

**North Carolina Security Breach Reporting Form  
Pursuant to the Identity Theft Protection Act of 2005**

Name of Business Owning or Licensing Information Affected by the Breach: Cole National Group, Inc.  
Address: 4000 Luxottica Place  
Mason, Ohio 45040  
Telephone: (513) 765-4483  
Fax: (513) 492-4483  
Email: ascholl@luxotticaretail.com

**PLEASE SUBMIT FORM TO:**  
Consumer Protection Division  
NC Attorney General's Office  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
Telephone: (919) 716-6000  
Toll Free in NC: (877) 566-7226  
FAX: (919) 716-6050

Date Security Breach Reporting Form submitted: December 12, 2008 (notification sent to Attorney General's office on October 10, 2008)  
Date the Security Breach was discovered: Unauthorized access confirmed on September 11, 2008.  
Estimated number of affected individuals: 59,511  
Estimated number of NC residents affected: 1,477

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b)): Cole National Group, Inc.

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: See attached.

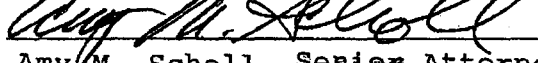
Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. \_\_\_\_\_ If so, please describe the security measures protecting the information: See attached.

Describe any measures taken to prevent a similar Security Breach from occurring in the future: See attached.

Date affected NC residents were/will be notified: Notice to NC residents mailed on October 14, 2008  
If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (c): Not applicable.

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the written request or the contemporaneous memorandum. Not applicable.

How NC residents were/will be notified?  written notice  
(pursuant to N.C.G.S. § 75-65(e))  electronic notice (email)  
Please attach copy of the notice if in written form or a copy of  telephone notice  
any scripted notice if in telephonic form.  substitute notice

Signature:  Date: December 12, 2008  
Contact Person, Title: Amy M. Scholl, Senior Attorney  
Address: \_\_\_\_\_  
(if different from above) \_\_\_\_\_  
Telephone: \_\_\_\_\_ Fax: \_\_\_\_\_ Email: \_\_\_\_\_

**Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format:**

An unknown, unauthorized person accessed an electronic file that was located on a company file transfer protocol ("FTP") server. The file contained payroll information for employees of Things Remembered, Inc. from 1998 through early 2005.

**Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner.**

This breach was an isolated incident that occurred due to the incorrect configuration of an externally-facing FTP server that was integrated into the company's infrastructure as a result of a corporate acquisition, without the realization that it was improperly configured. The server was inadvertently configured to permit "anonymous" login access, meaning that the server could be accessed without proper credentials. The data itself was not password protected or encrypted. This error does not comport with Cole's security policies and practices, and we have taken steps to ensure that an incident such as this does not occur again.

**If so, please describe the security measures protecting the information:**

Please see above answer.

**Describe any measures taken to prevent a similar Security Breach from occurring in the future:**

Cole's IT Security team turned off anonymous FTP login capability for the server, thereby restricting access to the file at issue. Cole has a dedicated IT security team that employs a variety of administrative, physical and technical safeguards to protect individuals' personal information. For example, servers with sensitive data reside in protected network segments with access limited to authorized individuals. Logs from firewalls, an intrusion prevention system and other security infrastructure protection devices are kept on an RSA Envision Security Logging, Auditing and Monitoring System, with access controlled exclusively by the security team. Information contained in Cole's email post offices is encrypted until being sent to a destination outside of the organization. Messages intended for external recipients must pass through a gateway, and are then analyzed by an e-mail encryption service, and finally must pass through an anti-spam and anti-malware appliance before being related through Cole's firewalls to the internet. Cole regularly scans all internal and external servers and networks for vulnerabilities.

**COLE NATIONAL GROUP, INC.**  
**4000 Luxottica Place**  
**Mason, Ohio 45040**

Direct Dial: 513 765-4483

OCT 23 2008

October 10, 2008

Office of the Attorney General  
9001 Mail Service Center  
Raleigh, North Carolina 27699-9001

Ladies and Gentlemen:

The purpose of this letter is to notify you of an incident involving unauthorized access to personal information of residents of North Carolina. We recently discovered that an unknown, unauthorized person accessed a file on a company server in April 2008. This file contained payroll information for Things Remembered, Inc. employees from 1998 through March 2005. The information included names, addresses, Social Security Numbers, dates of birth, and other information used for processing payroll. Based on the information in the file that was accessed, as well as address verification performed this week, we believe approximately 1,477 of the affected individuals currently reside in North Carolina.

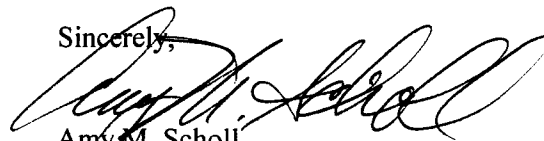
We have reported the incident to the appropriate law enforcement agencies, and are cooperating with their ongoing investigation. At this time, we have no evidence that the compromised data has been misused. We have carefully reviewed the security of the server on which this file was located, and believe this was an isolated and unusual incident.

