



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Paul T. McGurkin, Jr.
Office: (267) 930-4788
Fax: (267) 930-4771
Email: pmcgurkin@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

May 6, 2022

VIA E-MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent Ametros Financial Corporation (“Ametros”) located at 200 Ballardville Street, Suite 200 P.O. Box 827 Wilmington, MA 01887, and are writing to notify your office of an incident that occurred at Technology Management Resources (“TMR”), a vendor of Ametros’ subcontractor, IBERIABANK (“Iberia”), that may affect the security of some personal information relating to one (1) Maryland resident. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Ametros does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 14, 2021, TMR, Iberia’s lockbox vendor, identified unusual activity with a user account in its lockbox application. It was determined that the activity was unauthorized, and the account was promptly disabled. TMR investigated the incident and reported that the unauthorized activity occurred between October 12, 2021, and October 14, 2021. According to TMR’s investigation, an unauthorized party accessed bytes that were associated with certain images for lockbox payments and related documents. TMR has stated that the bytes (bits of computer data) accessed by the unauthorized party were in binary format only and as an encoded string (this means that the data was an encoded series of information stored in the form of ones and zeros). Technical manipulation of the bytes would be required to convert them into images. Iberia is unaware if actual images were viewed by the unauthorized party during the period of unauthorized access. TMR has advised that it is likely that these bytes were obtained by the unauthorized party based

upon traffic to the IP address. TMR's investigation has not revealed any evidence to confirm that unauthorized party converted the bytes into images, although this could have been possible. Iberia provided notice of this event to Ametros on January 7, 2022. On March 7, 2022, Iberia confirmed that the information that could have been subject to unauthorized access includes name, address, financial account information, medical information, and health insurance information of one (1) Maryland resident.

Notice to Maryland Resident

On or about May 6, 2022, Iberia on behalf of Ametros provided written notice of this incident to all affected individuals, which includes one (1) Maryland resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Ametros moved quickly to investigate and respond to the incident, assess the security of Ametros systems, and notify potentially affected individuals. Ametros is providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Ametros is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Ametros is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4788.

Very truly yours,

Paul T. McGurkin, Jr. of
MULLEN COUGHLIN LLC

PTM:bwt
Enclosure

Exhibit *A*

<<DATE>>

<<First Name>> <<Middle Name>> <<Last Name>>

<<Address 1>>

<<Address 2>>

<<City>>, <<State >> <<Zip Code>>

RE: Notice of Data Incident

Dear <<First Name>> <<Middle Name>> <<Last Name>> ,

IBERIABANK is writing, at the request of Ametros Financial Corporation (“Ametros”), to notify you of a security incident affecting one of IBERIABANK’s service providers, Technology Management Resources, Inc. (“TMR”). Ametros has a lockbox service with IBERIABANK for collecting and processing payments from its customers. IBERIABANK uses TMR as a third-party lockbox service provider to process payments and capture pertinent payment data for items received in the lockbox. You made a payment or submitted information to Ametros’ IBERIABANK lockbox. TMR recently provided notice to IBERIABANK of an incident which may have involved your protected health information. IBERIABANK subsequently reported this incident to Ametros. Please note this incident did not involve unauthorized access to Ametros’ systems. This correspondence is intended to provide you with information regarding the incident and the resources available to you to help protect your information, should you feel it appropriate to do so.

What happened? On October 14, 2021, TMR identified unusual activity with a user account in its lockbox application. It was determined that the activity was unauthorized, and the account was promptly disabled. TMR investigated the incident and reported that the unauthorized activity occurred between October 12, 2021, and October 14, 2021. According to TMR’s investigation, an unauthorized party accessed bytes that were associated with certain images for lockbox payments and related documents. TMR has stated that the bytes (bits of computer data) accessed by the unauthorized party were in binary format only and as an encoded string (this means that the data was an encoded series of information stored in the form of ones and zeros). Technical manipulation of the bytes would be required to convert them into images. We are unaware that actual images were viewed by the unauthorized party during the period of unauthorized access. TMR has advised that it is likely that these bytes were obtained by the unauthorized party based upon traffic to the IP address. TMR’s investigation has not revealed any evidence to confirm that unauthorized party converted the bytes into images, although this could have been possible.

