Briefing Note
Launch of new PCI Secure Telephone Payment Guidelines

Positioning & purpose

The Payment Card Industry Standards Security Council (PCI SSC) last published their Secure Telephone-based Payment Guidelines in 2011. The prevailing version of the PCI DSS was 2.0 and the document was focused very much on securing call recordings. Available globally, and used as the reference point for the acquiring banks and PCI DSS Certification communities (QSA's), the document did not include any reference to the technologies deployed since publication that aim to reduce the impact of PCI DSS on the contact centre environment and included little input from technology vendors and the wider QSA community.

Since publication in 2011 payment card fraud has evolved and as Chip&Pin is being rolled out globally, so there has been a significant increase in card not present (CNP) fraud. CNP fraud covers two areas, ecommerce and Mail Order Telephone Order (MOTO). Having worked hard over recent releases to secure the ecommerce channel (3.0, and 3.1), focus is now beginning to move towards MOTO with new references in the recently published PCI DSS 3.2.

In September 2015, the PCI SSC, working with two leading technology vendors and a global provider of QSA services approached Compliance3 to coordinate an effort to update the PCI SSC Secure Telephone-based Payment Guidelines. The PCI SSC brief was to prepare a first draft of a new document within eight weeks. To fast track the process Vendorcom offered to host a Special Interest Group, chaired by Compliance3, and from that base, solicit contributions from a three main groups. The widest possible engagement was required to provide a balanced view, as well as secure the documents credibility when published to a global audience. The three contributing groups were;

- The acquiring banks responsible for the contractual relationships between the payment card schemes (Visa, Mastercard, American Express, Discovery & JCB) and the merchants processing payment cards
- The QSA community responsible for the implementation and certification of PCI DSS for merchants processing > 1M transactions per annum, Third Party Service Providers processing >300K transactions per annum and those who may have experienced a data breach.
- The technology vendors themselves, many of which have a background in telephony or other contact centre related technologies.

Following feedback from the first draft, Compliance3 worked directly with the three groups to author subsequent drafts, balancing the very different objectives of each group and managing more directly the obvious underlying commercial agenda's within those groups. The end result has been a balanced draft that Compliance3 is now working on directly with the PCI SSC with the aim of releasing the document globally by September 2016.

The purpose of this Briefing Note is to inform those who have a significant role in representing the wider contact centre communities 'best interests'. Our aim is to engage help in communicating the 'availability' and the 'key messages' of the new PCI SSC Secure Telephone Payment Guidelines in a planned and structured way. They key point is to help the contact centre community understand the most effective way to digest the new guidelines and to help them understand the most cost effective ways to communicate them to their stakeholders and implement them with minimum impact to 'business as usual'.

Supporting you to support your members

As the authors of the document and committed contact centre professionals ourselves, the PCI SSC have asked Compliance3 to deliver a plan that engages the contact centre community prior to publication of their new secure telephone payment guidelines. To make that engagement meaningful and credible, we have secured diary time from the PCI SSC's lead, Jeremy King to support key messages in engagement with the global contact centre community.

The objective of the engagement is to brief community group leaders so that communication and supporting events can be diarised to coincide with the publication of the new guidelines.

The benefit to the community groups is clearly one of being able to secure messages directly from the PCI SSC and the document authors rather than through any of the individual groups engaged in the initial consultation phase or any other external body interpreting the document 'post publication'.

The benefit to Members is that they receive clear messages and interpretation of the guidelines as they apply to their own Telephone Environment, minimising the risk of misunderstanding and the breaking down common myths that have grown up in the absence of an update to existing guidelines since 2011 and the absence of guidelines regarding the impact of recent updates to the PSC DSS (3.0, 3.1 and 3.2) as they apply to the contact centre community.

General timings

- May to June
  - Initial engagement with contact centre community leaders
  - Agreement of communication support plan
- July to August
  - Circulation of supporting collateral
  - Publication of events
- September to December
  - Event support programme

Next actions

- Discuss the potential for a communication plan for Members.
- Answer questions and understand what help maybe required from the PCI SSC and ourselves.
- Agree a support plan for individual community groups.

Key messages within the new Secure Telephone Payment Guidelines

- Audience. The guidelines apply to any entity that takes payment card data over the telephone. The B&B through to a large contact centre and everything in between. The guidelines also apply to payment card issuers, acquiring banks, Third Party Service Providers as well as those qualified to support the PCI DSS certification process, the QSA community, becoming part of their own annual certification process.
- How PCI DSS should be applied to the Telephone Environment (a new inclusive term describing any physical location where telephone based payments are taken, to engage those entities who process telephone payments in a customer service environment, office, shop or reception desk).
- Overall approach to 'get risk off the table' and deploy technologies that 'devalue' the data, which means avoiding spoken payment card data entering the Telephone Environment.
- What this means for all entities and 'best practice' across key operational areas where spoken card data cannot be excluded.
- Change of status for existing technologies applying to call recorders and call recording storage.

Document ends.
Compliance3. 29.04.16