WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

December 15, 2020

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Online Submission

Attorney General Aaron Frey
Attorney General's Office
Office of Attorney General
6 State House Station
Augusta, ME 04333

Re: Data Security Incident
Client: Central Florida Cardiology Group
File No.: 15991.00832

Dear Attorney General Frey,

We represent Central Florida Cardiology Group ("CFCG") a private practice that treats cardiology conditions with multiple locations throughout the state of Florida. CFCG was notified by one of its vendors, IBERIABANK, about a data security incident affecting one of IBERIABANK's service providers, Technology Management Resources, Inc. ("TMR").

1. Nature of the incident.

Central Florida Cardiology Group ("CFCG") was notified by one of its vendors, IBERIABANK, on October 8, 2020 about a data security incident affecting one of its service providers, Technology Management Resources, Inc. ("TMR"). CFCG has a lockbox service with IBERIABANK for collecting and processing payments from its customers and/or patients. IBERIABANK uses TMR as a third-party lockbox service provider to process payments and capture pertinent payment data for items received in the lockbox. This incident did not affect CFCG's internal computer systems. On July 3, 2020, TMR discovered that a TMR employee's user account had been compromised. Upon discovery of the incident, TMR reported that they secured the account and began an investigation in consultation with external cybersecurity professionals. TMR has stated that their investigation determined that the threat actor may have viewed images of checks and related images containing potential Protected Health Information (PHI) related to customers of the Company.

According to TMR, their investigation concluded that the information potentially involved may have included patients' names, health information, banking information and Explanation of Benefits information, this includes provider name, treatment information, patient account number, and other information, mostly related to insurance/billing.

2. **Number of Maine residents affected.**

Two (2) Maine residents were potentially affected by this incident. Incident notification letters addressed to those individuals was mailed out on December 11, 2020 via First Class Mail. A sample copy of the Incident notification letters mailed to potentially affected residents of Maine is included with this letter at **Exhibit A**.

3. **Steps taken.**

At this time, there is no evidence that any information has been misused as a result of this incident. CFCG takes the security of all the information in its control very seriously, and is taking steps to prevent a similar event from occurring in the future.

IBERIABANK is offering complimentary credit monitoring to the affected individuals. TMR reports that they have taken several corrective actions to remediate the security incident, prevent a further security incident, and mitigate the effects of the security incident. According to TMR, TMR credentials have been reset or deactivated (as applicable). TMR also reports that they implemented additional rules in their firewall to more tightly control the ability to access the iRemit website from other countries, among other steps taken.

4. **Contact information.**

CFCG remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

Enclosure

EXHIBIT A

IBERIABANK Notification Letter Template for PII

This is an example of the form letter that IBERIABANK will send to your customers identified on the PII data file on your behalf if you request that IBERIABANK notify your customers regarding this incident. Please note that this letter is representative only and is subject to change in IBERIABANK's sole discretion. We are not able to negotiate changes as the language in the letter is intended to comply with various requirements of consumer notification laws and accommodating potential revisions could result in a delay in IBERIABANK making notifications.

The provision of this letter does not constitute legal advice on any particular facts or circumstances. Please consult with your organization's legal counsel to determine which laws apply to you and what your responsibilities may be regarding the Technology Management Resources security incident.

<<DATE>>

<<First Name>> <<Middle Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip Code>>

RE: Notice of Technology Management Resources Security Incident

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

IBERIABANK is writing, at the request of <<Company Name>> (the "Company"), to notify you of a security incident affecting one of our service providers, Technology Management Resources, Inc. (TMR). The Company has a lockbox service with IBERIABANK for collecting and processing payments from its customers and/or patients. IBERIABANK uses TMR as a third-party lockbox service provider to process payments and capture pertinent payment data for items received in the lockbox. TMR recently provided notice of an incident which may have involved your personal information. Although this incident did not affect IBERIABANK's or the Company's internal computer systems, we wanted to provide you with information regarding TMR's incident and the resources available to you to help protect your information, should you feel it appropriate to do so.

What happened? On July 3, 2020, TMR discovered that a TMR employee's user account had been compromised. Upon discovery of the incident, TMR reported that they secured the account and began an investigation in consultation with external cybersecurity professionals. TMR has stated that their investigation determined that the threat actor may have viewed images of checks related to customers of the Company. According to TMR, the threat actor activity occurred between August 5, 2018 and May 31, 2020, with the bulk of the activity occurring between February and May 2020. TMR notified the FBI of this incident.

What information was involved? According to TMR, their investigation concluded that the threat actor potentially viewed certain check images within TMR's iRemit application that may have contained personally identifiable information. TMR reported that these images consisted of information included on checks such as name, address, account numbers, and bank routing number. This information is similar to that which appears on a check anytime an individual makes a purchase or pays a bill. Driver's

license numbers, Social Security numbers, or other personal information not typically contained on the face of a check have not been identified by TMR as being included in your data that was potentially impacted by this incident. Specifically, after completing e-discovery on these images, TMR concluded that the information potentially involved may have included your name, address, account number, and bank routing number.

