revocation, CSO has been removed from the Council's lists of approved service providers and is no longer eligible to provide assessment services.

Q What was CSO doing wrong and how is the Council ensuring other QSAs and PA-QSAs are not doing the same thing?

A *The Council does not typically share details of its contractual relationships or performance regarding QSAs and PA-QSAs. However as this revocation demonstrates, PCI SSC is committed to maintaining a pool of highly qualified assessment providers globally.*

As part of the assessor validation process, PA-QSAs and QSAs agree to adhere to and participate in a robust quality assurance program, which is designed to help all assessment providers uphold a strong profile by following a process that ensures their consistency, credibility, competency and professional ethics. The quality assurance (QA) program is based on eight guiding principles:

1. *Uphold the best interest of the assessor client;*
2. *Adhere to validation requirements among the assessor company;*
3. *Adhere to validation requirements among the assessor employee;*
4. *Maintain consistent assessor procedures and reporting;*
5. *Interpret the PCI standards appropriately as applicable to the client's systems & environment;*
6. *Remain current with industry trends and PCI SSC updates in the assessor community;*

7. *Report all opinions as factual, documented and defendable, and;*
8. *Maintain a positive relationship between the assessor and PCI SSC.*

Q Why am I learning about this action now?

A *The Council is taking the earliest possible opportunity to notify you of the revocation of CSO as a QSA and PA-QSA. The decision for revocation signifies that a company has failed to meet the high standards of the QSA or PA-QSA program, or to demonstrate sufficient improvement through a remediation process. As part of the remediation requirements, companies agree to notify their customers that they have gone into remediation. This remediation status is also noted publically on the validated payment applications listing on the PCI SSC website.*

Q How can businesses using products validated by CSO guard against data breach?

A *Through the PCI Standards, assessment service providers and listings of validated products, the Council aims to provide any organization with resources to assist them in protecting cardholder data. Concerns regarding specific products should be addressed directly with product vendors.*

Q How can consumers minimize the risk to their payment data? Is there something PCI SSC needs consumers to do as a result of this situation?

A *No additional action is required of consumers as a result of the Council's revocation of CSO's QSA and PA-QSA status. This is an operational matter between the Council and a business partner. The Council always advises consumers to be vigilant about their cardholder data, reviewing card statements regularly and using their card in trusted environments. This advice stands today as it does every day.*

Q What does CSO's revocation mean for other assessors?

A *The Council works diligently to maintain the integrity of its validated payment application listing for the benefit of assessors and their customers. The revocation of CSO's QSA and PA-QSA status has no direct impact on another assessor's status as QSA or PA-QSA, on the current list of validated payment applications or on the programs themselves.*

Q As a QSA, if my customer is using a payment application that CSO has previously reviewed, is it still acceptable for them to do so?

A *QSA's should continue to use the PA-DSS listing as their source for the latest information on validated payment applications.*

Q As a QSA, how will this impact my customers' PCI DSS assessment?

A *The Council is focused on maintaining the integrity of its validated payment application listing. There is no reason for this change in QSA and PA-QSA status to impact an individual organization's assessment. Use of a validated payment application continues to be an important step in support of PCI compliance efforts.*

Q As a PA-QSA, how can I help CSO's customers?

A *There may be former CSO customers that are seeking new PA-QSA service providers. The Council is referring them to the latest PA-QSA listing. Speed, accuracy and quality of service may be top of mind for them as they select a new provider.*

Q As an ISO, what does CSO's revocation mean for me?

A *When choosing a payment application or working with customers to select one, ISOs should continue to reference the Council's listing of validated payment applications. Individual company revocations have no direct impact on ISO business.*

Q As a merchant, how do I know the payment application I'm using is secure?

A *Revoking the status of a QSA or PA-QSA is a very serious matter. This action was taken, however, to ensure that the Council can maintain the integrity of the PA-DSS validated payment applications list that you may use to select a payment application that helps your PCI DSS compliance efforts.*

The Council's listing of validated payment applications is the definitive source for the latest information on which payment applications have been assessed against the PA-DSS standard. Of course you may also direct any questions about your payment application to the vendor or sales contact you worked with to procure it, but the Council's listing should be used as the source for verifying any claims you hear during the purchasing process.

