Fix My Blinds
615 Conrad St.
Colorado Springs, CO 80915

[Customer Address] [date]

Re: Notice of Data Loss (Card ending in xxxx)

Dear Customer,

FIX MY BLINDS is writing to inform you of a data security incident that may impact the privacy of certain credit card payment information that may have occurred while you were on the website. This notification provides you with information about the incident, the response, and steps you may wish to take to better protect against the possibility of identity theft and fraud. As a small business focused on serving the needs of our customers, we sincerely apologize for any issues this incident may cause for you.

What Happened:
On or about May 23, 2019, FIX MY BLINDS received the initial notification from a payment processor that there were indications of a possible compromise of credit card or debit card information that had been used on the FIX MY BLINDS site. FIX MY BLINDS immediately contacted its partners responsible for maintaining the site, its security, and other partners involved with the payment processing platform. A third-party cybersecurity firm, and also an incident response team, were retained to investigate the matter. Despite an extensive investigation by the retained experts and ongoing coordination among different entities potentially in possession of information useful for determining the root cause for the incident, the hired forensics team was unable to conclusively determine that customer credit card information was removed from the FIX MY BLINDS' payment processing platform. Even though available evidence does not definitively establish a singular cause attributable to FIX MY BLINDS for the loss of credit card information, FIX MY BLINDS determined on August 14, 2019, that there was a duty to notify you concerning the loss of personal information associated with your visit to the FIX MY BLINDS site.

Additionally, FIX MY BLINDS is also notifying you that as a result of research and investigative efforts, there are indications that the FIX MY BLINDS site became caught up in an Internet ecosystem attack in which third-party computer code that is transient and existent to render the Internet and websites more functional and responsive to users may have caused an infection of the web browser on your computer which also could have caused the loss of certain private information.

Although FIX MY BLINDS believes it will not ever be able to confirm that personal information was in fact acquired by an unauthorized entity, the possibility cannot be ruled out that the incident or incidents may have compromised card information, as well as usernames and passwords for customers who have created profiles on the FIX MY BLINDS site.

FIX MY BLINDS continues to investigate this matter and is coordinating with the appropriate entities and authorities. However, this notification has not been delayed nor have any delays to our handling of this matter occurred as a result of coordination with law enforcement.

What Information Was Involved:
The following personal information may have been involved in the incident or incidents: (i) cardholder name, (ii) account number, (iii) expiration date, (iv) cardholder address, and (v) security code from payment cards used on the FIX MY BLINDS online site. The period covered by this notification (i.e., window of card usage dates on the FIX MY BLINDS site):

March 14, 2019 – June 12, 2019 (for the card number indicated above)

For users who have established a customer profile on the FIX MY BLINDS site, the following personal information may have been involved in the incident or incidents: (i) name, (ii) address, (iii) username and password, (iv) credit card information. Username, password and credit card information are encrypted on the third-party platform used by FIX MY BLINDS, but it cannot be determined by FIX MY BLINDS whether the third-party's security controls would have prevented the loss of this personal information.

What We Are Doing:

FIX MY BLINDS deactivated all credit card processing during the investigation as soon as the forensics team determined that attack vectors presented potential risk to credit card transactions. FIX MY BLINDS followed the advice of the incident response team throughout the forensics investigation and proceeded to mitigate the vulnerabilities and potential attack vectors identified by the team.

FIX MY BLINDS completely overhauled its payment processing platform and established new third-party relationships that offer more secure methods for processing credit card information.

FIX MY BLINDS also retained new cybersecurity consulting assistance and restored full compliance with Payment Card Industry (PCI) regulations (note that FIX MY BLINDS has historically received passing grades for compliance from security scans conducted pursuant to PCI security controls).

FIX MY BLINDS purchased encryption devices for use by staff having access to sensitive information and plans to institute improved data privacy protections across the company.

What You Can Do:

FIX MY BLINDS recommends that passwords be changed for users with a profile on the site. You should also monitor your credit card and bank statements and dispute any transactions that appear fraudulent. You should also report your credit card as compromised and obtain a new credit card.

You should use security software and run scans on your computer. Many computers and smartphones have security software installed, and both free and subscription-based programs are available for download from the Internet.

You can also find out more about rights, resources, and how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Better Protect Your Information.*

If you have additional questions about this notification of the incident(s), you may contact:

FMB Inquiries Service
inquiry@fmbinquiries.com
800-326-5022

More Information:

Once alerted about a loss of privacy, it is generally recommended to remain vigilant about monitoring financial and credit card statements, credit score and credit reports, and to be vigilant concerning potential identity theft. Suspected incidents of identity theft or fraud may be reported to local law enforcement or the state attorney general. You are generally entitled to a copy of a police report, once reported.

Additional useful resources and services to educate yourself and request assistance include:

- The Consumer Financial Protection Bureau – http://www.consumerfinance.gov/askcfpb/1243/what-identity-theft.html

- Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261

- Internet Crime Complaint Center (IC3), Federal Bureau of Investigation, https://www.ic3.gov/default.aspx

- Your state attorney general office may have additional resources or provide assistance.

- Commercial credit monitoring services are available and generally require a paid subscription. Your bank may also monitor your account and your credit card, and often there is no cost for this service for a limited time. Check with your bank or card issuer.

STEPS YOU CAN TAKE TO BETTER PROTECT YOUR INFORMATION

FIX MY BLINDS encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit http://www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/creditfreeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

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

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-680-7289
www.transunion.com/fraudvictim-resource/place-fraudalert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Although FIX MY BLINDS has no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim.

Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.
For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.
For New Mexico and New Jersey residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting
www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.
For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.