

NIXON PEABODY_{LLP}
ATTORNEYS AT LAW

900 Elm Street
Manchester, New Hampshire 03101-2031
(603) 628-4000
Fax: (603) 628-4040
Direct Dial: (603) 628-4051
Direct Fax: (866) 947-0896
E-Mail: jchood@nixonpeabody.com

December 3, 2008

Via First Class Mail

Lauren Noether, Esq.
State of New Hampshire, Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Notification Pursuant to New Hampshire Rev. Stat. § 359-C:20

Dear Lauren:

As I mentioned during our telephone conference on November 25, 2008, I serve as general counsel to the Zycorp family of companies, including Zycorp Entertainment I, LLC (“Zycorp”), which own and operate Cinemagic® Stadium Theatres. As a follow up to our conversation from last week, we are writing pursuant to RSA § 359-C:19 *et seq.*, to formally notify you of a potential security breach at the Cinemagic® theatre located in Merrimack, New Hampshire involving the probable compromise of credit card and/or debit card numbers, but without security codes, access codes, passwords or expiration dates. Radiant Systems, Inc. (“Radiant”), Zycorp’s payment application vendor, has confirmed that storage and transmission of credit card and/or debit card numbers are properly encrypted. While we do not believe Zycorp is required to provide notice pursuant to § 359-C:20 because it does not “own or license computerized data that includes personal information” and because the compromised data does not meet the definition of “personal information” within §359-C:20, we are writing this notice out of an abundance of caution.

On or about November 5, 2008, Visa notified Bank of America (BOA) Merchant Services (the “acquiring” bank) that Sovereign Bank and St. Mary’s Bank (“the issuing banks”) had contacted them identifying fraudulent transactions associated with approximately 36 Sovereign Bank Visa accounts and 20 St. Mary’s Bank Visa accounts. Visa concluded that all 56 accounts had legitimately been used at a Cinemagic® theatre between January 6, 2008 and October 17, 2008 (i.e. a common point of legitimate transaction). Radiant has, after investigation, determined that the legitimate transactions for the 56 accounts were processed at the Merrimack facility and that no other locations have been affected.

Zyacorp is not privy to the identification information for the affected individuals. Thus, Zyacorp has no way of knowing how many of the 56 accounts belong to New Hampshire residents. Under the circumstances, Zyacorp has, through BOA Merchant Services, notified those institutions whom it believes "owns" the compromised information under the provisions of RSA § 359-C:20, I(c). Notwithstanding the fact that it has not been provided such information, Zyacorp does not believe that it has an obligation to notify individual account holders under RSA § 359-C:20, I(a).

Since learning of the incident, Zyacorp has:

1. Cooperated fully with the United States Secret Service and state law enforcement which continue to actively investigate the incident;
2. Worked with BOA Merchant Services to upload the compromised card numbers to Visa's alert system (CAMS) which notifies the issuing banks of the compromised activity;
3. Conducted, and has caused to be conducted, internal investigations of its equipment, personnel policies, intellectual property and software programs and its on-site information technology.

Zyacorp is continuing to work with law enforcement as well as with its information technology to review current policies and procedures to identify the manner in which the security breach occurred and steps that can be taken to better protect against an incident of this kind.

If you have any questions regarding this incident or wish to speak with me further regarding the foregoing, please feel free to contact me or my colleague Courtney Brooks directly.

Very truly yours,



James C. Hood

JCH/cdm