What is IBERIABANK doing in response? We take the protection and proper use of personal information very seriously. As part of our ongoing commitment to information privacy and the security of information, we are notifying you of this incident. Although this incident in no way involved our internal security or computer systems, as a professional courtesy, we are offering you complementary credit monitoring and identity theft protection through CyberScout in order to give you peace of mind. You must complete the enrollment steps listed in this letter in order to activate these services. We are also reviewing all relevant business practices regarding the security of information maintained by TMR.

TMR reports that they have taken several corrective actions to remediate the security incident, prevent a further security incident, and mitigate the effects of the security incident. According to TMR, TMR credentials have been reset or deactivated (as applicable). TMR also reports that they implemented additional rules in their firewall to more tightly control the ability to access the iRemit website from other countries, among other steps taken.

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 and all claims information from your health insurance provider, and to monitor your credit reports for suspicious activity. We have included the attached "Steps You Can Take to Protect Personal Information", which you can implement as you deem appropriate. You may also enroll in the complementary credit monitoring and identity theft protection services we are making available to you as a professional courtesy and in an abundance of caution.

For more information. If you have additional questions about the Technology Management Resources security incident or the protections available to you, please call 1-888-905-0513, toll-free, Monday through Friday, 9:00 am – 9:00 pm Eastern Time. We apologize for any inconvenience this TMR security incident may have caused you.

Sincerely,

[Name]

[Title]

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Complimentary Credit Monitoring Services

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 Experian 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 remediation support from a CyberScout Fraud Investigator. 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 **https://www.myidmanager.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

In addition to enrolling in the complementary 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, 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.

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	P.O. Box 1000	P.O. Box 105788

Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-909-8872	1-800-685-1111
www.transunion.com	www.experian.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, II, 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.

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 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, DC 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 General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226, and www.ncdoj.com.

For residents of Maryland: The Maryland Office of the Attorney General can be contacted at 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

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.

IBERIABANK Notification Letter Template for PHI

This is an example of the form letter that IBERIABANK will send to your customers identified on the PHI data file on your behalf if you request that IBERIABANK notify your customers regarding this incident. Please note that this letter is representative only and is subject to change in IBERIABANK's sole discretion. We are not able to negotiate changes as the language in the letter is intended to comply with various requirements of consumer notification laws and accommodating potential revisions could result in a delay in IBERIABANK making notifications.

The provision of this letter does not constitute legal advice on any particular facts or circumstances. Please consult with your organization's legal counsel to determine which laws apply to you and what your responsibilities may be regarding the Technology Management Resources security incident.

<<DATE>>

<<First Name>> <<Middle Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip Code>>

RE: Notice of Technology Management Resources Security Incident

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

IBERIABANK is writing, at the request of <<Company Name>> (the "Company"), to notify you of a security incident affecting one of our service providers, Technology Management Resources, Inc. (TMR). The Company has a lockbox service with IBERIABANK for collecting and processing payments from its customers and/or patients. IBERIABANK uses TMR as a third-party lockbox service provider to process payments and capture pertinent payment data for items received in the lockbox. TMR recently provided notice of an incident which may have involved your protected health information. Although this incident did not affect IBERIABANK's or the Company's internal computer systems, we wanted to provide you with information regarding TMR's incident and the resources available to you to help protect your information, should you feel it appropriate to do so.

What happened? On July 3, 2020, TMR discovered that a TMR employee's user account had been compromised. Upon discovery of the incident, TMR reported that they secured the account and began an investigation in consultation with external cybersecurity professionals. TMR has stated that their investigation determined that the threat actor may have viewed images of checks and related images containing potential Protected Health Information (PHI) related to customers of the Company. According to TMR, the threat actor activity occurred between August 5, 2018 and May 31, 2020, with the bulk of the activity occurring between February and May 2020. TMR notified the FBI of this incident.

What information was involved? According to TMR, their investigation concluded that the threat actor potentially viewed images within TMR's iRemit application that may have contained PHI. Specifically, after completing e-discovery on these images, TMR concluded that the information potentially involved may have included your name and <<DATA ELEMENTS>>.

What is IBERIABANK doing in response? We take the protection and proper use of personal information very seriously. As part of our ongoing commitment to information privacy and the security of information, we are notifying you of this incident. Although this incident in no way involved our internal security or computer systems, as a professional courtesy, we are offering you complementary credit monitoring and identity theft protection through CyberScout in order to give you peace of mind. You must complete the enrollment steps listed in this letter in order to activate these services. We are also reviewing all relevant business practices regarding the security of information maintained by TMR.