Q If I'm using an application that was validated by CSO, what should I do?

A *The Council is reaching out to vendors that have products previously assessed by CSO to let them know of the revocation of CSO's status, and you are free to contact the vendor of any validated payment application you are using to find out if there is any additional information. In addition, the PA-DSS program provides for the delisting of applications known by PCI SSC to be insecure or otherwise not compliant with the PA-DSS, and any such applications will be removed from the list of validated payment applications on the PCI SSC website if the Council concludes that is appropriate.*

Q As a Council Participating Organization (PO), what does CSO's revocation mean for me?

A *Feedback from our Participating Organizations was a significant driver for establishing a quality assurance program for assessors. Revocation is a serious matter but necessary to uphold the quality of services that POs and other organizations require. There is no action necessary by POs as a result of this revocation.*

Q What steps is PCI SSC taking to communicate with CSO customers?

A *The Council is communicating directly to current and former CSO payment application vendor customers to notify them of the revocation. We are informing current customers of the need to find alternate PA-QSA services to complete their RoV and listed vendors are being alerted to our concerns regarding CSO in the context of the QSA and PA-QSA programs. The Council has no direct line of contact with PCI DSS assessment customers of CSO, and hence is providing this information to the market through our website.*

Q How does this move by the Council impact the integrity of the PA-DSS listing?

A *The revocation of CSO points to the commitment of PCI SSC to uphold the highest quality and consistency of assessment services to ensure that the PA-DSS validated payment application listings are as robust as possible*. The Council's listing remains the go-to source for information on PA-DSS compliant applications.

Q I'm a customer of CSO with a pending RoV. When will my product be validated?

A *With this revocation, CSO is no longer eligible to provide you with assessment services, and PCI SSC is unable to review the RoV prepared by CSO. The Council advises you to seek the services of an alternative PA-QSA from the listing on our website. We understand this may cause inconvenience to you, but it is imperative for all participants in the payment ecosystem that PCI SSC uphold the integrity of the PA-DSS validated payment applications listing. Acknowledging the delays you may have faced in completing the process of validation of your product, the Council will make every effort to ensure your next RoV is carefully reviewed in a timely fashion.*

Q I'm a customer of CSO currently undergoing a PCI DSS assessment (with a pending Report on Compliance).

A *Due to the revocation of its QSA status, CSO can no longer provide assessment services.The Council advises you to seek the services of an alternative QSA from the listing on our Website. We understand this may cause inconvenience to you, but it is imperative for all participants in the payment ecosystem that the PCI SSC uphold the integrity of our assessor programs and its listings.*

Q CSO is my PA-QSA and my RoV is in the quality assurance queue at the Council. Should I look for another PA-QSA?

A *Yes. Due to the revocation of its PA-QSA status, CSO can no longer provide assessment services and PCI SSC is unable to review the RoV prepared by CSO. The Council advises you to seek the services of an alternative PA-QSA from the listing on our website. We understand this may cause inconvenience to you, but it is imperative for all participants in the payment ecosystem that the PCI SSC uphold the integrity of the PA-DSS validated payment applications listing. Acknowledging the delays you may have faced in completing the process of validation of your product, the Council will make every effort to ensure your next RoV is carefully reviewed in a timely fashion.*

Q If I'm a customer of CSO with a payment application listed on the Council's website, am I required to have my product re-validated?

A *The quality assurance review that led to the revocation of CSOs PA-QSA status pertains to RoVs and work papers of applications that have not yet been approved or listed by PCI SSC. Although the revocation does not require a listed application to go through immediate revalidation, like all payment applications, it must be revalidated on a regular basis. Accordingly, if you have made changes to your payment application, you will need to seek the services of a new PA-QSA for your next validation. If you have not made changes, you will need to follow the current procedure as outlined in your revalidation notice.*

Q If I'm a customer of CSO with a payment application listed on the Council's website, am I required to notify my customers about CSO's revocation?

A *PCI SSC cannot require you to contact your customers due to CSO's revocation.*

Q Is the revocation of CSO's QSA and PA-QSA status permanent?

A *CSO has the right to appeal the revocation of its QSA and PA-QSA status. If it prevails, it will be eligible to have its status as a QSA or PA-QSA restored.*