

December 19, 2022

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Pl.
Baltimore, MD 21202
e-mail: Idtheft@oag.state.md.us



To Whom It May Concern:

On behalf of Banco Popular de Puerto Rico (the "Bank"), I am writing to inform you about a recent incident in which personal information relating to one individual Maryland resident (the "Consumer") was accessed by an unauthorized third party.

Specifically, the Bank discovered that on July 10, 2021, an unauthorized third party was able to log in to the Consumer's online banking application profile. The Consumer's online banking application was compromised due to the third party's automated attempts to guess log-in credentials. Through our investigation, the Bank has determined that the third party accessed the Consumer's username and password, potentially exposing the Consumer's name, address, phone number and email address.

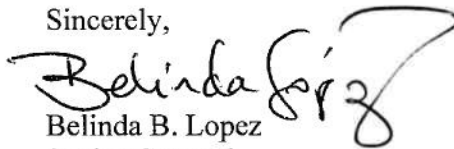
In response to this incident, the Bank conducted a reset of the Consumer's online banking profile to prevent unauthorized third parties from accessing the Consumer's account. Furthermore, the Bank continues to monitor and adjust its security measures to protect customer online account access and identify instances of unauthorized access.

The Bank will notify the Consumer of this incident on December 21, 2022 and provide the Consumer with an offer for one-year complimentary credit monitoring service. This service can help the Consumer detect possible misuse of information and provides identity protection support, focused on identification and resolution of identity theft.

Attached is a sample of the letter that the Bank is providing to the Consumer.

Please do not hesitate to contact me at 787-321-7217, if you have any questions.

Sincerely,



Belinda B. Lopez
Senior Counsel
Popular, Inc.

Enclosure

December 20, 2022

<<Customer Name>>

<<Address Line 1>>

<<Address Line 2>>

<<Address Line 3>>

Dear <<First Name>> <<Last Name>>:

We take customer privacy and the protection of your information seriously. As part of our regular monitoring efforts, we identified unusual activity in the user profile you use to log into the Mi Banco digital banking application ("Mi Banco"). Based on our investigation, we believe that an unauthorized third party was able to log in to your Mi Banco account profile, potentially exposing some of your account information.

What information was involved?

Our investigation determined that the unauthorized third party used your Mi Banco username and password to log into your account. After logging into your account, the third party may have been able to view your name, address, phone number and email address.

What are we doing?

We launched an investigation to determine the nature and scope of the incident and brought on a leading cybersecurity firm to assist us in these efforts. As part of our protocols, we have also alerted and are cooperating with law enforcement. In addition to these efforts, we continue to monitor and adjust our security measures to protect customer online account access and identify unauthorized access.

What can you do?

- **Activate 2-step verification:** We strongly recommend activating the 2-Step verification feature in your Mi Banco account. It provides an additional layer of protection by requiring a unique code to access Mi Banco. For additional information please visit:
www.popular.com/en/security/mobile/
 - **To activate this feature via the Mi Banco mobile app:**
 - *iPhone:* Select "More" in the lower right corner of the Mi Banco app; on the "Service" section, click on "2 Step verification" and follow instructions.
 - *Android:* Select "Settings" in the upper left corner, on the "Service" section, click on "2 Step verification" and follow instructions.
 - **To activate this feature via desktop:**
 - Log into Mi Banco, go to "My Information" in the main menu and choose "2 Step verification" and follow the instructions.
- **Use a complex and unique password:** We suggest that your password contain at least 10 characters, mixing numbers and letters (example: prin10so49). Avoid personal names, dates of

birth, numbers in sequence, or other sensitive information that may identify you. In addition, we recommend that you change your password for any online account for which you use the same password.

- **Enroll in free Equifax credit monitoring:** We have engaged Equifax to provide you with a one-year complimentary credit monitoring service. This service can help you detect possible misuse of information and provides identity protection support, focused on identification and resolution of identity theft. Enrolling in this service will not affect your credit score.

You have until March 31, 2023, to activate the free credit monitoring service by using the following activation code: 305752496712. This code is unique for your use and should not be shared. To enroll, please visit www.myservices.equifax.com/tri or call Equifax at (800) 685-1111.