TMR reports that they have taken several corrective actions to remediate the security incident, prevent a further security incident, and mitigate the effects of the security incident. According to TMR, TMR credentials have been reset or deactivated (as applicable). TMR also reports that they implemented additional rules in their firewall to more tightly control the ability to access the iRemit website from other countries, among other steps taken.

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 and all claims information from your health insurance provider, and to monitor your credit reports for suspicious activity. We have included the attached "Steps You Can Take to Protect Personal Information", which you can implement as you deem appropriate. You may also enroll in the complementary credit monitoring and identity theft protection services we are making available to you as a professional courtesy and in an abundance of caution.

For more information. If you have additional questions about the Technology Management Resources security incident or the protections available to you, please call 1-888-905-0513, toll-free, Monday through Friday, 9:00 am – 9:00 pm Eastern Time. We apologize for any inconvenience this TMR security incident may have caused you.

Sincerely,

[Name]

[Title]

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Complimentary Credit Monitoring Services

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 Experian 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 remediation support from a CyberScout Fraud Investigator. 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 **https://www.myidmanager.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

In addition to enrolling in the complementary 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, 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.

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	P.O. Box 1000	P.O. Box 105788

Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-909-8872	1-800-685-1111
www.transunion.com	www.experian.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, II, 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.

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 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, DC 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 General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226, and www.ncdoj.com.

For residents of Maryland: The Maryland Office of the Attorney General can be contacted at 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

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.

Customer Notification Letter Template for PII

This form letter may be used in circumstances where customer notifications are required for personally identifiable information (PII). Please note that this template is designed to assist in preparing notification letters for potentially affected individuals in connection with state consumer notification requirements. It must be tailored to reflect your company's particular circumstances and to address specific state law requirements, and to account for industry-specific federal or state legal requirements (such as HIPAA, etc.).

The provision of this template does not constitute legal advice on any particular facts or circumstances. Please consult with your organization's legal counsel to determine which laws apply to you and what your responsibilities may be regarding the Technology Management Resources security incident.

[Insert Date]

[Insert mailing address (if law requires notification by first class postal mail) or email address (if law permits notification by email)]

RE: Notice of Technology Management Resources Security Incident

Dear [Name],

We are writing to inform you of a security incident affecting one of our service providers that may have involved your personal information. [Company name] (the "Company") takes the protection and proper use of your information very seriously. Accordingly, although this incident did not affect the Company's internal computer systems, we wanted to provide you with information regarding the service provider incident and resources available to you to help protect your information, should you feel it appropriate to do so.

What happened? The Company has a lockbox service with IBERIABANK for collecting and processing payments from our patients and/or customers. IBERIABANK uses Technology Management Resources, Inc. (TMR) as a third-party lockbox service provider to process payments and capture pertinent payment data for items received in the lockbox. On July 3, 2020, TMR discovered that a TMR employee's user account had been compromised. The Company was notified of this incident on [insert date Company was notified by IBERIABANK] and has been actively seeking information regarding the incident to be able to provide this notice to you.

Upon discovery of the incident, TMR reported that they secured the account and began an investigation in consultation with external cybersecurity professionals. TMR has stated that their investigation determined that the threat actor may have viewed images of checks related to customers of the Company. According to TMR, the threat actor activity occurred between August 5, 2018 and May 31, 2020, with the bulk of the activity occurring between February and May 2020. TMR notified the FBI of this incident.

What information was involved? According to TMR, their investigation concluded that the threat actor potentially viewed certain check images within TMR's iRemit application that may have contained personally identifiable information. These images consisted of information traditionally included on the

front of checks such as name, address, account numbers, and bank routing numbers. This information is similar to that which appears on a check anytime an individual makes a purchase or pays a bill. Driver's license numbers, Social Security numbers, or other personal information not typically contained on the face of a check have not been identified by TMR as being was included in your data that was potentially impacted by this incident. Specifically, after completing e-discovery on these images, TMR concluded that the information potentially involved may have included your name, address, account number, and bank routing number.

What is the Company doing in response? As part of our ongoing commitment to information privacy and the security of information, we are notifying you of this incident. Additionally, although this incident in no way involved the Company's nor IBERIABANK internal security or computer systems, as a professional courtesy, IBERIABANK is offering you credit monitoring and identity theft protection through CyberScout in order to give you peace of mind. You must complete the enrollment steps listed in this letter in order to activate these services.

TMR reports that they have taken several corrective actions to remediate the security incident, prevent a further security incident, and mitigate the effects of the security incident. According to TMR, TMR credentials have been reset or deactivated (as applicable). TMR also reports that they implemented additional rules in their firewall to more tightly control the ability to access the iRemit website from other countries, among other steps taken.

