What are we announcing?

The PCI Security Standards Council is announcing the introduction of a new program that establishes and maintains the rules and requirements regarding eligibility, selection and performance of companies that provide forensic investigation services to ensure they meet PCI Security Standards.

Who is this program for?

This program primarily applies to any compromised or potentially compromised entity that would be required by a payment card brand to have a forensics investigation conducted.

This program also applies to companies that would potentially provide forensic investigation services to any compromised or potentially compromised entity.

What does this mean for compromised entities?

Compromised entities will now have a broader selection of PFIs that will be recognized by all payment card brands.

By consolidating a list of approved PCI Forensic Investigators, compromised entities now will have a single resource of forensic investigators recognized by each payment card brand. This eases the selection process for merchants, streamlines their process and ensures consistency and quality of forensic investigations.

Does this program replace similar programs currently managed by the payment card brands?

Each of the payment card brands will continue to develop, manage and enforce their individual programs regarding when and how forensic investigations may be required. In addition, payment card brands will continue to work with their members, compromised entities, and PFIs on specific issues with each investigation.

Through the PFI program, the PCI Security Standards Council will now manage:

- rules and requirements regarding eligibility of forensic investigators;
- selection and performance of forensic investigators;
- guidance on how investigations are to be conducted and reported; and
- the list of PCI Forensic Investigators (This list will replace the separate lists maintained by the payment card brands as of March 1, 2011).

PCI SSC will not actively be involved in forensic investigations.

When does this program go into effect?

This program is in effect immediately for any compromised or potentially compromised entity who wishes to employ the services of an approved PCI Forensic Investigator, should they be required by a payment card brand to have a forensics investigation conducted.

Forensic Investigators who are not currently recognized by one of the payment card brands but wish to become a PCI Forensic Investigator are invited to submit their application to the PCI SSC after March 1, 2011.

Where can I find the list of PCI Forensic Investigators?

The list will be posted to the Council website and updated periodically as enrollment increases. Please check back regularly for the most up-to-date list at www.pcisecuritystandards.org.

This program is eliminating the specific payment card brand lists of forensic investigators. When will the transition be complete and which list should compromised entities reference in the interim?

Until March 2011, when the payment card brand lists are removed, compromised entities may use forensic investigators from either list for their forensics needs. After March 1, 2011, only the PCI SSC list of approved PFIs will be accepted by the payment brands.

What constitutes the need for a company to engage a forensic investigator? Do PCI Security Standards require that companies do so?

Each payment card brand will continue to manage requirements as to when an entity must retain the services of a forensic investigator.

After March 1, 2011, when a forensic investigation is determined to be necessary, compromised entities are encouraged to engage forensic investigators that are listed on the PCI SSC PFI program resource list and contact the affected payment card brand(s) to confirm applicable procedures and requirements

Is this a certification program?

No. This is an approval process whereby the Council will validate the previously established credentials of companies that provide forensic investigation services to ensure they meet the requirements of PCI SSC.

What are the requirements for becoming a PCI Forensics Investigator?

First, prospective organizations need to be recognized as a QSA company. It is imperative that forensic investigators involved in this program completely understand the PCI DSS and its intended application within the cardholder data environment.

Beyond that, the Supplemental Requirements document provides details on a series of expectations that each PFI candidate company is required to meet that include:

- The existence of a dedicated forensic investigation practice within your company
- People with the right backgrounds and skills
- Experience performing investigations within the financial industry using proven investigative methodologies & tools
- Relationships with law enforcement to ensure you can support any resulting criminal investigations

Do those forensic investigators currently on the payment card brands' lists have to be qualified as PCI Forensic Investigators, or do they get grandfathered into the program?

Existing companies on the respective payment card brand lists are required to submit applications to the Council to be qualified as PCI Forensic Investigators and be included on the Council's list.

How long is approval good for?

Approvals need to renewed annually.

Will the PCI SSC be receiving forensic reports?

No, the PCI SSC will not be receiving forensic reports. All forensic reports will continue to be reported to the payment brands and relevant acquirers as applicable, per payment brand requirements. The PCI SSC will be receiving sanitized, generic trend data from PFI firms on a yearly basis as a source for evolving PCI Security Standards and programs as appropriate.

What are the benefits to being approved as a PCI Forensics Investigator? Why should a forensic investigator become PCI approved?

The PFI program aligns payment card brand requirements for forensic investigators and is intended to help simplify and expedite procedures and requirements for approving and engaging forensic investigators.

The Council provides standardized reporting templates that are accepted by all payment card brands.

In addition, the Council will facilitate the aggregation of sanitized attack trends and lessons learned that will be shared and discussed within the PFI community at an annual information sharing session.

Most importantly, compromised entities can now work with a single forensic investigator who is recognized to produce a single report that will be accepted by all payment card brands. Companies not on the list by February 28, 2011, when the program transitions from the payment card brands to the Council, will no longer be approved to conduct investigations. From that date forward, there will only be one industry recognized source from which compromised entities can select their approved PCI Forensic investigator.

Can a forensic investigator still perform investigations if not approved as a PCI Forensic Investigator?

Payment card brands will only accept investigative reports started on or after March 1, 2011 from approved PFIs.

What's the difference between a QSA and a PCI Forensic Investigator? Do you have to be a QSA to be a PCI Forensic Investigator?

A PCI Forensic Investigator refers to a company, organization or other legal entity that is in compliance with all PFI company Requirements (defined in the PFI Supplement) and has been approved as a PFI by the PCI SSC as a PFI.

A QSA is a security company qualified by the PCI SSC to perform PCI Data Security Assessments, according to the PCI Security Audit Procedures. Please visit the website for details on QSA program requirements.

Not all QSAs are PFIs. In order to be considered for approval as a PFI, an entity must already be qualified as a QSA, and then must satisfy additional requirements set forth in the PFI Supplement.

How can I become a PFI? What are the requirements?

To apply, you must first contact the PCI SSC. Contact pfi@pcisecuritystandards.org with your interest in participating in the program to receive access to the PFI Registration Portal. After completing the basic information, per the guidelines set out in the Supplemental Requirements document, you'll need to take some time to gather detailed information on:

- Corporate and employee QSA credentials
- Information on how your company's forensic investigation practice will ensure independence
- Insurance coverage

- Details on your company's Forensic investigator experience & service
- The skills & experience of each of your forensic investigation employees
- Evidence of an internal forensic investigation QA program to ensure the highest quality services
- Procedures for evidence handling
- Primary & secondary contacts
- Initial processing fees

What training do I need to take and how often?

All PFI employees are expected to either actively maintain incident response certifications, such as SANs GIAC Certified Incident Handler (GCIH), GIAC Certified Forensics Analyst (GCFA) or equivalent certification satisfactory to the PCI SSC; or demonstrate a minimum three (3) years of forensic investigation/incident handling experience. In addition, PFI companies are responsible to ensure that representatives from their company participate in annual information sharing sessions sponsored by PCI SSC.

As a merchant, how do I verify the quality of PFI services? Will there be a QA program attached to this program like the QSA program? Will there be a chance to submit feedback?

The PCI SSC has created a quality assurance process as part of the PFI program that will actively evaluate the level of service being provided to the community by PFIs. This process provides for feedback from both the payment card brands and for entities making use of a PFIs services.