- **Activate Mi Banco Alerts:** Get notified instantly on your accounts' transactions and activity through Push Notifications, email, or text message (SMS). For more information, please visit <https://www.popular.com/en/mi-banco/online/alerts/>.
- **Other Recommendations:**
 - **Report an incident** - You may contact the Federal Trade Commission (FTC) or law enforcement to report incidents of identity theft or to learn about other ways to protect yourself. To learn more, go to www.ftc.gov/idtheft, call (877) IDTHEFT (438-4338), or write to the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.
 - **Freeze or restrict access** - In addition, you can contact each of the credit reporting agencies to place a security freeze to restrict access to your credit report.
 - You must provide your name, address, date of birth, Social Security number and other personal information. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.
 - **Delete information** - If you discover information on your credit report arising from a fraudulent transaction, request that the credit reporting agency delete that information from your credit report file.
 - **Monitor your account** - You should remain vigilant over the next 12 to 24 months, including by regularly reviewing your account statements and monitoring free credit reports. If you identify any unusual or suspicious activity in your account's transaction history, please contact us at 787-763-3046, 1-855-763-3046.
 - **Place fraud alerts** - You may place a fraud alert in your credit report file by calling just one of the three nationwide credit reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. A fraud alert can make it more difficult for someone

- to get credit in your name because it alerts creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit.
- **Obtain a free copy of your credit report** - Under the Fair Credit Reporting Act (FCRA), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com, calling (877) 322-8228, or contacting the nationwide credit reporting agencies at:

Equifax
(800) 685-1111
PO Box 740241
Atlanta, GA 30374-0241
www.Equifax.com/personal/credit-report-services

Experian
(888) 397-3742
PO Box 9701
Allen, TX 75013
www.Experian.com/help

TransUnion
(888) 909-8872
Fraud Victim Assistance Division
PO Box 2000
Chester, PA 19022
www.TransUnion.com/credit-help

- **Other rights:** You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You also have other rights under the FCRA. For further information about your rights under the FCRA, please visit: https://files.consumerfinance.gov/f/documents/bcfc_consumer-rights-summary_2018-09.docx (English) or https://files.consumerfinance.gov/f/documents/bcfc_consumer-rights-summary_2018-09_es.docx (Spanish).

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
<http://www.ftc.gov/idtheft/>

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

We regret any inconvenience or concern this incident may have caused. For additional information, please contact us at 787- 763-3046, 1-855- 763-3046. One of our representatives will gladly assist you. You can also visit www.popular.com/security for tips on how to keep your accounts more secure.

We appreciate the opportunity to serve you and will continue to monitor for any unauthorized access to your account.

Cordially,

Luis De Jesús
Information Security Specialist



March 13, 2023

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Pl.
Baltimore, MD 21202
e-mail: Idtheft@oag.state.md.us



To Whom It May Concern:

On behalf of Banco Popular de Puerto Rico (the "Bank"), I am writing to inform you that we have identified another individual Maryland resident (the "Consumer"), whose personal information was accessed by an unauthorized third party with respect to the same incident that we communicated in a letter dated December 19, 2022, sent via certified mail. To date, the Bank has only identified two Maryland residents impacted by the incident.

As previously reported, the Bank discovered that on July 10, 2021, an unauthorized third party was able to log in to the Consumer's online banking application profile. The Consumer's online banking application was compromised due to the third party's automated attempts to guess log-in credentials. Through our investigation, the Bank has determined that the third party accessed the Consumer's username and password, potentially exposing the Consumer's name, address, phone number and email address.

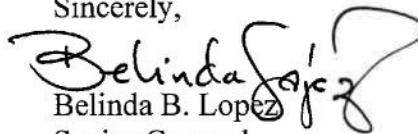
In response to this incident, the Bank conducted a reset of the Consumer's online banking profile to prevent unauthorized third parties from accessing the Consumer's account. Furthermore, the Bank continues to monitor and adjust its security measures to protect customer online account access and identify instances of unauthorized access,

The Bank will notify the Consumer of this incident on March 14, 2023, and provide the Consumer with an offer for one-year complimentary credit monitoring service. This service can help the Consumer detect possible misuse of information and provides identity protection support, focused on identification and resolution of identity theft.

Attached is a sample of the letter that the Bank is providing to the Consumer.

Please do not hesitate to contact me at 787-321-7217 if you have any questions.

Sincerely,


Belinda B. Lopez
Senior Counsel
Popular, Inc.

Enclosure

February __, 2023

<<Customer Name>>

<<Address Line 1>>

<<Address Line 2>>

<<Address Line 3>>

Dear <<First Name>> <<Last Name>>:

At Popular, we take customer privacy and the protection of your information seriously. As part of our regular monitoring efforts, we identified unusual activity in the user profile you use to log into the Mi Banco digital banking application ("Mi Banco"). Based on our investigation, we believe that an unauthorized third party was able to log in to your Mi Banco account profile, potentially exposing some of your account information.

