Background

Century Mail, with its headquarters in Hong Kong, provides a wide range of products (including health, leisure, fashion, household and outdoors) to a mature end-user client base predominantly based in Australia and New Zealand. Customers can purchase products via the following channels:

- Phone – handled by third party call centre based in the Philippines
- Website – using PayPal as the payment processor
- Mail order – coupons sent into a third party partner for fulfilment.

Century Mail processes card payments through all three of these channels and (as can be observed above) is reliant on third parties for its compliance with the Payment Card Industry Data Security Standard (PCI DSS). During 2015, URM was engaged by Century Mail to ensure its logistics (based in Hong Kong) and call centre (based in the Philippines) operations were compliant. This document highlights the 5 step approach adopted by URM in assisting Century Mail to be validated as a Level 1 compliant merchant.

5 Step Approach to Compliance

1. Data Flow Analysis

URM began by conducting a conference call with Century Mail to establish the high level flow of payment card information to understand the scope of the systems involved with the storage, processing and transmission of cardholder data. This process involved looking at both digital and paper systems.

2. Gap Analysis

Following the high level scoping exercise of Step 1, URM conducted a number of telephone interviews with operational personnel from Century Mail's logistics and call centre departments. These interviews helped to identify gaps in Century Mail's compliance position and formed the basis of a detailed gap analysis report.

3. Segmentation and Consolidation

Having produced the gap analysis report, URM conducted a remote workshop to clarify and explain the key findings. A key aspect of this workshop was helping to determine which systems, that were currently within the cardholder data environment (CDE), could be excluded to reduce the scope of PCI DSS. Within this, URM identified an opportunity for Century Mail to amend its process for handling cardholder data by adopting and utilising isolated virtual terminals. This approach enabled Century Mail to de-scope its CDE and segregate the payment card processing from its internal networks. Essentially, this meant introducing separate and isolated PCs installed and configured at the Philippines and Hong Kong sites which could only access a hosted virtual payment terminal (accessed as a HTTPS website). By utilising a virtual terminal approach, Century Mail could be assessed against the requirements of SAQ C-VT which contains approximately 75 requirements.

4. Remediation

This stage involved the resolution of further gaps identified in Step 2 which still existed following the segmentation activities undertaken in Step 3. In order to provide as much clarity as possible, URM produced a set of documents aimed at providing Century Mail with a baseline on which to build its PCI compliance around. Having established these necessary core documents, URM facilitated awareness

© 2019 URM

sessions to applicable staff highlighting the key messages and providing clarification where processes had been implemented or amended.

5. Validation

The final stage, involving a separate URM team, was to conduct a formal onsite assessment both in Hong Kong and Philippines, resulting in a successful Report on Compliance (RoC)

When asked to comment on the role played by URM, Phil Gebbett, Director at Century Mail commented “I was very impressed by the responsiveness, expertise and pragmatic approach of URM. There were a number of specific challenges attached to the project, most notably the tight deadlines and the involvement of third parties operating across a number of countries and with different languages and cultures. URM was able, however, through its consistent project management, combined with strong technical documentation and clear communication, to keep all parties fully aware and informed of exactly what actions were required to achieve compliance. URM’s advice around de-scoping elements of the cardholder data environment and the adoption of isolated, virtual terminals was invaluable.”

© 2019 URM