MUJI
無印良品

November 30, 2015

To Whom It May Concern:

We received information suggesting that we may have experienced a data compromise. Immediately, we closed our online web shop in order to protect our customers. At the same time as the closure, we immediately hired cybersecurity specialists to investigate the incident and provide a thorough report. The results of such investigation are now complete, enabling us to relay this information to you at this time. Below we explain in further detail the results of our investigation.

Based on the outcome of our recently completed investigation, we have determined that an unauthorized third party used malicious software (malware) to infiltrate our on-line server, which is hosted by a reputable service provider. We learned of the incident as the result of a thorough investigation, which we initiated immediately following the receipt of information suggesting a possible data compromise on our on-line shopping site. To adequately protect our customers, we shut down our on-line shopping site during the course of the investigation. Our investigation was recently completed, and we are now able to determine the scope of customers whose information was potentially exposed during the incident.

As a result of this incident, some information linked to credit cards may have been acquired by unauthorized third parties. This information may include information such as a customer's name, address, payment card account number, the expiration date of the card, and the CCV/CVV number listed on its back. We do not collect other personal information about our customers, such as Social Security number, personal identification number (PIN), driver's license number, or financial account information, and as a result, none of this type of personal information has been affected by this incident.

At this stage of the specialists' investigation, we believe the following facts to be true:

- Order information that was provided by customers during the period of January 22, 2015 – July 20, 2015 may have been at risk. Though we do not have the exact figures, we believe that approximately 664 residents of your state or commonwealth may have been impacted by this incident.

- We have discovered the malware used to capture personal information and have eliminated it. Further, we have increased our security by taking measures.

As required by law, we will send a notification to individuals affected by this incident. The notices will mirror the sample notice attached here and will include the same or similar content. Such notification will be mailed to the affected customers on or about November 27, 2015.

To further remedy the harm caused by this unexpected incident, we are offering each potentially impacted individual free access to ProtectMyID Elite, an identity protection product provided by Experian, a leading national credit bureau. Full details of this program are provided on page 2 of the attached sample notification.

If you have any questions about this situation, please contact me at the address and telephone number listed below.

Sincerely,

Asako Shimazaki

Asako Shimazaki
President
250 West 39th Street, Suite 605
New York, NY 10018
Tel: 646.366.0515
simazaki@muji.co.jp

MUJI
無印良品

November 16, 2015

NOTICE OF POTENTIAL DATA BREACH

Dear Valued Customer,

Here at MUJI U.S.A. LIMITED, we take the security of our customers' information seriously. Unfortunately, like many companies in today's global online economy, we received information suggesting that we may have experienced a data compromise. Immediately, we closed our online web shop in order to protect our customers. We regret that we might have caused any inconvenience for you due to the closure of our online shopping site. At the same time as the closure, we immediately hired cybersecurity specialists to investigate the incident and provide a thorough report. The results of such investigation are now complete, enabling us to relay this information to you at this time. Below we explain in further detail the results of our investigation.

What Happened?
Based on the outcome of our recently completed investigation, we have determined that an unauthorized third party used malicious software (malware) to infiltrate our on-line server, which is hosted by a reputable service provider. We learned of the incident as the result of a thorough investigation, which we initiated immediately following the receipt of information suggesting a possible data compromise on our on-line shopping site. To adequately protect our customers, we shut down our on-line shopping site during the course of the investigation. Our investigation was recently completed, and we are now able to determine the scope of customers whose information was potentially exposed during the incident. At this time, we believe order information that you and other customers provided during the period of January 22, 2015 – July 20, 2015 may have been at risk.

What Information Was Involved?
As a result of this incident, some information linked to credit cards may have been acquired by unauthorized third parties. This information may include information such as your name, address, payment card number, the expiration date of the card, and the CCV/CVV number listed on its back. Even if your credit card information was compromised, it does not automatically mean you are a victim of fraud. If you suspect that your credit card was used fraudulently, promptly notify the credit card company.

We do not collect other personal information about our customers, such as Social Security number, personal identification number (PIN), driver's license number, or financial account information, and as a result, none of this type of personal information has been affected by this incident.

What We Are Doing.
We deeply regret that this unexpected event occurred and we would like you to know a few important things:

- When the website reopens, it will be safe to shop at muji.com. The malware used to capture personal information has been eliminated and we have increased our security measures.
- As noted above, we do not collect any PIN information. As a result, even if someone gained access to your card information, without your PIN they cannot visit an ATM with a fraudulent debit card and withdraw cash.
- Out of an abundance of caution and at no cost to you, we are offering you free access to ProtectMyID Elite, an identity protection product provided by Experian, a leading national credit bureau. Full details of this program are provided on page 2. In addition on page 2, titled **What You Can Do,** you will also find a detailed list of strategies on how best to protect your credit card information in today's digital economy.