During the week of October 13, 2008, we plan to send notices by mail to all affected individuals; a sample copy of this notice is enclosed. The notice suggests steps that the individuals can take to help protect themselves from identity theft. Among other things, these notices contain the telephone numbers and websites of each of the three national consumer reporting agencies, and inform the individuals of their ability to contact any one of the agencies to obtain a copy of their credit reports or request that fraud alerts be placed on their credit files. We are also notifying the three national consumer reporting agencies of this incident and the number of affected individuals.

We are also offering each individual a complimentary 12-month membership for Triple Alert<sup>SM</sup>, a credit monitoring product offered by ConsumerInfo.com, Inc., an Experian<sup>®</sup> company.

If you need any further information, please contact me at 513-765-4483.

Sincerely,



Amy M. Scholl  
Sr. Attorney  
Cole National Group, Inc.

Enclosure

**COLE NATIONAL GROUP, INC.**  
**4000 Luxottica Place**  
**Mason, Ohio 45040**

October 14, 2008



T1 P1 \*\*\*\*\*AUTO\*\*5-DIGIT 44515 1

Dear [REDACTED]

Cole National Group, Inc. (a Luxottica Group Company) is contacting you because you were an employee of the Things Remembered brand at some point between 1998 and March 2005. We recently discovered that an unknown, unauthorized person accessed a file from a company server in April 2008. This file contained information used for processing payroll for Things Remembered employees during the time span noted above.

At this time, we have no evidence that the compromised data has been misused. We have carefully reviewed the security of the server on which this file was located, and believe this was an isolated and unusual incident.

Nonetheless, we want to provide you with details to detect and prevent misuse of your personal information. Your name, address, Social Security Number, date of birth and other information used for processing payroll were included in the file that was accessed.

We deeply regret that this has occurred and have taken action to ensure the security of this file going forward and to lessen the potential for harm. We have notified law enforcement of this incident, are conducting a full investigation, and will support prosecution of those involved.

We have also engaged ConsumerInfo.com, Inc., an Experian® company, to provide you with one full year of credit monitoring, at no cost to you. This credit monitoring product, known as Triple Alert<sup>SM</sup>, will identify and notify you of key changes that are detected on any of your credit reports from the three credit reporting companies: Experian, Equifax® and TransUnion®. This credit monitoring product is a powerful tool that you can use to help you identify possible fraudulent use of your information.

Your complimentary 12-month **Triple Alert<sup>SM</sup>** membership includes:

- Daily monitoring of your three credit reports from Experian, Equifax® and TransUnion®
- Email alerts if key changes are detected on any of your three credit reports
- Monthly "No Hit" alerts, if applicable
- Toll-free access to a dedicated team of Fraud Resolution Representatives if you should detect any fraudulent activity or become a victim of identity fraud
- \$25,000 in identity theft insurance provided by Virginia Surety Company, Inc. with no deductible\*

\*Please note that due to New York state law restrictions, identity theft insurance coverage cannot be offered to individuals who are residents of New York, nor is coverage available in U.S. overseas Commonwealths or Territories outside the continental U.S. (i.e., Puerto Rico, Guam, etc.).

You have ninety (90) days from the date of this letter to activate this membership, which will then continue for 12 full months. We encourage you to activate your credit monitoring membership as soon as possible.

To sign up, please visit <http://partner.consumerinfo.com/info1> and enter your individual activation code provided below. Please keep in mind that once activated, the code cannot be re-used. You will be instructed on how to enroll in your complimentary credit monitoring product. All credit alerts will be accessible online. If you need technical assistance, please call 1-866-252-0121.

Your Single Use Credit Monitoring Activation Code: XXXXXXXXXX

We have also advised the three major U.S. credit reporting companies about this incident. We have given them a general report, alerting them to the fact that the incident occurred. However, we have not notified them that your specific information was in the file breached.

We encourage you to take preventative measures now to help prevent and detect any misuse of your information. It is very important that you remain vigilant in protecting your identity by reviewing account statements and monitoring your free credit reports. To obtain a free copy of your credit report, you may visit <http://www.annualcreditreport.com> online, or call toll free 877-322-8228. Hearing impaired consumers can access TDD service at 877-730-4104.

We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit reporting companies. As soon as one credit reporting company confirms your fraud alert, the others are notified to place fraud alerts on your credit file. All three credit reports will be sent to you, free of charge, for your review.

Equifax	Experian	TransUnion Corp
800-685-1111	888-397-3742	800-680-7289
<a href="http://www.equifax.com">www.equifax.com</a>	<a href="http://www.experian.com">www.experian.com</a>	<a href="http://www.transunion.com">www.transunion.com</a>

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission ("FTC") recommends that you check your credit reports periodically. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts.

If you believe your information is being misused, you also should file a complaint with the FTC at <http://www.ftc.gov/idtheft> or at 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

Finally, we also recommend you visit the FTC website which provides a comprehensive guide to help you with security of your personal information and guard against its misuse by others at <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idtheft4.shtm>.

Again, we sincerely apologize that this incident has occurred. The action steps we are taking, and suggest you consider taking, are preventative. If you have any questions about this incident, please call us at 1-866-285-7669 (Monday through Friday, 8:00 a.m. - 5:00 p.m. ET).

Sincerely,

Cole National Group, Inc.