What information was involved? According to TMR, the encoded data was associated with certain check images and related documents within TMR’s client payment application (iRemit) that may have contained protected health information. Specifically, the information potentially involved may have included your name, [Data Elements].

What is IBERIABANK doing in response? IBERIABANK takes the protection and proper use of personal information provided to us very seriously. As part of our ongoing commitment to information privacy and the security of information, we are notifying you of this incident. Although we are not aware of any misuse of your information as a result of this incident, out of an abundance of caution, we are offering you complimentary credit monitoring and identity theft protection through TransUnion. These services will be

available to you for twelve (12) months at no cost in order to give you peace of mind. You must complete the enrollment steps listed in this letter to activate these services. We are also reviewing all relevant business practices regarding the security of information maintained by TMR.

What you can do. As a best practice, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your financial account statements, Explanation of Benefits, and to monitor your credit reports for suspicious activity. We encourage you to review the attached “Steps You Can Take to Protect Your Personal Information” which includes additional information and resources to assist you in protecting your personal information, should you feel it appropriate to do so. We also encourage you to enroll in the complimentary credit monitoring and identity theft protection services we are making available to you.

For more information. If you have additional questions about the 2021 lockbox service provider security incident or the protections available to you, please call [Number], toll-free, Monday through Friday, 9:00 a.m. – 9:00 p.m. Eastern Time. We apologize for any inconvenience this 2021 lockbox service provider security incident may have caused you. You may also write to Ametros at 200 Ballardvale Street, Suite 200 P.O. Box 827 Wilmington, MA 01887.

Sincerely,

[Name]

[Title]

IBERIABANK

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Enroll in Credit Monitoring

We are providing you with access to Single Bureau Credit Monitoring services at no charge. Services are for 12 months from the date of enrollment. When changes occur to your TransUnion credit file, notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud, you will also have access to identity protection support. In order for you to receive the monitoring service described above, you must enroll within 90 days from the date of this letter.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to www.mytrueidentity.com and follow the instructions provided. When prompted please provide the following unique code to receive services: <CODE HERE>. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

Monitor Your Accounts and Order Your Free Annual Credit Reports

In addition to enrolling in the complimentary credit monitoring services above, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your financial account statements, debit/credit card statements, and other statements, and to monitor your credit reports for suspicious activity to detect errors. (For Oregon and Iowa residents: Report any suspected identity theft to law enforcement, the Federal Trade Commission and your State Attorney General). Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus to request a free copy of your report. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the three consumer reporting agencies directly to obtain such additional reports). Periodically review a copy of your credit report for discrepancies and identify any accounts you did not open or inquiries you did not authorize.

Freeze Your Credit File

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place a security freeze on your credit report. Note that a security freeze generally does not apply to an existing creditor or its agents or affiliates for certain types of account review, collection, fraud Control or similar activities. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	TransUnion	Equifax
P.O. Box 9554 Allen, TX 75013	P.O. Box 160 Woodlyn, PA 19094	P.O. Box 105788 Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com	www.transunion.com	www.equifax.com

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report or complaint to a law enforcement agency concerning identity theft.

If you request a security freeze via toll-free telephone or other secure electronic means, the credit reporting agencies have one (1) business day after receiving the request to place the freeze. In the case of a request made by mail, the bureaus have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving a request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving the request to remove the freeze.

Place Fraud Alerts on Your Credit File

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon

seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should you wish to place a fraud alert, please contact any one of the consumer reporting agencies listed above to activate an alert.

File or Obtain a Police Report

You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission (FTC) can be reached at 600 Pennsylvania Avenue NW, Washington, D.C. 20580, by phone at 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261, or by going to www.ftc.gov/idtheft. The FTC encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file a complaint through the above-referenced contact information.

