Clark Hill

Richard Halm
T (312)985-5564
F (312)985-5952
Email:rhalm@clarkhill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

January 30, 2025

VIA ELECTRONIC MAIL

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Dear Attorney General Brown:

We represent Bankers Cooperative Group, Inc. ("BCG") with respect to a data security incident involving personal information described below. BCG is a business associate as defined under the Health Insurance Portability and Accountability Act ("HIPAA"). BCG suffered a data security incident impacting health insurance information of certain covered entities. BCG takes the security of the information in its control seriously and is committed to answering any questions you may have about the data security incident its response, and steps taken to prevent a similar incident from occurring in the future.

1. **Nature of security incident.**

BCG assists banking institutions in obtaining insurance coverage for their employees. On August 13, 2024, BCG identified suspicious activity associated with one employee email account. BCG immediately implemented its incident response protocols, disabled the email account, and began an internal investigation. BCG, through counsel, engaged external computer forensic specialists to assist with determining what occurred and whether any data was at risk. This investigation concluded on August 28, 2024, at which time a vendor began to review of the contents of the email account to identify potentially impacted individuals and data elements and BCG had to supplement these results with mailing addresses. This was completed on January 17, 2025. Notice was provided to individuals and potentially impacted information includes name, address date of birth, Social Security number, and health insurance information. There is no evidence of unauthorized access to any emails in the affected email account, nor is BCG aware of misuse of any information.

2. **Number of residents affected.**

One (1) Maryland individual was notified of the incident on behalf of a covered entity. A notification letter was sent to the potentially affected individuals on January 30, 2025 (a copy of the form notification letter is enclosed as Exhibit A).

3. Steps taken in response to the incident.

Since this incident, BCG reset passwords and retrained all employees on recognizing and responding to suspicious emails. Email accounts have multifactor authentication enabled, and all employees are required to take cybersecurity training on a yearly basis. Additional security features have been enabled to further enhance the security of BCG's systems. Additionally, potentially affected individuals were offered 12 months of credit monitoring and identity protection services through Experian at no cost.

4. Contact Information

BCG takes the security of the information in its control seriously and is committed to ensuring it is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me rhalm@clarkhill.com or (312) 985-5564.

Sincerely,

CLARK HILL

Richard Halm
Senior Attorney

cc: Mariah Leffingwell – mleffingwell@clarkhill.com

BCG

EMPLOYEE BENEFITS

Return Mail Processing
PO Box 999
Suwanee, GA 30024

28 1 8777 ************************************SNGLP
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

January 30, 2025

Dear Sample A. Sample:

We wanted to let you know about a data security incident that may have impacted your personal information. Bankers Cooperative Group ("BCG") may have been provided your information by your current or former employer to obtain insurance coverage. BCG may also have your information if you were listed as a dependent of an employee. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

What Happened?

On August 13, 2024, we discovered suspicious activity associated with one employee email account. We immediately implemented our incident response protocols, disabled the email account, and, through counsel, engaged independent computer forensic experts to assist with an investigation into the incident. This investigation sought to help us determine what had occurred, and whether any information was at risk. The forensic investigation concluded on August 28, 2024, and determined that there were some emails within the impacted email account may have been accessible to the unauthorized actor. A third party was engaged to review these emails and on November 15, 2024, determined that some of your personal information may have been contained in those emails. After we learned this, we notified your current or former employer your information was potentially impacted and arranged for you to receive credit monitoring and identity protection services. While there is no evidence that the emails potentially containing your information were accessed and we are not aware of any misuse of your information, we wanted to inform you of this incident and provide you with resources to protect your information.

What Information Was Involved?

The potentially impacted information includes your name, address, and the following: [Extra3].

What We Are Doing:

We want to assure you that we are taking steps to prevent a similar incident from happening in the future. Email accounts have multifactor authentication enabled, and all employees are required to take cybersecurity training on a yearly basis. Since this incident, BCG reset passwords and retrained all employees on recognizing and responding to suspicious emails. Additional security features have been enabled to further enhance the security of BCG systems. In addition, while we are not aware of any misuse of your information, we have arranged for you to receive credit monitoring and identity protection services at no cost to you through Experian for [Extra1] months.

