July 5, 2018

VIA U.S. MAIL
New Hampshire Department of Justice
Gordon J. MacDonald, Attorney General
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Security Incident Notification

Dear Attorney General MacDonald:

I am writing on behalf of the Village of Wellington (the "Village"), located in Florida, to notify you pursuant to N.H. Rev. Stat. § 359-C:20(I)(b), that an unknown third-party was able to gain unauthorized access to one-time payments made through the Click2Gov online-payment system used by the Village to collect payments for utilities, building permits, business licenses, and parking tickets. Personal information affected by the incident includes payment card information (card number, security code, and expiration date), first and last name, middle initial, address, city, state, and zip code. The date range of the incident is November 28, 2017, to June 4, 2018, for utilities payments and March 15, 2018, to June 4, 2018 for building permits, business licenses, and parking tickets.

In response, the Village undertook an independent third-party investigation and implemented additional security measures designed to prevent the recurrence of such an attack. The Village has been in communication with the Florida Office of the Attorney General over the last two weeks about the subject incident. Additionally, the Village reported the incident to the Palm Beach Sheriff's Office.

Approximately one (1) New Hampshire resident was likely affected by the security incident. Notice will be sent to the affected individual by mail (where a mailing address is available) on July 6, 2018, and by substitute notice on July 6, 2018.

A sample of the notification letter to the affected individual is enclosed. Please contact me if you need any additional information regarding this incident.

Very truly yours,

Lauri Cohen
Village Attorney

12300 Forest Hill Boulevard • Wellington, Florida 33414 • (561) 791-4000 • Fax (561) 791-4045
www.wellingtonfl.gov

THE VILLAGE OF WELLINGTON
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>>

Dear <<Name 1>>:

We are writing to let you know about an incident that may have exposed your personal information to unauthorized persons. It recently came to our attention that between November 28, 2017, and June 4, 2018, an unknown third-party was able to gain access to payments made through the Click2Gov online-payment system we use for utilities payments. Personal information affected by the incident includes payment card information (card number, security code, and expiration date), first and last name, middle initial, address, city, state, and ZIP code. Only one-time payments were affected, whether made by manually entering your information at the time of payment or by using information stored in your Wallet to make the one-time payment.

Our records indicate that you may have used the Click2Gov online-payment system to make a one-time utilities payment during the time noted above.

The Village of Wellington values your privacy and deeply regrets that this incident occurred. We have implemented additional security measures designed to prevent a recurrence of such an attack, and to protect your privacy. We also notified the Palm Beach Sheriff's Office of the incident and are working closely with law enforcement to ensure the incident is properly addressed.

Please also consider the following steps you can take to protect your information:

- **Remain vigilant** – We encourage you to remain vigilant by reviewing your account statements and free credit reports.
    - If you discover errors or suspicious activity on your credit card account, you should immediately contact the credit card company and inform them that you have received this letter. Confirm the address they have on file for you is your current address, and that all charges on the account are legitimate.
    - To obtain an annual free copy of your credit reports, visit www.annualcreditreport.com or call 1-877-322-8228. Review your credit reports carefully for inquiries from companies you did not contact, accounts you did not open, or debts on your accounts that you do not recognize. Also make sure to verify the accuracy of your Social Security number, address(es), complete name, and employer(s) information. If information on a report is incorrect, notify the credit bureau directly using the telephone number on the report. Additional contact information for the major credit bureaus is as follows:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
1-866-349-5191	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

- **Consider placing a fraud alert or security freeze on your credit file** – Credit bureaus have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag, which is placed on your credit file to notify lenders and others that they should take special precautions to ensure your identity before extending credit. Although this may cause some short delay if you are the one applying for credit, it might protect against someone else obtaining credit in your name. Call any one of the three credit-reporting agencies at the numbers below to place fraud alerts with all three of the agencies.

Equifax	**Experian**	**TransUnion**
1-866-349-5191	1-888-397-3742	1-800-916-8800

- A security freeze is a more dramatic step that will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a security freeze in place, even you will need to take special steps when applying for credit. A security freeze may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. A security freeze will need to be obtained separately from each credit-reporting agency. You must contact each credit agency separately to order a security freeze. You can obtain more information by visiting the credit bureaus at the following addresses.

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

- If you request a security freeze from a credit-reporting agency there may be a fee of up to $10 to place, lift, or remove the security freeze. In order to place a security freeze, you may be required to provide the credit-reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement.

- **Report suspicious activity** – If you believe you are the victim of fraud or identity theft, file a police report and get a copy of the report to submit to your creditors and others that may require proof of a crime to clear up your records. The report may also provide you with access to services that are free to identity-theft victims. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to your state attorney general and/or the Federal Trade Commission. To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Additional Free Resources on Identity Theft** – You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft: A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

* * *

Protecting the privacy of your personal information is important to us, and we regret any inconvenience this incident may cause you. Should you have any questions or concerns about the incident or the personal information we maintained, please call our customer care center toll free Monday through Friday from 9 am to 9 pm Eastern Time, at 800-931-4009 and one of our representatives will be happy to assist you.

Sincerely,

Paul Schofield
Wellington Village Manager