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 and claims information from your health insurance provider, and to monitor your credit reports for suspicious activity. We have included the attached "Steps You Can Take to Protect Personal Information", which you can implement as you deem appropriate. You may also enroll in the credit monitoring and identity theft protection services available to you through CyberScout. These services are being offered in an abundance of caution and as a professional courtesy to you.

For more information. If you have additional questions about the Technology Management Resources security incident or the protections available to you, please call 1-888-905-0513, toll-free, Monday through Friday, 9:00 am – 9:00 pm Eastern Time. We apologize for any inconvenience this Technology Management Resources security incident may have caused you.

Sincerely,

[Name]

[Title]

[Organization]

Customer Notification Letter Template for PHI

This form letter may be used in circumstances where customer notifications are required for PHI. Please note that this template is designed to assist in preparing notification letters for potentially affected individuals in connection with state consumer notification requirements. It must be tailored to reflect your company's particular circumstances and to address specific state law requirements, and to account for industry-specific federal or state legal requirements (such as HIPAA, etc.).

The provision of this template does not constitute legal advice on any particular facts or circumstances. Please consult with your organization's legal counsel to determine which laws apply to you and what your responsibilities may be regarding the Technology Management Resources security incident.

[Insert Date]

[Insert mailing address (if law requires notification by first class postal mail) or email address (if law permits notification by email)]

RE: Notice of Technology Management Resources Security Incident

Dear [Name],

We are writing to inform you of a security incident affecting one of our service providers that may have involved your protected health information. [Company name] (the "Company") takes the protection and proper use of your information very seriously. Accordingly, although this incident did not affect the Company's internal computer systems, we wanted to provide you with information regarding the service provider incident and resources available to you to help protect your information, should you feel it appropriate to do so.

What happened? The Company has a lockbox service with IBERIABANK for collecting and processing payments from our patients and/or customers. IBERIABANK uses Technology Management Resources, Inc. (TMR) as a third-party lockbox service provider to process payments and capture pertinent payment data for items received in the lockbox. On July 3, 2020, TMR discovered that a TMR employee's user account had been compromised. The Company was notified of this incident on [insert date Company was notified by IBERIABANK] and has been actively seeking information regarding the incident to be able to provide this notice to you.

Upon discovery of the incident, TMR reported that they secured the account and began an investigation in consultation with external cybersecurity professionals. TMR has stated that their investigation determined that the threat actor may have viewed images of checks and related images containing potential Protected Health Information (PHI) related to customers of the Company. According to TMR, the threat actor activity occurred between August 5, 2018 and May 31, 2020, with the bulk of the activity occurring between February and May 2020. TMR notified the FBI of this incident.

What information was involved? According to TMR, their investigation concluded that the threat actor potentially viewed images within TMR's iRemit application that may have contained PHI. Specifically, after completing e-discovery on these images, TMR concluded that the information potentially involved may have included your name and <<DATA ELEMENTS>>.

What is the Company doing in response? As part of our ongoing commitment to information privacy and the security of information, we are notifying you of this incident. Additionally, although this incident in no way involved the Company's nor IBERIABANK internal security or computer systems, as a professional courtesy, IBERIABANK is offering you credit monitoring and identity theft protection through CyberScout in order to give you peace of mind. You must complete the enrollment steps listed in this letter in order to activate these services.

TMR reports that they have taken several corrective actions to remediate the security incident, prevent a further security incident, and mitigate the effects of the security incident. According to TMR, TMR credentials have been reset or deactivated (as applicable). TMR also reports that they implemented additional rules in their firewall to more tightly control the ability to access the iRemit website from other countries, among other steps taken.

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 and claims information from your health insurance provider, and to monitor your credit reports for suspicious activity. We have included the attached "Steps You Can Take to Protect Personal Information", which you can implement as you deem appropriate. You may also enroll in the credit monitoring and identity theft protection services available to you through CyberScout. These services are being offered in an abundance of caution and as a professional courtesy to you.

For more information. If you have additional questions about the Technology Management Resources security incident or the protections available to you, please call 1-888-905-0513, toll-free, Monday through Friday, 9:00 am – 9:00 pm Eastern Time. We apologize for any inconvenience this Technology Management Resources security incident may have caused you.

Sincerely,

[Name]

[Title]

[Organization]

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Complimentary Credit Monitoring Services

IBERIABANK is 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 Experian 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 remediation support from a CyberScout Fraud Investigator. 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 **https://www.myidmanager.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

In addition to enrolling in the complementary 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, 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.

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	P.O. Box 1000	P.O. Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348

1-888-397-3742	1-800-909-8872	1-800-685-1111
www.transunion.com	www.experian.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, II, 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.

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 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, DC 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 General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226, and www.ncdoj.com.

For residents of Maryland: The Maryland Office of the Attorney General can be contacted at 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

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.