What You Can Do:

Again, at this time, there is no evidence that your information has been misused. However, we strongly encourage you to take full advantage of this service offering. Experian representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your information. We also encourage you to remain vigilant against incidents of identity theft by reviewing bank accounts and other financial statements. More information on how to protect your identity can be found on the following pages.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for [Extra1] months. If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [Extra1] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [Extra1]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by April 23, 2025 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your activation code: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-833-918-5956 by April 23, 2025 (5:59 UTC). Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

For More Information:

If you have any questions or concerns, please call 1-833-918-5956, Monday through Friday from 9 am - 9 pm Eastern Time, excluding holidays. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you

Sincerely,

Bankers Cooperative Group, Inc.

Recommended Steps to help Protect your Information

1. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever 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 some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

2. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well.

You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

4. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: 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. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, 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 a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can 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.

New York Residents: 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/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. A total of 1 Rhode Island resident was notified of this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

BCG
EMPLOYEE BENEFITS

Return Mail Processing
PO Box 999
Suwanee, GA 30024

28 1 8766 ************************************SNGLP
SAMPLE A. SAMPLE - L02
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

January 30, 2025

Dear Sample A. Sample:

We wanted to let you know about a data security incident that may have impacted your personal information. Bankers Cooperative Group ("BCG") is a third party service provider to (i) your current or former employer; or (ii) the current or former employer of your health care benefits policy holder and may have been provided your information to obtain health insurance. This data security incident occurred solely within BCG's email system and not within any systems of your current or former employer. Furthermore, this data security incident had no impact on your employer or former employer's systems and was not the result of any action or inaction on their part. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

What Happened?

On August 13, 2024, we discovered suspicious activity associated with one BCG employee email account. We immediately implemented our incident response protocols, disabled the email account, and, through counsel, engaged independent computer forensic experts to assist with an investigation into the incident. This investigation sought to help us determine what had occurred, and whether any information was at risk. The forensic investigation concluded on August 28, 2024, and determined that there were some emails within the impacted email account may have been accessible to the unauthorized actor. A third party was engaged to review these emails and on November 15, 2024, determined that some of your personal information may have been contained in those emails. After we learned this, we notified your current or former employer on December 13, 2024, that your information was potentially impacted and arranged for you to receive credit monitoring and identity protection services. While there is no evidence that the emails potentially containing your information were accessed and we are not aware of any misuse of your information, we wanted to inform you of this incident and provide you with resources to protect your information.

What Information Was Involved?

The potentially impacted information includes your name, address, and the following: [Extra3].

What We Are Doing:

We want to assure you that we are taking steps to prevent a similar incident from happening in the future. Email accounts have multifactor authentication enabled, and all employees are required to take cybersecurity training on a yearly basis. Since this incident, BCG reset passwords and retrained all employees on recognizing and responding to suspicious emails. Additional security features have been enabled to further enhance the security of BCG systems. In addition, while we are not aware of any misuse of your information, we have arranged for you to receive credit monitoring and identity protection services at no cost to you through Experian for [Extra1] months.

What You Can Do:

Again, at this time, there is no evidence that your information has been misused. However, we strongly encourage you to take full advantage of this service offering. Experian representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your information. We also encourage you to remain vigilant against incidents of identity theft by reviewing bank accounts and other financial statements. More information on how to protect your identity can be found on the following pages.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for [Extra1] months. If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [Extra1] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [Extra1]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by April 23, 2025 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your activation code: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-833-918-5956 by April 23, 2025 (5:59 UTC). Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

For More Information:

If you have any questions or concerns, please call 1-833-918-5956, Monday through Friday from 9 am - 9 pm Eastern Time, excluding holidays. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you

Sincerely,

Bankers Cooperative Group, Inc.

Recommended Steps to help Protect your Information

1. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever 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 some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

2. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well.

You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

4. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: 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. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, 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 a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can 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.

New York Residents: 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/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. A total of 1 Rhode Island resident was notified of this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.