What information was involved?

Our investigation determined that the unauthorized third party used your Mi Banco username and password to log into your account. After logging into your account, the third party may have been able to view your name, address, phone number and email address.

What are we doing?

We launched an investigation to determine the nature and scope of the incident and brought on a leading cybersecurity firm to assist us in these efforts. As part of our protocols, we have also alerted and are cooperating with law enforcement. In addition to these efforts, we continue to monitor and adjust our security measures to protect customer online account access and identify unauthorized access.

What can you do?

- **Activate 2-step verification:** We strongly recommend activating the 2-Step verification feature in your Mi Banco account. It provides an additional layer of protection by requiring a unique code to access Mi Banco. For additional information please visit:
www.popular.com/en/security/mobile/.
 - **To activate this feature via the Mi Banco mobile app:**
 - *iPhone:* Select "More" in the lower right corner of the Mi Banco app; on the "Service" section, click on "2 Step verification" and follow instructions.
 - *Android:* Select "Settings" in the upper left corner, on the "Service" section, click on "2 Step verification" and follow instructions.
 - **To activate this feature via desktop:**
 - Log into Mi Banco, go to "My Information" in the main menu and choose "2 Step verification" and follow the instructions.
- **Use a complex and unique password:** We suggest that your password contain at least 10 characters, mixing numbers and letters (example: prin10so49). Avoid personal names, dates of

birth, numbers in sequence, or other sensitive information that may identify you. In addition, we recommend that you change your password for any online account for which you use the same password.

- **Enroll in free Equifax credit monitoring:** We have engaged Equifax to provide you with a one-year complimentary credit monitoring service. This service can help you detect possible misuse of information and provides identity protection support, focused on identification and resolution of identity theft. Enrolling in this service will not affect your credit score.

You have until March 31, 2023, to activate the free credit monitoring service by using the following activation code: 305752496712. This code is unique for your use and should not be shared. To enroll, please visit www.myservices.equifax.com/tri or call Equifax at (800) 685-1111.

- **Activate Mi Banco Alerts:** Get notified instantly on your accounts' transactions and activity through Push Notifications, email, or text message (SMS). For more information, please visit <https://www.popular.com/en/mi-banco/online/alerts/>.
- **Other Recommendations:**
 - **Report an incident** - You may contact the Federal Trade Commission (FTC) or law enforcement to report incidents of identity theft or to learn about other ways to protect yourself. To learn more, go to www.ftc.gov/idtheft, call (877) IDTHEFT (438-4338), or write to the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.
 - **Freeze or restrict access** - In addition, you can contact each of the credit reporting agencies to place a security freeze to restrict access to your credit report.
 - You must provide your name, address, date of birth, Social Security number and other personal information. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.
 - **Delete information** - If you discover information on your credit report arising from a fraudulent transaction, request that the credit reporting agency delete that information from your credit report file.
 - **Monitor your account** - You should remain vigilant over the next 12 to 24 months, including by regularly reviewing your account statements and monitoring free credit reports. If you identify any unusual or suspicious activity in your account's transaction history, please contact us at 787-763-3046, 1-855-763-3046.
 - **Place fraud alerts** - You may place a fraud alert in your credit report file by calling just one of the three nationwide credit reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. A fraud alert can make it more difficult for someone

- to get credit in your name because it alerts creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit.
- **Obtain a free copy of your credit report** - Under the Fair Credit Reporting Act (FCRA), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com, calling (877) 322-8228, or contacting the nationwide credit reporting agencies at:

Equifax
(800) 685-1111
PO Box 740241
Atlanta, GA 30374-0241
www.Equifax.com/personal/credit-report-services

Experian
(888) 397-3742
PO Box 9701
Allen, TX 75013
www.Experian.com/help

TransUnion
(888) 909-8872
Fraud Victim Assistance Division
PO Box 2000
Chester, PA 19022
www.TransUnion.com/credit-help

- **Other rights:** You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You also have other rights under the FCRA. For further information about your rights under the FCRA, please visit: https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.docx (English) or https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09_es.docx (Spanish).

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
<http://www.ftc.gov/idtheft/>

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

We regret any inconvenience or concern this incident may have caused. For additional information, please contact us at 787- 763-3046, 1-855- 763-3046. One of our representatives will gladly assist you. You can also visit www.popular.com/security for tips on how to keep your accounts more secure.

We appreciate the opportunity to serve you and will continue to monitor for any unauthorized access to your account.

Cordially,

Luis De Jesús
Information Security Specialist