Respond to Dayton Office

August 8, 2011

VIA OVERNIGHT MAIL

New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: Thirty-One Gifts, LLC

Dear Office of the Attorney General:

This letter is sent pursuant to the notice requirements of New Hampshire Revised Statutes § 359-C:20 as a result of recent incidents where Thirty-One Gifts, LLC ("Thirty-One"), a company headquartered in Columbus Ohio, learned of a data breach. During its investigation, Thirty-One discovered that a laptop containing personal information of a number of employees and consultants was missing.

An internal investigation produced evidence that someone had misappropriated employee administrative credentials to illegally alter commission payments on the profiles of 28 Thirty-One Consultants and route those payments to his own bank accounts; Thirty-One is actively working with law enforcement to investigate the incident and identify the person responsible. There were no consumers from New Hampshire whose name, address, Social Security Number, and bank account information may have been accessed.

During its investigation, Thirty-One discovered that a laptop containing personal information of a number of Consultants was missing. There were 27 New Hampshire residents whose name, address and bank account information may have been on the laptop. There is no evidence to suggest that the events were related, or that any consumer has been the victim of identity theft. However, in an abundance of caution, Thirty-One has decided to notify all

Consultants whose personal information may have been on the laptop, as well as the 28 Consultants whose personal information was accessed by the intruder.

Thirty-One plans to send the notification letters on August 10, 2011. Enclosed is a copy of the notice to be sent to New Hampshire residents.

Thirty-One takes the protection and security of consumer personal information in its possession very seriously. In response to this incident, Thirty-One has taken a number of steps to improve its security policies and procedures, to investigate the breach, and to further protect its Consultants, employees and customers from a similar breach in the future, including the following actions:

- Thirty-One retained Kroll Inc. ("Kroll") to conduct a thorough investigation of the incident and to prepare a report, which was provided to the Federal Bureau of Investigation to assist it in its efforts.

- All affected Consultants and employees will be offered, without charge, one year of enrollment in Kroll's ID TheftSmart service. This service includes identity theft consultation and restoration and continuous credit monitoring.

- A toll-free telephone number will be established where affected Consultants and employees can obtain more information. In addition, Thirty-One is advising that accounts be monitored for unusual activity and that suspected identity theft be reported to law enforcement.

- Thirty-One engaged Ira Winkler of Internet Security Advisors Group, a nationally-recognized expert on information security, to conduct a complete assessment of Thirty-One's systems and policies and to provide recommendations for improvement. Thirty-One continues to work with Mr. Winkler to improve its security.

- Until recently, Thirty-One relied on a software package called Party Plan, hosted by a third-party, for sales and commissions functions; Thirty-One had little control over security controls embedded in the Party Plan solution. Thirty-One has licensed the Party Plan software source code in order to exercise better control over its security features.

- An expert in payment card industry and information security procedures has been hired as a full-time employee in Thirty-One's Information Technology Department.

- Thirty-One has strengthened its policies regarding system access rights to ensure that personal information may only be accessed by persons who have a legitimate business use for that information.

- Training is being provided to Thirty-One consultants regarding current best practices for handling credit card information.

Please do not hesitate to contact me if I can be of further assistance.

Very truly yours,

Ronald I. Raether, Jr.

RIR/bsf
Enclosure

thirty-one™

URGENT — Please Open Immediately.

<<FirstName>> <<MiddleName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<StateProvince>> <<PostalCode>>
<INTELLIGENT MAIL BARCODE>

ID TheftSmart™

<<FirstName>> <<MiddleName>> <<LastName>>
Membership Number: <<MembershipNumber>>

Member Services: 1-855-XXX-31GCus
8:00 a.m. to 5:00 p.m. (Central Time), Monday through Friday
If you have questions or feel you may have an identity theft issue, please call ID TheftSmart member services.

<<Date>> (Format: Month Day, Year)

RE: Thirty-One Gifts Missing Laptop

Dear <<FirstName>> <<MiddleName>> <<LastName>>,

I am writing to inform you that your personal information may have resided on a laptop that turned up missing. While we currently have no evidence to suggest that identity theft has occurred, it is possible that someone may have illegally gained unauthorized access to your personal information stored on the password protected laptop, including your name, address, and bank account information. None of your other personal information was on this laptop.

We learned the laptop was missing during an investigation into a criminal attempt to defraud and steal from Thirty-One. We have been actively working with law enforcement to investigate an individual's inappropriate use of an employee's administrative credentials to illegally alter commission payments on the profiles of 28 Consultants and route those payments to his own bank accounts. Internally, we quickly detected this activity, and it only persisted over the course of two commission cycles. If you are one of these 28 Consultants, then you already know about this incident as we have reached out to you separately.

We have discovered no evidence that the two events are related, but out of an abundance of caution, we are providing notice to you and all the other Consultants whose information we believe may have been on the laptop. While we currently have no evidence to suggest that identity theft has occurred, there is some possibility—however unlikely—that someone may have illegally gained unauthorized access to your personal information stored on this laptop.

We have been actively engaged with the FBI and the United States Attorney's Office for the Southern District of Ohio as they investigated the misuse of our systems. The incident that causes us to write you occurred late last year; we could not tell you until now because law enforcement requested we not notify you or talk about this incident while they conducted their investigation, and until they lifted that "hold"—which they did on August 10, 2011.

While we instruct all our employees to safeguard company equipment, this laptop, while stored in a secure location, went missing. Regardless, we have re-examined our security policies. We further enhanced our internal systems and controls to safeguard our information to help prevent additional criminal attacks, partnering with a nationally-respected security expert to help us with this effort. I can assure you that privacy protection will continue to be a central commitment to our mission to empower women through offering quality products and the opportunity to become successful business owners.

<u>Services Thirty-One Is Providing to You</u>

Because securing your personal information is so important to us, we have engaged Kroll Inc., the world's leading risk consulting company, to provide its ID TheftSmart™ service to you for one year without any cost to you. Kroll's Fraud Solutions team has extensive experience in helping people who have experienced the unintentional exposure of confidential data. Thirty-One is providing you with access to:

Enhanced Identity Theft Consultation and Restoration. Licensed Investigators who understand the problems surrounding identity theft are available to listen, to answer your questions, and to offer their expertise regarding any concerns you may have. Should your name and credit be affected by this incident, your investigator will help restore your identity to pre-theft status.

Continuous Credit Monitoring. Monitoring alerts make you aware of key changes using data from your Experian credit file that could indicate the kind of unauthorized activity commonly associated with identity theft and fraud.

Please see the enclosed brochure for simple instructions to take advantage of Kroll's ID TheftSmart service. To receive online credit services, please visit www.idintegrity.com to complete your authorization. To receive offline credit services through the mail, please fill out and return the enclosed *Consumer Credit Report and Credit Monitoring Authorization Form*. Note, however, that if you fill out and return the authorization form to receive credit services through the mail, you cannot sign up online.

You may call 1-855-XXX-31GCus, 8:00 a.m. to 5:00 p.m. (Central Time), Monday through Friday, if you have any questions or feel you may have an identity theft issue.

The success and growth of our company is a very real testament to each of you and your enthusiasm, your skills and hard work. As we look to the future, please be assured that we will continue to do what is right to help ensure the long-term success of our thriving company for our customers, our Consultants, and our employees.

Very truly yours,

Cindy Monroe
Founder & CEO

Enclosure