MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

James E. Prendergast
Office: 267-930-4798
Fax: 267-930-4771
Email: jprendergast@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

March 4, 2019

***INTENDED FOR ADDRESSEE(S) ONLY***
***VIA U.S. 1ST-CLASS MAIL***

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

**Re: Notice of Data Event**

Dear Attorney General MacDonald:

Our office represents TEMPTU, Inc. ("TEMPTU") located at 26 W 17th St Rm 302, New York, NY 10011-5730. We write to notify you of an event that may affect the security of personal information relating to four (4) New Hampshire residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, TEMPTU does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

**Background**

On December 18, 2018, TEMPTU was notified by Bank of America Merchant Services that credit cards used on its website were subject to unauthorized access. TEMPTU immediately launched an internal investigation into this issue and removed all malware found on the website within twenty-four (24) hours. TEMPTU also engaged an independent third-party investigator to conduct a forensic investigation. Through the investigation, TEMPTU determined that any credit cards used on its website from November 1, 2018 to November 21, 2018 may have been subject to unauthorized access. Accordingly, TEMPTU reviewed all of the credit card transactions during the period of compromise. On January 7, 2018, TEMPTU determined the following type of information related to four (4) New Hampshire residents included the individuals name and credit cards number.

**Notice to New Hampshire Residents**

On March 4, 2019, TEMPTU mailed written notice of this incident to all potentially impacted individuals. Written notice will be provided in substantially the same form as the letter attached here as ***Exhibit A.***

**Other Steps Taken and To Be Taken**

TEMPTU is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state attorney general, and law enforcement to report attempted or actual identity theft and fraud. TEMPTU is working to implement additional safeguards and employee training in response to this incident. In addition to providing this notice to your office, TEMPTU is providing notice to other state regulators, as required.

**Contact Information**

Should you have any questions regarding this notification or other aspects of this event, please contact me at (267) 930-4798.

Very truly yours,

James E. Prendergast of
MULLEN COUGHLIN LLC

JEP:cds
Enclosure

# EXHIBIT A

# TEMPTU

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

RE: Notice of Data Breach

Dear <<Name 1>>:

TEMPTU, Inc. ("TEMPTU") is writing to notify you of a recent data security incident that may impact the security of your personal information. TEMPTU writes to advise you of our investigation and the steps we are taking in response to this incident as well as steps you can take to protect your personal information should you feel it is appropriate to do so.

***What Happened?*** On December 18, 2018, TEMPTU was notified by Bank of America Merchant Services that credit cards used on its website were subject to unauthorized access. TEMPTU immediately launched an internal investigation into this issue and removed all malware found on the website within twenty-four (24) hours. TEMPTU also engaged an independent third-party investigator to conduct a forensic investigation. Through the investigation, TEMPTU determined that any credit cards used on its website from November 1, 2018 to November 21, 2018 may have been subject to unauthorized access. Accordingly, TEMPTU reviewed all of the credit card transactions during the period of compromise and determined that credit card information related to you may have been at risk.

***What Information Was Involved?*** The information related to you that was potentially subject to unauthorized access includes your name and credit card number.

***What We Are Doing.*** We take the security of personal information in our care very seriously. We have security measures in place to protect the data on our systems and we are working to implement additional safeguards.

***What You Can Do.*** You can review the enclosed "Steps You Can Take to Protect Against Identity Theft and Fraud." In addition, we advise you to report suspected incidents of identity theft to local law enforcement or the Attorney General.

***For More Information.*** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance please call the TEMPTU team at 855-983-4433.

We sincerely apologize for this incident and regret any concern or inconvenience this has caused you.

Sincerely,

*Greg Mandor*

Greg Mandor
Chief Financial & Operating Officer
TEMPTU, Inc.

## Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage 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 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** | **TransUnion** | **Equifax** |
|---|---|---|
| PO Box 9554 | P.O. Box 2000 | PO Box 105788 |
| Allen, TX 75013 | Chester, PA 19016 | Atlanta, GA 30348-5788 |
| 1-888-397-3742 | 1-888-909-8872 | 1-800-685-1111 |
| www.experian.com/freeze/center.html | www.transunion.com/credit-freeze | www.equifax.com/personal/credit-report-services |

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** | **TransUnion** | **Equifax** |
|---|---|---|
| P.O. Box 2002 | P.O. Box 2000 | P.O. Box 105069 |
| Allen, TX 75013 | Chester, PA 19106 | Atlanta, GA 30348 |
| 1-888-397-3742 | 1-800-680-7289 | 1-888-766-0008 |
| www.experian.com/fraud/center.html | www.transunion.com/fraud-victim-resource/place-fraud-alert | www.equifax.com/personal/credit-report-services |

Although we have 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. This notice has not been delayed by law enforcement.

**For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. **For New Mexico 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 North Carolina residents**, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. **For Rhode Island residents**, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of 5 Rhode Island residents may be impacted by this incident.