

Colin M. Battersby
Direct Dial: 248-593-2952
E-mail: cbattersby@mcdonaldhopkins.com

August 7, 2023

VIA E-MAIL

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Banco Popular de Puerto Rico – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Banco Popular de Puerto Rico (“Popular”). I am writing to provide notification of an incident at Popular’s vendor that affected the security of personal information of approximately 123 Maryland residents. Popular’s investigation is ongoing, and this notification will be supplemented with any significant facts or findings subsequent to this submission, if any. By providing this notice, Popular does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Popular’s vendor PricewaterhouseCoopers (“PwC”) has been a victim of a cybersecurity breach that included certain personal information of Popular’s customers. The breach involved the compromise of a software, MOVEit, used by PwC to transfer files for a small number of its clients, including Popular. As a public corporation that trades in the stock market, Popular is required to use the services of an auditing and accounting firm such as PwC. The job of auditing Popular requires, due to its nature, that Popular share client information so that PwC can perform certain independent validations necessary for Popular to issue financial statements. Upon learning of the incident, PwC immediately launched an investigation and ceased using the impacted software. As a result of this investigation, it was determined on July 24, 2023, that certain of the files compromised in the incident included personal information of Popular customers. The compromised personal information includes names, Social Security numbers, mortgage loan numbers, and mortgage-related fields.

Out of an abundance of caution, Popular wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Popular is providing the affected residents with written notification of this incident commencing on or about August 7, 2023 in substantially the same form as the letter

attached hereto. Popular is offering the affected residents complimentary two-year membership with a credit monitoring service. Popular is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies, the Federal Trade Commission, and the Maryland Attorney General. The affected residents are also being provided a toll-free telephone number to call with any questions or concerns.

Popular takes this issue very seriously and regrets that this incident occurred. Should you have any questions concerning this notification, please contact me at (248) 593-2952 or cbattersby@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

A handwritten signature in blue ink, appearing to read 'Colin M. Battersby', with a large, stylized initial 'C' and 'B'.

Colin M. Battersby

Encl.



August X, 2023

<<Customer Name>>

<<Address Line 1>>

<<Address Line 2>>

<<Address Line 3>>

Dear <<Full Name>>:

We write to inform you that one of our vendors, PricewaterhouseCoopers (PwC), has been a victim of a cybersecurity breach that included certain personal information of our customers. The breach involved the compromise of a software, MOVEit, used by PwC to transfer files for a small number of its clients, including Banco Popular de Puerto Rico (Popular).

As a public corporation that trades in the stock market, Popular is required to use the services of an auditing and accounting firm such as PwC. The job of auditing Popular requires, due to its nature, that Popular share client information so that PwC can perform certain independent validations necessary for Popular to issue financial statements.

Upon learning of the incident, PwC immediately launched an investigation and ceased using the impacted software. As a result of this investigation, it was determined on July 24th, 2023, that certain of the files compromised in the incident included personal information of our customers. The compromised personal information includes your name, Social Security number, mortgage loan number ending in <XXXX>, and mortgage-related fields.

This notice explains the services available to you and other steps you may take in response. We want you to know that we take this issue very seriously and regret that this incident occurred.

Free credit monitoring and identity protection service:

We have arranged for you, at your option, to enroll in a free, two-year (2) credit monitoring service with Equifax.

This service will help you detect possible misuse of information and provides identity protection support. Enrolling in this service will not affect your credit score.



To subscribe to these Equifax services, access the QR code or www.equifax.com/activate and follow the enclosed instructions, or call **1.866.815.8535** for enrollment support. Please use the following activation code **XXXXXXXXXXXX** to subscribe on or before **November 30, 2023**.

Our recommendations:

- **Activate Mi Banco Alerts:** Sign up to receive instant notifications about account transactions and activity through push notifications, emails, or text messages (SMS). For additional information, visit <https://www.popular.com/en/mi-banco/online/alerts/>.
- **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.
- **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.
- **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).



You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1.888.743.0023.

We regret any inconvenience or concern this incident may have caused. For additional information, please call 787.771.6530 or our toll-free number 1.855.220.2201. One of our representatives will gladly assist you. You can also visit www.popular.com/en/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,

Department of Customer Service
Banco Popular Puerto Rico



Enrollment Deadline: **November 30, 2023**

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product.

Key Features

- Annual access to your 3-bureau credit report and VantageScore¹ credit scores.
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score.
- 3-bureau credit monitoring² with email notifications of key changes to your credit reports.
- WebScan notifications³ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites.
- Automatic fraud alerts⁴, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock⁵.
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf.
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁶.
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to www.equifax.com/activate.

Enter your unique Activation Code of **<Activation Code>** then click "Submit".

1. Register:

Complete the form with your contact information and click "Continue".

If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4.

2. Create Account:

Enter your email address, create a password, and accept the terms of use.

3. Verify Identity:

To enroll in your product, we will ask you to complete our identity verification process.

4. Checkout:

Upon successful verification of your identity, you will see the Checkout Page.

Click 'Sign Me Up' to finish enrolling.

You're done!

The confirmation page shows your completed enrollment.

Click "View My Product" to access the product features.

¹The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

²Credit monitoring from Experian and TransUnion will take several days to begin.

³WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

⁴The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

⁵Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

⁶The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.