

CCR CCR DATA SYSTEMS, INC.

www.ccrdata.com • (603) 224-7757 • FAX (603) 224-7709

July 27, 2012

Attorney General Michael Delaney
Office of the Attorney General
NH Department of Justice
33 Capitol Street
Concord, NH 03301

Dear Attorney General Delaney:

My company is writing to notify you of a breach of security and possible unauthorized access or use of personal information involving an unknown number of Massachusetts and New Hampshire residents. This occurred at one of our customers: Tobacco Haven at 44C Route 13 in Brookline, NH.

NATURE OF THE SECURITY BREACH

The store utilizes an NCR Advanced Checkout Solution system installed by CCR Data Systems at 128 Airport Road in Concord, NH. This system accepts credit/debit payments from a Verifone pinpad unit at each lane as part of the point of sale (POS) transaction and then hands payment information over to a WorldPay computer, installed in the store by C&S wholesale. The WorldPay computer communicates with the processor computers via a secure Internet connection to receive an approval and then communicates this back to the POS registers. Within the last few months C&S staff was informed by Citi Fraud Services and the Secret Service that some suspicious activities were occurring regarding credit cards that had been swiped at the store. C&S informed CCR of the possibility of a breach of the system. In early July Secret Service agents became involved, seeking to track the possible criminal activity. CCR technicians also examined these computers and noticed certain suspicious processes running on the NCR POS file server. Upon further investigation it became clear that these processes were malware and that they appeared to be taking snapshots of network traffic and saving aside cardholder data in a log file.

NUMBER OF RESIDENTS AFFECTED

While the log file discovered contained credit card records, it is not possible for us to determine if this log was ever harvested or had previously been cleared out by the criminals.

STEPS TAKEN RELATING TO THE BREACH

CCR Data Systems was unable to ascertain how the malware came to reside on the system. The Sonicwall firewall was in place and functioning. CCR immediately changed the PC Anywhere remote support access password. After being informed by the Secret Service that their criminal investigation was completed, CCR staff

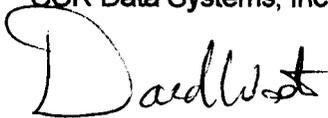
July 27, 2012

quarantined the malware, confirmed that the system was clean and continues to monitor the network. Store management put procedures in place to ensure that no email or internet browsing whatsoever takes place on the POS computers. The antivirus was updated. Store management also changed the access passwords for the NCR POS system.

OTHER NOTIFICATION AND CONTACT INFORMATION

The US Secret Service has been involved and has done forensic work in conjunction with this infection. The agent that was working on this is Special Agent Matt O'Neill at 603-626-5631.

Sincerely,
CCR Data Systems, Inc.

A handwritten signature in black ink, appearing to read "David Woetzel". The signature is written in a cursive style with a large initial "D".

David Woetzel
President/CEO

cc: Tobacco Haven