You also have rights under the federal Fair Credit Reporting Act (FCRA), which promotes the accuracy, fairness and privacy of information in the files of consumer reporting agencies. These rights include the right to receive a copy of your credit report, the right to ask for a credit score, the right to dispute incomplete or inaccurate information, and the right to obtain corrections to your report or delete inaccurate, incomplete, unverifiable information. Consumer reporting agencies may not report outdated negative information. Access to your file is limited, and you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you receive based upon information in your credit report. You may have additional rights under the FCRA not summarized here. We recommend and encourage you to review your rights pursuant to the FCRA at https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Avenue N.W., Washington D.C., 20580.

For residents of North Carolina: The North Carolina Office of the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226, and www.ncdoj.com. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For residents of Maryland: The Maryland Office of the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us. You can obtain information from the Attorney General or Federal Trade Commission about preventing identity theft.

For residents of New Mexico: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your

credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Furthermore, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccuracies, incomplete or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For residents of New York: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

For residents of Rhode Island: The Rhode Island Office of the Attorney General can be contacted at: 150 South Main Street, Providence, RI 02903, 1-401-274-4400 and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed regarding this incident. There are [X] Rhode Island residents impacted by this incident.

For residents of the District of Columbia: The Attorney General may be contacted at: 400 6th Street NW, Washington, D.C. 20001, 1-(202) 727-3400 and <https://oag.dc.gov/>. You may obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Paul T. McGurkin, Jr.
Office: (267) 930-4788
Fax: (267) 930-4771
Email: pmcgurkin@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

May 11, 2022

VIA E-MAIL

Office of the Attorney General
Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Supplemental Notice of Data Event

Dear Sir or Madam:

We represent Ametros Financial Corporation (“Ametros”) located at 200 Ballardville Street, Suite 200 P.O. Box 827 Wilmington, MA 01887, and are writing to supplement our May 6, 2022 notice to you, attached here as ***Exhibit A***. By providing this notice, Ametros does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

As stated in the May 6, 2022 notice to your office, on October 14, 2021, TMR, Iberia’s lockbox vendor, identified unusual activity with a user account in its lockbox application. It was determined that the activity was unauthorized, and the account was promptly disabled. TMR investigated the incident and reported that the unauthorized activity occurred between October 12, 2021, and October 14, 2021. According to TMR’s investigation, an unauthorized party accessed bytes that were associated with certain images for lockbox payments and related documents. TMR has stated that the bytes (bits of computer data) accessed by the unauthorized party were in binary format only and as an encoded string (this means that the data was an encoded series of information stored in the form of ones and zeros). Technical manipulation of the bytes would be required to convert them into images. Iberia is unaware if actual images were viewed by the unauthorized party during the period of unauthorized access. TMR has advised that it is likely that these bytes were obtained by the unauthorized party based upon traffic to the IP address. TMR’s investigation has not revealed any evidence to confirm that unauthorized party converted the bytes into images, although this could have been possible. Iberia provided notice of this event to Ametros on January

7, 2022. On March 7, 2022, Iberia confirmed that the information that could have been subject to unauthorized access includes name, address, financial account information, medical information, and health insurance information of one (1) Maryland resident. Following Ametros' May 6, 2022 notice to your office, Iberia provided notification to an additional fourteen (14) Maryland residents.

Notice to Maryland Residents

On May 11, 2022, Iberia on behalf of Ametros provided written notice of this incident to additional affected individuals, which includes fourteen (14) Maryland residents. Therefore, fifteen (15) Maryland residents will be notified of this event. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon discovering the event, Ametros moved quickly to investigate and respond to the incident, assess the security of Ametros systems, and notify potentially affected individuals. Iberia, on behalf of Ametros, is providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Ametros is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Ametros is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4788.

