



STATE OF MAINE
 DEPARTMENT OF PROFESSIONAL
 AND FINANCIAL REGULATION
 BUREAU OF CONSUMER CREDIT PROTECTION
 35 STATE HOUSE STATION
 AUGUSTA, MAINE
 04333-0035

JOHN ELIAS BALDACCI
 GOVERNOR

WILLIAM N. LUND
 SUPERINTENDENT

October 27, 2009

Linda Conti
 Assistant Attorney General
 Office of the Attorney General
 6 State House Station
 Augusta, ME 04333-0006

Re: **The Vernon Company: Notification of Security Breach**

Dear Ms. Conti:

Enclosed please find notification of security breach from The Vernon Company.

We are forwarding this to your attention because we do not regulate the company as it is not a creditor and is out of our jurisdiction.

Feel free to contact me with any questions.

Sincerely,

Doris A. Whitaker, Assistant to
 William N. Lund, Superintendent

cc: Joseph M. Stocker
 Vice President, Secretary-Treasurer
 The Vernon Company
 One Promotion Place
 Newton, IA 50208

CONSUMER PROTECTION DIVISION
 RECEIVED
 OCT 28 2009

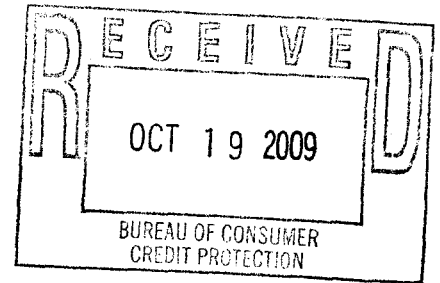


PRINTED ON RECYCLED PAPER

vernon
SALES PROMOTION

Joseph M. Stocker
Vice President, Secretary-Treasurer

The Vernon Company
One Promotion Place
Newton, Iowa 50208
641-792-9000 x. 8341
641-791-8603 (fax)
joes@vernoncompany.com



October 12, 2009

Department of Professional & Financial Regulation
Bureau of Consumer Credit Protection
35 State House Station
Augusta, Maine 04333

RE: Notification of Security Breach

Dear Sir/Madam:

I am writing to notify you of possible unauthorized access of personal information involving 8 Maine customers.

On the afternoon of October 6, The Vernon Company Information Technology Department discovered possible unauthorized access to The Vernon computer software database through the vernoncompany.com website. After further investigation, it is reasoned to believe this unauthorized access may have happened as early as July 2009. Vernon believes this attack originated in Singapore. Vernon immediately shut down the website and has taken action to prevent a recurrence of this incident.

We believe the unknown person or persons gained access to names, addresses, and credit card information of 8 customers located in Maine. To-date Vernon has notified its general counsel and the FBI of the breach and is working to notify the other governmental and law enforcement entities as required by applicable local laws. On October 13, Vernon intends to send written notification to the affected customers of Maine. A copy of this notice is attached.

Please contact me with any questions or concerns regarding this incident.

Sincerely,

Joseph M. Stocker
Vice President, Secretary-Treasurer

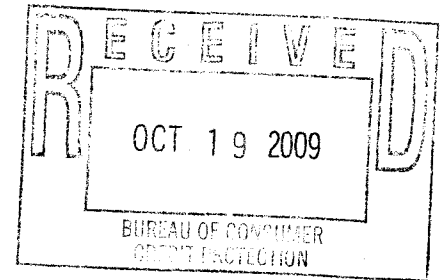


Notification to Customers

October 12, 2009

Customer Name
Customer Company
Customer Street
Customer City, State, Zip

Re: Card Type - XXXX
Ending in - XXXX



Dear Customer,

On October 6, 2009, our Information Technology Department discovered possible unauthorized access to The Vernon Company computer software database. If this in fact did occur, it was in violation of both civil and criminal laws. Vernon has been in contact with federal law enforcement to assist in the investigation of this incident.

In general, the computer systems contained customer information such as name and address, the number on a credit or debit card, and the expiration date on the card. I would like to stress that the computer systems contained no social security numbers.

We are notifying you of this breach because you are one of the customers whose information was contained in the computer system. Although we have no evidence that an unauthorized individual has actually retrieved and is using your personal data, we are bringing this to your attention so that you can be extra alert to signs of any possible misuse of your information.

Upon discovering the possible breach on October 6, 2009, we immediately shut down the vernoncompany.com web site until all vulnerabilities were patched with secured code. After additional analysis it was determined the possible breach may have occurred as early as July 2009. Vernon values your privacy and has implemented additional security measures designed to prevent a recurrence of such an attack. In addition we are providing the following steps you can take to help protect yourself:

- **To protect yourself from the possibility of identity theft, we recommend you immediately contact the bank that issued your credit card and inform them of the possible breach. They will be able to take any further action that may be required.**
- **You should also review your account statements and your credit reports carefully and often, to make certain there have been no unauthorized transactions made or new accounts opened in your name. Specifically, review the information for accounts you did not open, inquiries from creditors that you did not initiate and personal information that are inaccurate. If you detect any suspicious activity on your account**

statement(s) or credit report(s), you should promptly notify the credit card issuing bank or other financial institution(s) as well as your local police department, State Attorney's General and the Federal Trade Commission.

- Contact the three credit bureau agencies. You have the right to obtain a copy of your credit report for free once a year from each credit reporting agency by contacting one of the agencies listed below or by visiting www.annualcreditreport.com or by calling toll free 877-322-8228. Hearing impaired consumers can access TTD service at 877-730-4104. You may order one, two or three reports at the same time, or you may stagger your requests during a 12-month period to keep an eye on the information in your reports. The contact information for the three bureaus is as follows:

Equifax
(877) 478-7625
www.equifax.com

Experian
(888) 397-3742
www.experian.com

TransUnion
(800) 680-7289
www.transunion.com

- You also have the right to place an initial "fraud alert" on your credit file. A "fraud alert" lets creditors know that they should contact you before they open a new account in your name. You can do this by calling any one of the three credit reporting agencies at the numbers above. This will let you automatically place fraud alerts with all three agencies listed above. The "fraud alert" will stay on your account for ninety days. After that, you can renew the alert for additional ninety-day periods by calling anyone of the three agencies.
- To obtain additional information on how to avoid identity theft, please contact the Federal Trade Commission at 1-877-438-4338 or www.ftc.gov/idtheft..

We deeply regret this situation and any inconvenience or alarm it may cause you, but we believe it is important for you to be fully informed of any potential risk. Again, we want to assure you we have no evidence your data has been misused. We are continually modifying our systems and practices to enhance the security of sensitive information.

Should you have further questions about this matter, please contact:

Dave Regan, Vice President – Sales at daver@vernoncompany.com or 1-800-743-7545, extension, 8256, Sharla Elscott, Business Development Manager at sharlae@vernoncompany.com, or extension 8242, or Andrea Smith, Recruiting Specialist at andreas@vernoncompany.com, or extension 8168.