Citizens Financial Group, Inc.
Customer Incident Response Program (CIRP)
Data Breach Notification

SUPERVISORY OFFICE/BANK		RESPONSE
1.	Name of Bank:	Citizens Financial Group, Inc.
2.	Bank Charter Number:	
3.	Field Office:	Providence, Rhode Island
4.	Budget Code:	
5.	Name of ADC/LBEIC:	
6.	Name of C/MBS Portfolio Manager/Contact Person:	
7.	Name of banker reporting the incident:	Dan Hoye
8.	Title of banker reporting the incident:	Head of Privacy
EVENT		**RESPONSE**
9.	Date the incident took place:	Timeframe: 6/15/17 – 6/29/17
10.	Date incident was discovered by institution:	7/3/2017
11.	Method of discovery (describe how the bank learned about the incident):	Suspicious cash out activity
12.	Does the bank have a response program?	☒ Yes (Customer Incident Response Program - CIRP) ☐ No
12.(a)	If Yes to Question 12, was the response program activated?	☒ Yes ☐ No
13.	Type of incident/information lost:	☒ Electronic ☐ Hard-Copy ☐ Other Media Additional Information:
14.	CFG's Privacy Office Customer Incident Response Program tier risk rating:	☒ Tier 1 (Customer & Regulatory Notification) ☐ Tier 2 (Regulatory Notification Only)
15.	Description of the incident: CFG was alerted to potential ATM skimming activity through suspicious cash out activities in Massachusetts, New York, and Mexico. After identifying the cash out activity and analyzing the transaction history of the cards involved, Fraud Analytics determined that 15 CFG owned ATMs located in the Boston, MA area were the point of compromise. 4837 customers were impacted. There are approximately $1.6 million in losses to the bank. All ATMs involved are CFG owned Opteva ATMs. Video surveillance has confirmed the use of a deep insert skimmers in all ATMs involved in this incident.	
16.	Is the incident internal? (*i.e.,* bank personnel involved)	☐ Yes ☐ Undetermined ☒ No ☐ N/A
17.	Did the incident involve a system or data hosted by a Technology Service Provider (TSP)?	☐ Yes ☐ Undetermined ☒ No ☐ N/A
17.(a)	If Yes to Question 17, what is the TSP name and location:	Name: City: , State: Country: USA
17.(b)	If Yes to Question 17, is it likely that other customer banks of the TSP are affected as well?	☐ Yes ☐ Undetermined ☐ No ☐ N/A

18.	Did the incident involve a service conducted by a subcontractor of the bank's TSP?	☐ Yes ☐ Undetermined ☒ No ☐ N/A
19.	Did the incident impact or compromise the operational systems of the bank or TSP?	☐ Yes ☐ Undetermined ☒ No ☐ N/A
20.	Did the incident compromise or cause a loss of bank data?	☒ Yes ☐ Undetermined ☐ No ☐ N/A
CUSTOMER INFORMATION		**RESPONSE**
21.	Did the incident compromise the confidentiality of sensitive customer information?	☒ Yes ☐ Undetermined ☐ No ☐ N/A
21.(a)	If Yes to Question 21, what confidential data was included?	☒ Nonpublic Personal Information ☒ Customer Sensitive Information ☐ Other:
	Additional details if known:	☒ Name ☐ SSN ☐ Address ☐ Driver's License ☐ Telephone No. ☒ CCard/DCard ☐ Bank Acct. No. ☒ PIN ☐ Financial Info. ☐ Username ☐ Medical Info. ☐ Password
21.(b)	If Yes to Question 21, number of customers known to be affected.	4837
21.(c)	If Yes to Question 21, number of additional customers potentially affected.	☐ Undetermined ☐ N/A 0 Customers; 0 Commercial
22.	Could the compromised information expose a retail customer to financial loss through fraud or identify theft?	☒ Yes ☐ Undetermined ☐ No ☐ N/A
22.(a)	If Yes to Question 22, what is the amount of any retail losses to date:	☐ Determined $0.00 ☒ Undetermined ☐ Other:
23.	Could the compromised information expose a commercial customer to financial loss through fraud or identify theft?	☐ Yes ☐ Undetermined ☒ No ☐ N/A
23.(a)	If Yes to Question 23, what is the amount of any commercial customer losses to date:	☒ Determined – $0.00 ☐ Undetermined ☐ Other:
24.	Estimated bank's financial losses:	☒ Determined – $1,632,487 ☐ Undetermined ☐ Other: $
25.	Estimated customer's financial losses:	☒ Determined - $0.00 ☐ Undetermined ☐ Other:
BANK RESPONSE		**RESPONSE**
26.	Provide a brief description of actions taken to date by bank.	☒ Internal Investigation ☒ External Investigation ☐ Employee Education/Training ☐ Other:
27.	Has the bank successfully contained the incident?	☒ Yes ☐ Undetermined ☐ No ☐ N/A

