POLSINELLI

150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

March 13, 2019

Bruce A. Radke

312-463-6211
312-819-1910
bradke@polsinelli.com

**VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)**
**AND FEDERAL EXPRESS**

The Honorable Gordon MacDonald
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

***Re: Notification of a Data Security Incident***

Dear Attorney General MacDonald:

We represent Grow Financial Federal Credit Union ("Grow Financial") in connection with an incident that involved the personal information of one (1) New Hampshire resident and provide this notice on behalf of Grow Financial pursuant to N.H. REV. STAT. ANN. § 359-C:20.

This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While Grow Financial is notifying you of this incident, Grow Financial does not waive any rights or defenses relating to the incident or this notice, or the applicability of New Hampshire law on personal jurisdiction.

## NATURE OF THE INCIDENT

Grow Financial recently discovered that skimming devices may have been placed on the ATMs at the credit union's Clearwater branch located at 2474 State Road 580, Clearwater, FL 33761 from December 30, 2018 to January 5, 2019 and from January 7, 2019 to January 10, 2019. The skimming device is believed to have acquired the following personal information stored on the affected debit card of the affected New Hampshire resident: name, card number, expiration date and personal identification number (PIN).

POLSINELLI



## NOTIFICATION TO THE ONE (1) NEW HAMPSHIRE RESIDENT

Grow Financial determined that one (1) New Hampshire resident may have been impacted by this incident. Grow Financial will be notifying the impacted individual of the incident by letter on March 13, 2019. Enclosed is a copy of the notice that is being sent to the impacted New Hampshire resident.

## STEPS TAKEN RELATING TO THE INCIDENT

Upon discovery of the situation, Grow Financial and its ATM servicer confirmed the removal of the skimming device from the ATMs and promptly alerted local law enforcement. Grow Financial has already begun taking measures to help prevent this type of incident from occurring in the future, including working with its ATM manufacturer to further secure its ATMs. Grow Financial is monitoring the accounts of potentially affected members and is issuing new cards to those members who have been impacted by this incident. Members who experience losses due to fraudulent transactions as a result of this incident will have their funds fully restored.

## CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

Bruce A. Radke

Enclosure

cc: Dierdre K. White, Chief Legal Officer, Grow Financial Federal Credit Union

Grow Financial Federal Credit Union
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111

grow financial
federal credit union

March 13, 2019

[redacted]

A-18

Dear [redacted],

We value your membership and fully understand that the privacy of your personal information is of the utmost importance. It is for this reason that, as a precautionary measure, we are writing to let you know about an occurrence involving your personal information that we believe to be a very low risk to you.

On January 28, 2019, Grow Financial Federal Credit Union ("Grow Financial") discovered that skimming devices may have been placed on the ATMs at the credit union's Clearwater branch located at 2474 State Road 580, Clearwater, FL 33761 from December 30, 2018 to January 5, 2019 and from January 7, 2019 to January 10, 2019. Upon discovery of the situation, Grow Financial and its ATM servicer confirmed the removal of the skimming device from the ATMs and promptly alerted local law enforcement.

We believe that the skimming device acquired the following personal information stored on your affected debit card: your name, card number, expiration date and personal identification number (PIN). The skimming devices did not acquire your Social Security number, driver's license number, address, phone number or any of your other financial information. Grow Financial's core banking systems were not compromised or impacted as a result of this incident.

We take this kind of incident very seriously and have already begun taking measures to help prevent this type of incident from occurring in the future, including working with our ATM manufacturer to further secure our ATMs. We are monitoring the accounts of potentially affected members and are issuing new cards to those members who have been impacted by this incident. Members who experience losses due to fraudulent transactions as a result of this incident will have their funds fully restored.

We have established a direct telephone inquiry line to assist you with any questions you might have regarding this incident. This inquiry line is available at no cost to you between 8 a.m. and 5 p.m., Eastern Time, Monday through Friday, at 1-833-800-0018.

Sincerely,

Thomas R. Feindt

Thomas Feindt, President

## Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify Grow Financial or the other financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

**Credit Reports:** You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting http://www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files, is as follows:

| Equifax | Experian | TransUnion |
|---|---|---|
| 1-800-349-9960 | 1-888-397-3742 | 1-888-909-8872 |
| www.equifax.com | www.experian.com | www.transunion.com |
| P.O. Box 105788 | P.O. Box 9554 | P.O. Box 2000 |
| Atlanta, GA 30348 | Allen, TX 75013 | Chester, PA 19022 |

**Fraud Alerts:** You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at http://www.annualcreditreport.com.

**Credit and Security Freezes:** You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified above to find out more information. You can also obtain more information about fraud alerts and credit freezes by contacting the FTC at the address listed above.