Very truly yours,

Paul T. McGurkin, Jr. of
MULLEN COUGHLIN LLC

PTM:bwt
Enclosure

Exhibit *A*



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Paul T. McGurkin, Jr.
Office: (267) 930-4788
Fax: (267) 930-4771
Email: pmcgurkin@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

May 6, 2022

VIA E-MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent Ametros Financial Corporation (“Ametros”) located at 200 Ballardville Street, Suite 200 P.O. Box 827 Wilmington, MA 01887, and are writing to notify your office of an incident that occurred at Technology Management Resources (“TMR”), a vendor of Ametros’ subcontractor, IBERIABANK (“Iberia”), that may affect the security of some personal information relating to one (1) Maryland resident. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Ametros does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On October 14, 2021, TMR, Iberia’s lockbox vendor, identified unusual activity with a user account in its lockbox application. It was determined that the activity was unauthorized, and the account was promptly disabled. TMR investigated the incident and reported that the unauthorized activity occurred between October 12, 2021, and October 14, 2021. According to TMR’s investigation, an unauthorized party accessed bytes that were associated with certain images for lockbox payments and related documents. TMR has stated that the bytes (bits of computer data) accessed by the unauthorized party were in binary format only and as an encoded string (this means that the data was an encoded series of information stored in the form of ones and zeros). Technical manipulation of the bytes would be required to convert them into images. Iberia is unaware if actual images were viewed by the unauthorized party during the period of unauthorized access. TMR has advised that it is likely that these bytes were obtained by the unauthorized party based

upon traffic to the IP address. TMR's investigation has not revealed any evidence to confirm that unauthorized party converted the bytes into images, although this could have been possible. Iberia provided notice of this event to Ametros on January 7, 2022. On March 7, 2022, Iberia confirmed that the information that could have been subject to unauthorized access includes name, address, financial account information, medical information, and health insurance information of one (1) Maryland resident.

Notice to Maryland Resident

On or about May 6, 2022, Iberia on behalf of Ametros provided written notice of this incident to all affected individuals, which includes one (1) Maryland resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Ametros moved quickly to investigate and respond to the incident, assess the security of Ametros systems, and notify potentially affected individuals. Ametros is providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Ametros is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Ametros is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4788.

Very truly yours,



Paul T. McGurkin, Jr. of
MULLEN COUGHLIN LLC

PTM:bwt
Enclosure

Exhibit *A*

<<DATE>>

<<First Name>> <<Middle Name>> <<Last Name>>

<<Address 1>>

<<Address 2>>

<<City>>, <<State >> <<Zip Code>>

RE: Notice of Data Incident

Dear <<First Name>> <<Middle Name>> <<Last Name>> ,

IBERIABANK is writing, at the request of Ametros Financial Corporation (“Ametros”), to notify you of a security incident affecting one of IBERIABANK’s service providers, Technology Management Resources, Inc. (“TMR”). Ametros has a lockbox service with IBERIABANK for collecting and processing payments from its customers. IBERIABANK uses TMR as a third-party lockbox service provider to process payments and capture pertinent payment data for items received in the lockbox. You made a payment or submitted information to Ametros’ IBERIABANK lockbox. TMR recently provided notice to IBERIABANK of an incident which may have involved your protected health information. IBERIABANK subsequently reported this incident to Ametros. Please note this incident did not involve unauthorized access to Ametros’ systems. This correspondence is intended to provide you with information regarding the incident and the resources available to you to help protect your information, should you feel it appropriate to do so.

What happened? On October 14, 2021, TMR identified unusual activity with a user account in its lockbox application. It was determined that the activity was unauthorized, and the account was promptly disabled. TMR investigated the incident and reported that the unauthorized activity occurred between October 12, 2021, and October 14, 2021. According to TMR’s investigation, an unauthorized party accessed bytes that were associated with certain images for lockbox payments and related documents. TMR has stated that the bytes (bits of computer data) accessed by the unauthorized party were in binary format only and as an encoded string (this means that the data was an encoded series of information stored in the form of ones and zeros). Technical manipulation of the bytes would be required to convert them into images. We are unaware that actual images were viewed by the unauthorized party during the period of unauthorized access. TMR has advised that it is likely that these bytes were obtained by the unauthorized party based upon traffic to the IP address. TMR’s investigation has not revealed any evidence to confirm that unauthorized party converted the bytes into images, although this could have been possible.

What information was involved? According to TMR, the encoded data was associated with certain check images and related documents within TMR’s client payment application (iRemit) that may have contained protected health information. Specifically, the information potentially involved may have included your name, [Data Elements].