27.(a)	If Yes to Question 27, describe the current status.	All cards have been reissued. All customers have been contacted informing them of this incident.
28.	Have the perpetrators (alleged criminal) been identified?	☒ Yes ☐ Undetermined ☐ No ☐ N/A
28.(a)	If Yes to Question 28, who?	2 suspects have been arrested to date.
29.	Has the bank reported the incident to law enforcement authorities?	☒ Yes ☐ Undetermined ☐ No ☐ N/A
29.(a)	If Yes to Question 29, provide name(s) of law enforcement authorities notified (*i.e.,* FBI, Secret Service, Local Police, State Attorney, Others)	☒ FBI ☒ State Police ☒ USSS ☒ Local Police ☐ USPIS ☐ State AG ☐ DOJ ☐ State Offices ☐ Other Fed. Other States: ☐ Intern'l
30.	Has any law enforcement authority requested, in writing, that the bank delay notifying affected customers in order not to compromise their criminal investigation?	☐ Yes ☐ Undetermined Month , Year ☐ N/A ☒ No
30.(a)	If Yes to Question 30, which law enforcement authority?	☐ FBI ☐ State Police ☐ USSS ☐ Local Police ☐ USPIS ☐ State AG ☐ DOJ ☐ State Offices ☐ Other Fed. Other States: ☐ Intern'l
30.(b)	If Yes to Question 30, has any law enforcement subsequently informed the bank that notifying the affected customers will no longer compromise their criminal investigation?	☐ Yes ☐ Undetermined Month , Year ☐ N/A ☐ No
31.	Has the bank filed a SAR or is the bank going to file a SAR?	☐ Yes ☒ No ☐ N/A
32.	Has the bank sent notice to affected customers or is it in the process of sending notification?	☒ Yes ☐ No ☐ N/A
32.(a)	If Yes to Question 32, when?	
32.(b)	If Yes to Question 32, how many customers?	4837
32.(c)	If Yes to Question 32, method of notification (*i.e.,* Telephone, Fax, E-Mail, Letter).	☒ Written Letter ☒ Telephone Call ☐ E-Mail ☐ Website Posting ☐ Fax ☐ Media Alert
33.	Actions bank plans to take:	☐ Credit Monitoring Offered ☐ CRAs Notified ☒ State Agency Notification ☐ Other: ☐ No additional actions at this time

EXTERNAL KNOWLEDGE OF INCIDENT	RESPONSE
34. Is the media aware of the event? (Description should include extent of media coverage, tone of media coverage, bank press release or statements, congressional awareness, CAG complaints or inquiries into the event.)	☒ Yes ☐ No ☐ N/A Fox News 25 in Boston, MA, posted an article related to skimming events at several local financial institutions and posted a video clip on their website.
REGULATORS NOTIFIED	**RESPONSE**
35. What regulators has the bank notified?	☒ FDIC ☒ FED ☒ OCC ☒ CFPB ☒ Other: MA, NH, VT, NY, ME, CT

Citizens Bank

c/o GCG
PO Box 10459
Dublin, OH 43017-4059

<<FirstName>> <<LastName>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

RE: IMPORTANT NOTICE ABOUT YOUR SENSITIVE CUSTOMER INFORMATION

Dear <<FirstName>> <<LastName>>:

We are writing to inform you that due to a security incident at an«Line_Number» 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. To prevent potential fraudulent use, we have issued you a new ATM/Debit card. You should receive your card within ten business days if you have not already.

Your Citizens Bank ATM/Debit card is protected by Citizens Bank's Zero Liability Policy. To learn more about Zero Liability protection and coverage, visit https://www.citizensbank.com/checking/debit-cards/zero-liability.aspx.

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 reduce 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 lower 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. Please also notify Citizens Bank immediately of any unauthorized use.

❑ **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.