Raynes, Nancy

From: Allan, Holly B <holly.b.allan@citizensbank.com>
Sent: Thursday, April 13, 2017 12:21 PM
To: DOJ: Consumer Protection Bureau
Subject: Data Breach Notification
Attachments: NH2017T103.docx; ATM Compromise Privacy Letter Citizens.doc

Good Afternoon,

Attached please find notification of a recent data breach affecting two New Hampshire residents. A sample of the customer notification is also attached.

If you have any questions or need any additional information, please do not hesitate to contact me.

Thank you,

Holly Allan, CIPP/US
Sr. Compliance Officer
CFG Compliance- Privacy
100 Sockanosset Cross Road
Cranston, RI 02920
(401) 282-4207 (office)
holly.b.allan@citizensbank.com

Citizens
Financial Group, Inc.

April 13, 2017

Consumer Protection and Antitrust Bureau
Department of Justice
33 Capitol Street
Concord, NH 03301

To Whom It May Concern:

I am writing on behalf of Citizens Financial Group, Inc. ("Citizens") to notify the New Hampshire Department of Justice of a recent data security incident of ATM skimming involving New Hampshire residents. Our investigation into the incident determined that ATM skimming took place at a Citizen's Bank ATM located in Auburn, Massachusetts. The skimming events took place on various dates in January 2017, and were discovered by Citizens on April 10, 2017. Customer name, debit card number, and PIN were compromised as a result of this incident.

Our investigation into the incident indicates that two of the affected Citizens customers reside in New Hampshire. To our knowledge, these New Hampshire residents have not experienced any type of identity theft as a result of the incident. All affected customers were notified by a personal letter (*See* Attached Customer Letter). This letter includes information on preventing identity theft and a telephone number that customers may call to obtain further information on the incident.

In accordance with the federal bank regulatory agencies' Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, Citizens has notified its four federal banking regulators.

If you have any questions, please contact the undersigned.

Sincerely,

Daniel Hoye
Head of Privacy
Citizens Financial Group
100 Sockanosset Crossroads
Cranston, RI 02920
Daniel.Hoye@citizensbank.com
(401) 282-7546

Citizens
Financial Group, Inc.

April 13, 2017

Consumer Protection and Antitrust Bureau
Department of Justice
33 Capitol Street
Concord, NH 03301

To Whom It May Concern:

I am writing on behalf of Citizens Financial Group, Inc. ("Citizens") to notify the New Hampshire Department of Justice of a recent data security incident of ATM skimming involving New Hampshire residents. Our investigation into the incident determined that ATM skimming took place at a Citizen's Bank ATM located in Auburn, Massachusetts. The skimming events took place on various dates in January 2017, and were discovered by Citizens on April 10, 2017. Customer name, debit card number, and PIN were compromised as a result of this incident.

Our investigation into the incident indicates that two of the affected Citizens customers reside in New Hampshire. To our knowledge, these New Hampshire residents have not experienced any type of identity theft as a result of the incident. All affected customers were notified by a personal letter (*See* Attached Customer Letter). This letter includes information on preventing identity theft and a telephone number that customers may call to obtain further information on the incident.

In accordance with the federal bank regulatory agencies' Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, Citizens has notified its four federal banking regulators.

If you have any questions, please contact the undersigned.

Sincerely,

Daniel Hoye
Head of Privacy
Citizens Financial Group
100 Sockanosset Crossroads
Cranston, RI 02920
Daniel.Hoye@citizensbank.com
(401) 282-7546

Citizens Bank

RE: IMPORTANT NOTICE ABOUT YOUR SENSITIVE CUSTOMER INFORMATION

Dear XXXX

We are writing to inform you that due to a security incident at the XXXXXX ATM, your ATM/Debit card may have been compromised. Appropriate measures were taken to secure the ATM upon discovery of the incident. The information that may have been compromised includes your name, ATM/Debit card number, PIN and card expiration date.

For this reason we have reissued your ATM/Debit card. Please note: you have zero liability for unauthorized transactions.

