WIGGIN AND DANA

Counsellors at Law

Wiggin and Dana LLP
One CityPlace
185 Asylum Street
Hartford, Connecticut
06103-3402
www.wiggin.com

Aaron S. Bayer

VIA OVERNIGHT DELIVERY

January 31, 2011

The Honorable Michael A. Delaney
Attorney General
New Hampshire Attorney General's Office
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Breach

To Whom It May Concern:

We write on behalf of our client, the University of Connecticut Cooperative Corporation (the "Co-op"), to advise you that a hacker has obtained unauthorized access to a database that contains customer information, including credit card information, for customers who have purchased products from HuskyDirect.com, a website owned by the Co-op and hosted and managed by its vendor Fuss & O'Neill Technologies LLC (doing business as Fandotech), with offices at 893 Main Street, Manchester, CT 06040. The database contained information for 286 residents of New Hampshire. The Co-op is a not-for-profit corporation that sells textbooks and other educational supplies to University of Connecticut students and other merchandise to the University's community, including fans.

Discovery of the Breach. The breach was discovered because customers called the Co-op reporting that their cards had been misused. On December 28, 2010, the Co-op called Fandotech to inform Fandotech about the reports of credit card misuse, and the Co-op asked Fandotech to investigate. Fandotech reported that it found no evidence of any breach. The Co-op then called a few more times over the subsequent days asking Fandotech to investigate again. It took some time for Fandotech to uncover the breach, and on January 5, 2011, Fandotech determined that a hacking incident had taken place on December 26, 2010, when the hacker gained access using Fandotech's administrative password. Fandotech has sole access, authority, and control over that administrative password.

Data Involved. The database accessed by the hacker contained information on a total of 18,059 individuals, and of those people 286 are residents of New Hampshire. The HuskyDirect.com database contained some or all of the following information for customers who used that site: name, address, telephone number, email address, and credit card number, expiration date, and security code. The database did not contain any dates of birth, bank account information, or Social Security Numbers. Accordingly, the risk from this breach is credit card misuse, not identity theft. The

breach also did not involve any of the databases related to the Co-op's sales in-person or through other web sites.

The information obtained from customers through the HuskyDirect.com website was secured on a server hosted by Fandotech. The Co-op understood from Fandotech that it employed a firewall, antivirus software, encryption, and a secure, administrative password to safeguard this data, and believed that Fandotech was PCI compliant. Fandotech can provide additional information about the security measures it employed to protect the data.

Response to the Discovery. Initially, the Co-op contacted Fandotech, which undertook its own investigation. The Co-op also contacted: (1) the University of Connecticut ("UConn") campus police, which, in turn contacted the Manchester, CT Police and the FBI; (2) the affected individuals to alert them of the possible compromise of their credit cards and advise them about the steps they should take to protect themselves (the Co-op's notice to these individuals is attached hereto as Exhibit A); (3) the Co-op's merchant processor, Trisource, to provide a list of the credit card numbers so that the card issuers could be notified; and (4) the Connecticut Attorney General's Office. The Co-op also directed Fandotech to take the HuskyDirect.com website down, and, despite significant commercial cost, has not returned the site to operation. The Co-op has engaged a company (Debix) to provide credit monitoring and identity theft insurance to the affected individuals and a company (Trustwave) to perform a forensic computer audit to determine the cause and cure for the problem. On January 21, 2011, the Co-op contacted the affected individuals a second time via email/letter encouraging them to take actions to safeguard their credit cards, including closing their account or changing the card number on the relevant card (the Co-op's second notice is attached as Exhibit B). In approximately one week, the Co-op, through the services of Debix, will send a third notice to all affected individuals to offer them one year of free credit monitoring and identity theft insurance (a copy of that letter is attached as Exhibit C). The delay in offering these services is a result of the Co-op's protracted contract negotiations with Debix to ensure that sufficient protections for customer's information provided to Debix were included in the contract.

Fandotech can provide additional information about the specific steps that it took once it discovered the hacking incident.

In addition to the steps identified above to investigate this incident, the Co-op is taking steps to prevent any future breaches. The Co-op will not reopen the old web site, but instead intends to

create a new website for the sale of UConn merchandise. The Co-op will not operate a new website for this purpose until the Co-op has assurance that the website is in a secure environment.

The Co-op regrets the inconvenience this incident may have caused to any residents of New Hampshire. If you have any additional questions, please contact me.

Sincerely,

Aaron S. Bayer

Enclosures

1945\1\2508666.1