



VIA CERTIFIED MAIL

Consumer Protection and Antitrust Bureau
c/o Lauren Noether
SECURITY BREACH NOTIFICATION
33 Capital Street
Concord, NH 03301

Dear Ms. Noether:

Pursuant to the N.H. Rev. Stat. Ann. (§ 359-C:20) (2007), this letter is to inform you that S&K Famous Brands ("S&K") recently experienced a data security breach in its online store located at www.skmenswear.com. S&K has reason to believe that the personal information of 25 of its online customers who reside in the State of New Hampshire may have been accessed on or about October 24, 2007 without proper authorization. The personal information affected may include the name and address of the resident, his or her credit card number, and the expiration date of his or her credit card. S&K has determined, however, that no social security numbers, CVV2 data, or track 2 magnetic stripe data were compromised during the breach.

S&K was notified of a suspicious e-mail addressed to its customers on Wednesday, October 24th at approximately 3:00 p.m. (a copy is attached for your convenience). The e-mail was sent from a fictitious S&K e-mail address. The body of the e-mail appeared to contain an S&K order number and the last four digits of the credit card number used by the customer to whom it was addressed. The e-mail requested that the customer provide a credit card identification number.

Once notified, S&K immediately assembled a response team to assess the situation. Because the response team could not readily determine if there had been a breach of the online store or if someone had intercepted an S&K order confirmation e-mail, a decision was made at 3:30 p.m. the same day to disconnect the online store and disable remote access to S&K's network. Further to these actions, S&K:

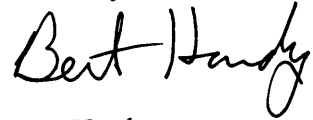
- Notified credit card issuers
- Purged or masked credit card data on its servers
- Changed all user names and passwords on the system
- Hired a leading provider of information security to conduct a full forensic security audit as required by the major credit card issuers
- Notified various law enforcement agencies including the FBI and Secret Service

S&K Famous Brands, Inc.
Mailing: P.O. Box 31800, Richmond, Virginia 23294-1800
Shipping: 11100 West Broad Street, Glen Allen, VA 23060
Telephone: 804-346-2500 Fax: 804-747-3979 <http://www.skmenswear.com>

S&K's investigation of this incident is ongoing. In addition to continuing its investigation, S&K plans to send notices to all affected New Hampshire residents no later than Wednesday, December 5, 2007 as required by the N.H. Rev. Stat. Ann. (§ 359-C:20) (2007).

S&K believes this letter is compliant with the notice requirements delineated in the N.H. Rev. Stat. Ann. (§ 359-C:20) (2007). If, however, you require additional information or documentation, please do not hesitate to contact Bert Hardy at (804) 346-2500. Thank you for your time and attention.

Sincerely,

A handwritten signature in cursive script that reads "Bert Hardy".

Bert Hardy
Chief Information Officer

Example of email:

From: skmenswear@gmail.com [mailto:skmenswear@gmail.com] **On Behalf Of** - S&K Menswear

Sent: Monday, October 22, 2007 5:32 AM

To: pterhune@carolina.rr.com

Subject: S&K Menswear notice: Verify order number 26372 - Please hit reply to all when sending e-mail back -

Order number:26372
Card ending ...2374

Thank you for your recent order on **S&K Menswear Store** , referenced above.

For security reasons, please include the card identification number in your reply - this is a 4 digit number on the front of American Express cards, and on all other cards, it is the last 3 digits printed in the signature area on the back of the card.

Please reply promptly to verify your order, usually within 24 hours.

Thank you.

Please hit reply to all when sending e-mail back

S&K Famous Brands, Inc.
11100 West Broad Street
Glen Allen, VA, 23060

December 10, 2007

You do not need to make any changes to your S&K menswear accounts or to change the way you do business with us.

Dear Valued Customer:

Let us tell you why you are receiving this email. While investigating reports of suspicious email activity, we recently discovered unauthorized access to our online store www.skmenswear.com. This unauthorized access was immediately eliminated; however, certain customer information stored in one of our databases has been retrieved by external sources. This letter is to inform you that S&K Menswear has discovered that your personal information—including your name, address, credit card number, and expiration date—may have been accessed on or about October 24, 2007 without proper authorization. We want to stress, however, that no social security number, CVV2 data or track 2 magnetic stripe data was compromised at all.

Upon learning of this unauthorized access, S&K Famous Brands:

- Disconnected the system in question
- Immediately began an investigation, which is still ongoing at this time
- Notified the credit card issuers
- Purged or masked credit card data on our servers
- Changed all user names and passwords on the system
- Hired a leading provider of information security to conduct a full forensic security audit as required by the major credit card issuers
- Notified various law enforcement agencies including the FBI and Secret Service

As always, we encourage you to remain alert in guarding your personal information, regularly review your account statements, and monitor your credit activity from the major reporting agencies (see the attachment to this correspondence if you suspect identity theft).

We sincerely apologize to you for this situation and want to assure you that protecting the security and privacy of your information remains a top priority. We have made and will continue to make significant investments in security software, systems and procedures, and we will remain vigilant about protecting you.

We want to answer any questions and address any concerns that you may have about this matter. For more information, including a list of Frequently Asked Questions (FAQs), please go

to www.skmenwear.com/security/faq.htm or contact us at 1 (800) 690-4996. We encourage you to review the FAQs and, if you have a question, send us an email at security@skmenwear.com. Once again, please be assured that your security and privacy are our top concern at S&K Menswear.