What we are doing to protect your information:

In an effort to protect you from possible fraudulent use of your card number, a new ATM/Debit card has been produced for you as stated above. Please note that **your old card was deactivated**, so activate and begin using the new card immediately and destroy your old card in a secure fashion. Your Personal Identification Number (PIN) will remain the same.

What you can do to protect your information:

There are actions you can take to mitigate the chances of fraud or identity theft to your account(s). Attached to this letter is a list of prudent and proactive steps you can take to reduce the risk to your account(s).

We are committed to providing you with timely and concise communications about issues affecting your customer information. As you are our valued customer, please do not hesitate to call 1-888-922-9999 with any questions or concerns.

Sincerely,

Don Cyr

Head of Fraud Operations

PROACTIVE STEPS YOU SHOULD TAKE TO HELP PROTECT YOUR INFORMATION

☐ **REMAIN VIGILANT FOR THE NEXT 12 TO 24 MONTHS.**

Carefully review your credit reports and bank, credit card and other account statements. If you discover unauthorized or suspicious activity on your credit report or by any other means, please call your local police immediately and file an identity theft report and/or obtain a copy of a police report.

☐ **CLOSE ANY AFFECTED ACCOUNT(S) AND OPEN NEW CITIZENS BANK ACCOUNT(S).**

We recommend you close your account(s) and open a new account(s) – a step we would like to take care of for you. Please call us at 1-888-922-9999 so we can put you in touch with Citizens Bank Colleagues specifically designated to handle this for you. All costs associated with closing your accounts and opening new accounts will be waived.

☐ **ORDER YOUR FREE ANNUAL CREDIT REPORTS.**

To order your free annual credit reports, call toll-free 1-877-322-8228, visit www.annualcreditreport.com, or complete the Annual Credit Report Request Form online and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Hearing impaired consumers can access the TDD service at 1-800-821-7232. For your free annual credit reports, do not contact the three nationwide consumer reporting agencies individually; they provide this service only through www.annualcreditreport.com.

☐ **WHEN YOU RECEIVE YOUR CREDIT REPORTS, REVIEW THEM CAREFULLY.**

Once you receive your credit reports, review them carefully. Please look for accounts you did not open or inquiries from creditors that you did not initiate. Verify that all the information is accurate. If you have questions or notice inaccurate information, please call the relevant consumer reporting agency at the telephone number listed on the report.

☐ **PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE.**

A fraud alert notifies creditors that you may be the victim of fraud and tells them to contact you before opening any new accounts. To place a fraud alert on your file, please call any one of the three nationwide consumer reporting agencies listed below. By calling one consumer reporting agency, the other two will automatically be notified. They will place a fraud alert on your credit file and will also assist you in getting a free credit report from each of the three agencies. The initial fraud alert will last for 90 days. You may want to renew it after the first 90 days. If you have already filed an identity theft report with your local police department, you should place an extended fraud alert on your credit file. This extended fraud alert is a free service and is valid for 7 years.

Equifax
Equifax Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374
1-877-478-7625
www.alerts.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834
1-800-680-7289
www.transunion.com

☐ **PLACE A SECURITY FREEZE ON YOUR CREDIT FILE.**

You may wish to place a security freeze on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide consumer reporting agencies without your consent. You can request a security freeze by contacting each of the three consumer reporting agencies at:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion Fraud Victim Assistance
P.O. Box 6790
Fullerton, CA 92834
1-888-909-8872
www.transunion.com

The consumer reporting agencies may charge a reasonable fee to place a security freeze on your account and may require that you provide proper identification prior to honoring your request.

☐ **LEARN MORE ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF.**

The Federal Trade Commission has online guidance about the steps consumers can take to protect themselves against identity theft. You can call 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261; write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; or visit the Federal Trade Commission's website at www.ftc.gov/idtheft to get more information. We also encourage you to report suspected identity theft to the Federal Trade Commission. If you suspect you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.