What is IBERIABANK doing in response? IBERIABANK takes the protection and proper use of personal information provided to us very seriously. As part of our ongoing commitment to information privacy and the security of information, we are notifying you of this incident. Although we are not aware of any misuse of your information as a result of this incident, out of an abundance of caution, we are offering you complimentary credit monitoring and identity theft protection through TransUnion. These services will be

available to you for twelve (12) months at no cost in order to give you peace of mind. You must complete the enrollment steps listed in this letter to activate these services. We are also reviewing all relevant business practices regarding the security of information maintained by TMR.

What you can do. As a best practice, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your financial account statements, Explanation of Benefits, and to monitor your credit reports for suspicious activity. We encourage you to review the attached “Steps You Can Take to Protect Your Personal Information” which includes additional information and resources to assist you in protecting your personal information, should you feel it appropriate to do so. We also encourage you to enroll in the complimentary credit monitoring and identity theft protection services we are making available to you.

For more information. If you have additional questions about the 2021 lockbox service provider security incident or the protections available to you, please call [Number], toll-free, Monday through Friday, 9:00 a.m. – 9:00 p.m. Eastern Time. We apologize for any inconvenience this 2021 lockbox service provider security incident may have caused you. You may also write to Ametros at 200 Ballardvale Street, Suite 200 P.O. Box 827 Wilmington, MA 01887.

Sincerely,

[Name]

[Title]

IBERIABANK

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Enroll in Credit Monitoring

We are providing you with access to Single Bureau Credit Monitoring services at no charge. Services are for 12 months from the date of enrollment. When changes occur to your TransUnion credit file, notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud, you will also have access to identity protection support. In order for you to receive the monitoring service described above, you must enroll within 90 days from the date of this letter.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to www.mytrueidentity.com and follow the instructions provided. When prompted please provide the following unique code to receive services: <CODE HERE>. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

Monitor Your Accounts and Order Your Free Annual Credit Reports

In addition to enrolling in the complimentary credit monitoring services above, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your financial account statements, debit/credit card statements, and other statements, and to monitor your credit reports for suspicious activity to detect errors. (For Oregon and Iowa residents: Report any suspected identity theft to law enforcement, the Federal Trade Commission and your State Attorney General). Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus to request a free copy of your report. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the three consumer reporting agencies directly to obtain such additional reports). Periodically review a copy of your credit report for discrepancies and identify any accounts you did not open or inquiries you did not authorize.

Freeze Your Credit File

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place a security freeze on your credit report. Note that a security freeze generally does not apply to an existing creditor or its agents or affiliates for certain types of account review, collection, fraud Control or similar activities. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	TransUnion	Equifax
P.O. Box 9554 Allen, TX 75013	P.O. Box 160 Woodlyn, PA 19094	P.O. Box 105788 Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com	www.transunion.com	www.equifax.com

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report or complaint to a law enforcement agency concerning identity theft.

If you request a security freeze via toll-free telephone or other secure electronic means, the credit reporting agencies have one (1) business day after receiving the request to place the freeze. In the case of a request made by mail, the bureaus have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving a request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving the request to remove the freeze.

Place Fraud Alerts on Your Credit File

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon

seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should you wish to place a fraud alert, please contact any one of the consumer reporting agencies listed above to activate an alert.

File or Obtain a Police Report

You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission (FTC) can be reached at 600 Pennsylvania Avenue NW, Washington, D.C. 20580, by phone at 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261, or by going to www.ftc.gov/idtheft. The FTC encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file a complaint through the above-referenced contact information.

You also have rights under the federal Fair Credit Reporting Act (FCRA), which promotes the accuracy, fairness and privacy of information in the files of consumer reporting agencies. These rights include the right to receive a copy of your credit report, the right to ask for a credit score, the right to dispute incomplete or inaccurate information, and the right to obtain corrections to your report or delete inaccurate, incomplete, unverifiable information. Consumer reporting agencies may not report outdated negative information. Access to your file is limited, and you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you receive based upon information in your credit report. You may have additional rights under the FCRA not summarized here. We recommend and encourage you to review your rights pursuant to the FCRA at https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Avenue N.W., Washington D.C., 20580.