For More Information.
If you have any questions about this situation, our Customer Service team is available toll-free at 1-844-866-0515 from 9 am - 6 pm Eastern Time, Monday - Friday.

I would like to sincerely apologize for this incident, and I regret any inconvenience it may have caused you. I want to assure you that we take this incident very seriously and continue to address it thoroughly.

Thank you for your continued confidence and support.

Asako Shimazaki

Asako Shimazaki
President

What You Can Do:
Steps To Protect the Security of Your Personal Information

By taking the following steps, you can help reduce the risk that your personal information may be misused.

1. Enroll in ProtectMyID Elite, the product that we are providing at no cost to you. You must personally activate the identity protection product for it to be effective. If you wish to enroll in ProtectMyID Elite, please do the following:

- **VISIT** The ProtectMyID Elite Web Site: http://www.protectmyid.com/protect or call 877-297-7780 to enroll
- **PROVIDE** Your Activation Code: «CODE» Enrollment Deadline: February 29, 2016

If you prefer to enroll over the phone for delivery of your membership via US mail, please call Experian at 877-297-7780 and provide Engagement #: PC97515. Enrolling in ProtectMyID Elite will not affect your credit score.

Experian's ProtectMyID Elite product will provide the following:

- **Credit Report**: A free copy of your Experian credit report.
- **Daily Credit Monitoring**: Alerts you of suspicious activity including new inquiries, newly opened accounts, delinquencies, or medical collections.
- **Identity Theft Resolution**: If you have been a victim of identity theft, you will be assigned a dedicated, U.S.- based Experian Identity Theft Resolution Agent who will walk you through the fraud resolution process.
- **$1 Million Identity Theft Insurance**: As a ProtectMyID Elite member, you are immediately covered by a $1 Million insurance policy that may help you cover certain costs, such as lost wages, private investigator fees, and unauthorized electronic fund transfers.

2. Review your credit reports. You can receive free credit reports by placing a fraud alert (described below). Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three national credit bureaus. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report from one of the three credit bureaus every four months.

3. Review your account statements. You should carefully review for suspicious activity the statements that you receive from credit card companies, banks, utilities, and other service providers.

4. Remain vigilant and respond to suspicious activity. If you receive an e-mail or mail alert from Experian, contact a ProtectMyID Elite fraud resolution representative *Toll-Free* at 877-297-7780 or http://www.protectmyid.com/protect. If you notice suspicious activity on an account statement, report it to your credit card company or service provider and consider closing the account. You also should consider reporting such activity to your local police department, your state's attorney general, and the Federal Trade Commission.

5. Consider placing a fraud alert or a security freeze with one of the three national credit bureaus. You can place an initial fraud alert by contacting one of the three national credit bureaus listed below. For 90 days, an initial fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you but also may delay you when you seek to obtain credit. If you decide to enroll in ProtectMyID Elite, you should place the fraud alert after enrolling. Contact information for all three bureaus is:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

In addition, you can visit the credit bureau links below to learn more about placing a security freeze on your credit report which would prohibit a credit bureau from releasing information from your credit report without prior authorization from you.

- Equifax security freeze: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
- Experian security freeze: http://www.experian.com/consumer/security_freeze.html
- TransUnion security freeze: http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page

6. Special notice to Massachusetts residents. Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. As mentioned above, a security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services.

Security freezes may cost up to $5.00 to place, temporarily lift, or permanently remove. However, if you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, a credit reporting agency cannot charge you to place, lift or remove a security freeze. To effectively place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies listed above.

In order to request a security freeze, you will need to provide the following information:

- Your full name;
- Social Security number;
- Date of birth;
- The addresses where you have lived over the prior five (5) years provided that you have moved during that time;
- Proof of current address (*e.g.*, mail received in your name);
- A legible photocopy of a government issued identification card (*e.g.*, state driver's license or ID card or military identification);
- If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
- If you are not a victim of identity theft, payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only).

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

7. Additional Information. You can obtain additional information about steps you can take to avoid identity theft from the following:

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
http://www.ftc.gov/bcp/edu/microsites/idtheft/
(877) IDTHEFT (438-4338)
TDD: (866) 653-4261

For Maryland and North Carolina Residents, further information is available at the following:

Maryland:
Office of the Attorney General
Consumer Protection Division
Maryland Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
http://www.oag.state.md.us/idtheft/index.htm
1-410-528-8662

North Carolina:
North Carolina Office of the Attorney General
9001 Mail Service Center
Raleigh, NC 27699-9001
1-919-716-6400
http://www.ncdoj.gov/Crime.asp