Message to All Non-CBM Merchants with Virtual Terminal Processes with TD and Moneris

Last updated: Sep 18, 2010

The following message is being sent on behalf of
Ram Muhunthan (PCI Program Manager) and Larry Carson (Associate Director, Information Security Management).

We have obtained approvals from both TD Merchant Services and Moneris for Virtual Terminals to be a SAQ C if the following requirements/conditions are met by your unit:

1. Merchant clerks will be typing credit card information via web browser straight into the payment processor's web page that is hosted on the payment processor's web site via SSL or TLS. Merchant clerks are NOT using card swipe machines for entering the credit card information into the payment processor's web page.
2. Credit card info will never be stored on the merchant PC
3. Merchant clerks will be trained on how to use the browser in a secure fashion
4. The Security policy will strictly cover acceptable use of the PC Security mechanisms such as personal firewall, anti-malware, anti-virus, network access control and data loss prevention will be installed on each PC
5. Virtual Terminals will be segmented from the rest of our environment. We will be using host based firewalls and Network Access Control (NAC) for segmentation and they will be managed via a central policy server. Furthermore, we have DLP (Data Loss Prevention) as an added level of protection to further control and limit the risk.

Larry Carson has made a proposal for a central Enterprise Console to be setup for full Sophos endpoint deployment (anti-virus, anti-malware, host firewall, NAC & DLP) but does not know if this request will be approved.

Update Sep 18, 2010: the Enterprise Console has been deployed and is currently in the pilot stage. All Non-CBM merchants, who have not already secured their VTs (as described above) via the endpoint security controls, should be piloting with the intention to be fully compliant before the end of Sep 2010.

In the meantime, if you want your Virtual Terminal process(es) to fall under a SAQ C, it is advisable that you start working towards achieving compliance following the above Virtual Terminal guidelines along with the SAQ C requirements. If the request is approved to build out a central Enterprise Console, you can switch over at that time. **To avoid duplication of effort, please inform Linda Ma (linda.ma@ubc.ca) and Ram Muhunthan (ram.muhunthan@finance.ubc.ca) of your plans and progress for your Virtual Terminals.**

Your unit will have to address the following:

1. **A central Enterprise Console for Sophos along with deployment and management ability for host-based firewall, anti-malware, anti-virus, network access control and data loss protection**
   Our Sophos licensing includes the Endpoint Security & Control product. So for desktops you can install the centrally managed Anti-virus, Anti-malware, host based firewall (ingress – egress filtering), data loss prevention and Network access control; this will address the QSA's recommendation for the virtual terminals.

2. **Develop a training process for how to use a Virtual Terminal in a safe fashion, including the browser**
   We have no documentation on processes for this, nor do we have training material. It needs to be developed for your specific business operation for all Virtual Terminal users – if we

have a breach on a Virtual Terminal because a user was not properly trained then it is highly probable that the acquirers will put Virtual Terminals back to a SAQ-D for all of UBC.

3. **An acceptable use policy for Virtual Terminals needs to be developed**
   Any users of Virtual Terminals must sign-off on the AUP and re-certify (via sign-off – we need actual signatures on paper) annually that they understand and are adhering to the requirements of that policy document.

Please distribute this to all in your units who need to know or who are affected by this.

Thank you,