For residents of North Carolina: The North Carolina Office of the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226, and www.ncdoj.com. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For residents of Maryland: The Maryland Office of the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us. You can obtain information from the Attorney General or Federal Trade Commission about preventing identity theft.

For residents of New Mexico: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your

credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Furthermore, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccuracies, incomplete or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For residents of New York: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

For residents of Rhode Island: The Rhode Island Office of the Attorney General can be contacted at: 150 South Main Street, Providence, RI 02903, 1-401-274-4400 and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed regarding this incident. There are [X] Rhode Island residents impacted by this incident.

For residents of the District of Columbia: The Attorney General may be contacted at: 400 6th Street NW, Washington, D.C. 20001, 1-(202) 727-3400 and <https://oag.dc.gov/>. You may obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

Exhibit B

<<DATE>>

<<First Name>> <<Middle Name>> <<Last Name>>

<<Address 1>>

<<Address 2>>

<<City>>, <<State >> <<Zip Code>>

RE: Notice of Data Incident

Dear <<First Name>> <<Middle Name>> <<Last Name>> ,

IBERIABANK is writing, at the request of Ametros Financial Corporation (“Ametros”), to notify you of a security incident affecting one of IBERIABANK’s service providers, Technology Management Resources, Inc. (“TMR”). Ametros has a lockbox service with IBERIABANK for collecting and processing payments from its customers. IBERIABANK uses TMR as a third-party lockbox service provider to process payments and capture pertinent payment data for items received in the lockbox. You made a payment or submitted information to Ametros’ IBERIABANK lockbox. TMR recently provided notice to IBERIABANK of an incident which may have involved your protected health information. IBERIABANK subsequently reported this incident to Ametros. Please note this incident did not involve unauthorized access to Ametros’ systems. This correspondence is intended to provide you with information regarding the incident and the resources available to you to help protect your information, should you feel it appropriate to do so.

What happened? On October 14, 2021, TMR identified unusual activity with a user account in its lockbox application. It was determined that the activity was unauthorized, and the account was promptly disabled. TMR investigated the incident and reported that the unauthorized activity occurred between October 12, 2021, and October 14, 2021. According to TMR’s investigation, an unauthorized party accessed bytes that were associated with certain images for lockbox payments and related documents. TMR has stated that the bytes (bits of computer data) accessed by the unauthorized party were in binary format only and as an encoded string (this means that the data was an encoded series of information stored in the form of ones and zeros). Technical manipulation of the bytes would be required to convert them into images. We are unaware that actual images were viewed by the unauthorized party during the period of unauthorized access. TMR has advised that it is likely that these bytes were obtained by the unauthorized party based upon traffic to the IP address. TMR’s investigation has not revealed any evidence to confirm that unauthorized party converted the bytes into images, although this could have been possible.

What information was involved? According to TMR, the encoded data was associated with certain check images and related documents within TMR’s client payment application (iRemit) that may have contained protected health information. Specifically, the information potentially involved may have included your name, [Data Elements].

What is IBERIABANK doing in response? IBERIABANK takes the protection and proper use of personal information provided to us very seriously. As part of our ongoing commitment to information privacy and the security of information, we are notifying you of this incident. Although we are not aware of any misuse of your information as a result of this incident, out of an abundance of caution, we are offering you complimentary credit monitoring and identity theft protection through TransUnion. These services will be

available to you for twelve (12) months at no cost in order to give you peace of mind. You must complete the enrollment steps listed in this letter to activate these services. We are also reviewing all relevant business practices regarding the security of information maintained by TMR.

What you can do. As a best practice, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your financial account statements, Explanation of Benefits, and to monitor your credit reports for suspicious activity. We encourage you to review the attached “Steps You Can Take to Protect Your Personal Information” which includes additional information and resources to assist you in protecting your personal information, should you feel it appropriate to do so. We also encourage you to enroll in the complimentary credit monitoring and identity theft protection services we are making available to you.