Sincerely,

S&K Menswear

Attachment – what to do if you suspect identity theft:

S&K Famous Brands is providing you with the following information to help protect you from potential misuse of your information, including the potential of identity theft. If you suspect identity theft, we recommend that you contact the credit reporting agencies in order to:

- Place a fraud alert or security freeze on your credit file. A fraud alert tells creditors to take extra precautions before they open any new accounts or change any existing accounts. A security freeze prevents third parties from accessing your credit report without your consent.

A fraud alert can be placed by calling the Automated Fraud Alert systems at the numbers below for any one of the three credit reporting agencies. You only need to contact one of the three credit reporting agencies; your request will be shared electronically with the other two repositories.

A request for a security freeze, however, must be made with each of three credit reporting agencies for it to appear in their records. Such requests are typically required to be made in writing.

- Request a free copy of your credit report and review the credit report for suspicious activity. Credit bureau employees are available to help you interpret your report once you receive a copy of it, if needed.
- Check your credit card and other account statements regularly. Also check your credit report periodically. If you find suspicious activity on your account statements or credit report or have reason to believe your information is being misused, you should call your local law enforcement agency and file a police report. You should get a copy of the police report since many creditors want the information it contains to address the fraudulent debts. You should also notify Experian, TransUnion and Equifax as well as file a complaint with the FTC at www.consumer.gov/idtheft or at 1-877ID-THEFT (438-4338). The complaint will be accessible to law enforcement for their investigations.

Equifax Credit Information Services, Inc.
P.O. Box 740256
Atlanta, GA 30374
www.equifax.com
Automated Fraud Alert-
1.800.525.6285
Order Credit Report-1.800.685.1111

Transunion Credit Bureau
P.O. Box 6970
Fullerton, CA 92834
www.transunion.com/
Automated Fraud Alert-
1.800.680.7289
Order Credit Report-1.800.680.7289

Experian
P.O. Box 9532
Allen, TX 75013
www.experian.com
Automated Fraud Alert-
1.888.397.3742
Order Credit Report-1.888.397.3742

You should also know that the Federal Trade Commission (FTC) offers consumer assistance and educational materials relating to identity theft and privacy issues. The FTC can be contacted by either visiting www.consumer.gov/idtheft or by calling (877) 438-4338.

Data Breach FAQs

Q: Is this a major breach?

A: No, our credit card security manager classifies this as minor

Q: Did this affect any transactions in S&K stores?

A: No, just S&K's online eStore – www.skmenwear.com

Q: What information was compromised?

A: Name, Address, credit card number and order information. We want to stress that no social security number, CVV2 data or track 2 magnetic stripe data was compromised at all.

Q: I recently noticed fraud on my account. Is this fraud related to the recent incident?

A: If you identify fraud on your account, please contact the financial institution that issued your card right away to report the incident.

Q: Does this incident impact Visa, MasterCard, American Express and Discover?

A: Yes. All card brands are impacted.

Q: What are the chances that I become a victim of identity theft as a result of this incident?

A: It is important to know that Social Security numbers were not stolen, so we believe that the risk of identity theft is reduced. In fact, fraud rarely occurs on accounts compromised during a data breach. However, it's always a good idea to check your credit report regularly for incorrect information. See the "what to do if you suspect identity theft" section below.

Q: What can I do to ensure I am not a victim of fraud?

A: While we employ the latest systems and technology to monitor and prevent card fraud, and many merchants also take the necessary precautions to protect your card information, there are some practical steps you can take to help protect yourself.

- Check your account statement promptly and immediately report any transactions that you don't recognize.
- Destroy all receipts before discarding them since some of them may have your card number printed on it.
- Guard your card — don't use it as collateral or give out your card number to someone on the phone, unless you initiated the call for a purchase.
- Check your credit report at least annually to ensure its accuracy.

Q: Are there any other tips you can provide to reduce my chances of card fraud?
A: Yes. There are several actions you can take to protect your personal information.

DO...

- Shred all personal and financial information — such as bills, bank statements, ATM receipts and credit card offers — before you throw it away.
- Keep your personal documentation (e.g., birth certificate, Social Security card etc.) and your bank and credit card records in a secure place.
- Call the post office immediately if you are not receiving your mail. To get the personal information needed to use your identity, a thief can forge your signature and have your mail forwarded.
- Be aware of your surroundings when entering your Personal Identification Number (PIN) at an ATM.
- Limit the number of credit cards and other personal information that you carry in our wallet or purse.
- Report lost or stolen credit cards immediately.
- Review and consider whether you need currently inactive card accounts. Even when not being used, these accounts appear on your credit report, which is accessible to thieves. If you have applied for a credit card and have not received the card in a timely manner, immediately notify the appropriate financial institution.
- Closely monitor the expiration dates on your credit cards. Contact the credit issuer if the replacement card is not received prior to your credit card's expiration date.
- Sign all new credit cards upon receipt.
- Review your credit reports annually.
- Use passwords on your credit cards, bank accounts and phone cards. Avoid using the obvious passwords — your mother's maiden name, your birth date or the last four digits of your Social Security or phone number.
- Match your credit card receipts against monthly bills to make sure there are no unauthorized charges.

DON'T ...

- Volunteer any personal information when you use your credit card.
- Give your Social Security number, credit card number or any bank account details over the phone unless you have initiated the call and know that the business that you are dealing with is reputable.
- Leave receipts at ATMs, bank counters or unattended gasoline pumps.
- Leave envelopes containing your credit card payments or checks in your home mailbox for postal carrier pickup.
- Record your Social Security number or passwords on paper and store them in your wallet or purse. Memorize your numbers and/or passwords.
- Disclose bank account numbers, credit card account numbers or other personal financial data on any Web site or online service location, unless you receive a secured authentication key from your provider.