Feb. 18, 2008

VeriFone Response to questions:

- Which testing laboratory evaluated the Dione PED under the Visa PED specification.

  This is confidential information and is covered under Non-Disclosure.

- Were the vulnerabilities we identified recognized during the evaluation?

  The Xtreme PED hardware was successfully evaluated against the then current Visa PED specifications.

- If so, how were they dealt with? If not, where do you think the evaluation process failed?

  N/A

- Can we have the evaluation report?

  The evaluation report is covered under strict Non-Disclosure and is not available to the public.

- Can you explain why certification reports are not public when they are of public interest and their results affect customers?

  The reports contain highly detailed proprietary design documentation which is VeriFone and security laboratory confidential.

- Is the certification of the PED we studied to be withdrawn?

  Not that we are aware.

- Is the affected PED to be withdrawn from use, and if so, when?

  N/A

- If we find further vulnerabilities in other PEDs, will those be promptly withdrawn from the market?

  That is a decision made by APACS and PCI.

- Are you aware of other PEDs with the same issues?

  It is a question for APACS and law enforcement if there are PEDS which have been compromised.

- If so, will their certification be withdrawn?

  N/A

- Is the testing lab who performed the evaluations to have their accreditation revoked?

  This is a question for the Common Criteria certification agency and PCI SSC.

- What changes, if any, will be made to the certification processes in order to prevent such failures in the future?

  We are not aware of any failures of the system. The security requirements have been evolving and updated continually over the years, in fact we are already two revisions beyond the version which was used in the evaluation of the products covered in this report.

- What measures are in place or being put into place to mitigate the vulnerabilities we discuss?

The PED Hardware security is only one piece of the overall security of the merchant environment. The card associations have had in place other best practices for merchants to follow as well as system level security requirements such as PCI DSS.

- Were these vulnerabilities recognized during the PED development process?

We consider many potential attack scenarios as do the security labs as part of the security evaluation process.

- What changes in the PED development process are to be taken to prevent further vulnerabilities?

See the note about updated security requirements above. VeriFone is continually updating and enhancing the security of our systems to meet the latest requirements.

- Are you aware of any cases where PED tampering was used for fraud? If so, can you provide details? If no details can be provided, can you at least provide the number of cases seen and the sums involved?

We have been made aware of a limited number of cases. We do not have detailed information on these cases.

- Can you assess the risk to customers from these vulnerabilities based on your (yet, non-public) knowledge of the types of fraud committed by criminals?

The hardware security requirements (UKCC and PCI PED) are pushing the fraudsters to use other easier attacks and those which don't put them in personal exposure.

- Will any other action be taken as a response to our paper?

Security is a moving target. Anything we can learn we are interested to consider in our products.

- Will you provide us newly approved PEDs for evaluation?

We would consider this if your organization becomes an accredited PCI and CC laboratory. We work with virtually all approved security laboratories around the world.

- Do you have any further comments to add?

We believe it is not in the best interest of the consumers, merchants and overall payment industry to publish the details of product designs describing potential attacks however remote those might be. Even if these attacks are difficult to be accomplished it gives the bad guys a leg up on research they would not have to do and encourages bad behavior.

We would like a copy of the full technical report to understand what exactly was done and how it was done.

We would like to know which publication this report will be published and when.