For more information. If you have additional questions about the 2021 lockbox service provider security incident or the protections available to you, please call [Number], toll-free, Monday through Friday, 9:00 a.m. – 9:00 p.m. Eastern Time. We apologize for any inconvenience this 2021 lockbox service provider security incident may have caused you. You may also write to Ametros at 200 Ballardvale Street, Suite 200 P.O. Box 827 Wilmington, MA 01887.

Sincerely,

[Name]

[Title]

IBERIABANK

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Enroll in Credit Monitoring

We are providing you with access to Single Bureau Credit Monitoring services at no charge. Services are for 12 months from the date of enrollment. When changes occur to your TransUnion credit file, notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud, you will also have access to identity protection support. In order for you to receive the monitoring service described above, you must enroll within 90 days from the date of this letter.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to www.mytrueidentity.com and follow the instructions provided. When prompted please provide the following unique code to receive services: <CODE HERE>. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

Monitor Your Accounts and Order Your Free Annual Credit Reports

In addition to enrolling in the complimentary credit monitoring services above, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your financial account statements, debit/credit card statements, and other statements, and to monitor your credit reports for suspicious activity to detect errors. (For Oregon and Iowa residents: Report any suspected identity theft to law enforcement, the Federal Trade Commission and your State Attorney General). Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus to request a free copy of your report. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the three consumer reporting agencies directly to obtain such additional reports). Periodically review a copy of your credit report for discrepancies and identify any accounts you did not open or inquiries you did not authorize.

Freeze Your Credit File

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place a security freeze on your credit report. Note that a security freeze generally does not apply to an existing creditor or its agents or affiliates for certain types of account review, collection, fraud Control or similar activities. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	TransUnion	Equifax
P.O. Box 9554 Allen, TX 75013	P.O. Box 160 Woodlyn, PA 19094	P.O. Box 105788 Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com	www.transunion.com	www.equifax.com

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report or complaint to a law enforcement agency concerning identity theft.

If you request a security freeze via toll-free telephone or other secure electronic means, the credit reporting agencies have one (1) business day after receiving the request to place the freeze. In the case of a request made by mail, the bureaus have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving a request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving the request to remove the freeze.

Place Fraud Alerts on Your Credit File

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon

seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should you wish to place a fraud alert, please contact any one of the consumer reporting agencies listed above to activate an alert.

File or Obtain a Police Report

You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission (FTC) can be reached at 600 Pennsylvania Avenue NW, Washington, D.C. 20580, by phone at 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261, or by going to www.ftc.gov/idtheft. The FTC encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file a complaint through the above-referenced contact information.

You also have rights under the federal Fair Credit Reporting Act (FCRA), which promotes the accuracy, fairness and privacy of information in the files of consumer reporting agencies. These rights include the right to receive a copy of your credit report, the right to ask for a credit score, the right to dispute incomplete or inaccurate information, and the right to obtain corrections to your report or delete inaccurate, incomplete, unverifiable information. Consumer reporting agencies may not report outdated negative information. Access to your file is limited, and you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you receive based upon information in your credit report. You may have additional rights under the FCRA not summarized here. We recommend and encourage you to review your rights pursuant to the FCRA at https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Avenue N.W., Washington D.C., 20580.

For residents of North Carolina: The North Carolina Office of the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226, and www.ncdoj.com. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For residents of Maryland: The Maryland Office of the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us. You can obtain information from the Attorney General or Federal Trade Commission about preventing identity theft.

For residents of New Mexico: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your

credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Furthermore, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccuracies, incomplete or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For residents of New York: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

For residents of Rhode Island: The Rhode Island Office of the Attorney General can be contacted at: 150 South Main Street, Providence, RI 02903, 1-401-274-4400 and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed regarding this incident. There are [X] Rhode Island residents impacted by this incident.

For residents of the District of Columbia: The Attorney General may be contacted at: 400 6th Street NW, Washington, D.C. 20001, 1-(202) 727-3400 and <https://oag.dc.gov/>. You may obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.