



June 19, 2024

Via email to: idtheft@oag.state.md.us

Office of the Attorney General
St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202

RE: FCCI Insurance Group – Notice of Security Incident

Dear Sir/Madam:

FCCI Insurance Group, a group of insurers with its lead domicile state in Florida,¹ is writing to inform you that FCCI suffered a security incident and determined on June 5, 2024, that the incident involved potential unauthorized access to four Maryland residents' personal information. This incident was the result of unauthorized access to a limited number of FCCI's email accounts.

Investigation

In early February 2024, we detected suspicious email activity coming from FCCI email accounts. We promptly engaged outside counsel and began working with third-party forensic experts to investigate. Those experts determined that a threat actor used a phishing attack to gain access to a small number of FCCI email accounts on December 5, 2023, and then from January 29 to February 2, 2024. With that access, the forensic experts determined that the threat actor (1) engaged in activity consistent with attempts to commit financial fraud by misdirecting payments and (2) did not download the account contents ("sync") to a local email client.

The forensic experts were also able to identify the potentially impacted emails. Once we received those findings, we promptly shared the emails with a data-review firm to determine what was in those files. The data-review firm provided us their results on April 30. We have been working diligently since then to assess our notification obligations and ensure we have accurate contact information for individuals

¹ FCCI Insurance Group is comprised of: National Trust Insurance Company (domiciled in Indiana); Monroe Guaranty Insurance Company (domiciled in Indiana); FCCI Commercial Insurance Company (domiciled in Florida); FCCI Insurance Company (domiciled in Florida); FCCI Advantage Insurance Company (domiciled in Florida); and Brierfield Insurance Company (domiciled in Mississippi).

requiring notice.

Potentially Affected Information

Having reviewed the data, we have reason to believe that the threat actor potentially acquired the personal information of four Maryland residents. The affected files contained information such as names, birthdates, contact information, Social Security numbers, driver's license numbers, and limited health details for our customers or those associated with their accounts. (But not all that information was necessarily affected for Maryland residents.) We currently have no reason to suspect this information was, or will be, misused.

Notification and Other Remediation

We are mailing notice to potentially affected individuals, including four Maryland residents, on June 21, 2024. In those notices, we are including free credit monitoring for individuals who may have had their government identification (such as a Social Security number) affected. I have attached copies of the notices we are sending to all impacted individuals—not just Maryland residents.

In addition to notifying affected individuals, we took multiple steps to bolster our security. This includes, among other measures: resetting passwords, resetting tokens, adding more access restrictions based on geographic location, restricting large email groups, and removing a link from our public website that employees could use to access our remote login.

Contact Us

If you have any questions, please contact Josh Hansen, our outside counsel for this incident. He can be reached via email at jahansen@shb.com or by phone at (303) 285-5306.

Sincerely,

A handwritten signature in cursive script that reads "Jessica Markun".

Jessica Markun
VP, Risk, Audit & Administrative Services



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<last_name>>

FCCI Insurance Group is writing to inform you of an incident involving potential unauthorized access to your information that we obtained in connection with insurance that we offer or provide to you or another person or business. Earlier this year, we detected an incident involving unauthorized access to a limited number of our emails. We promptly began investigating, and we recently determined some of your personal information was contained in those emails. FCCI Insurance Group is providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED

An unauthorized third party had access to a small number of our emails between December 2023 and February 2024. Once we discovered the unauthorized activity, we promptly began investigating. We identified the affected files and engaged a data-review firm to analyze their contents. We received those results in May and have been working since then to ensure we have accurate contact information for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED

Based on the investigation, we determined that the third party who accessed our systems was likely attempting to create fraudulent payment requests rather than gather information on individuals. But, in the course of doing so, the third party may have accessed emails that potentially included your name, contact information, date of birth, and government identification (such as a Social Security number or driver's license number) as well as limited health information. We collected this information in connection with insurance we offer or provide to you or another person or business.

WHAT WE ARE DOING

We hired third-party experts to address this situation, to perform an investigation into the unauthorized activity, and to further secure our systems.

WHAT YOU CAN DO

We currently have no evidence that the unauthorized third party has, or will, use this information to harm you. Nonetheless, we encourage you to remain vigilant for any signs of unauthorized financial activity. Please also review the next page for steps you can take to protect yourself against fraud and identity theft.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at [TFN](#), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

A handwritten signature in dark ink that reads "Jessica Markun". The script is cursive and fluid.

Jessica Markun
VP, Risk, Audit & Administrative Services

ADDITIONAL STEPS YOU CAN TAKE

Activate your complimentary credit monitoring – To help protect you from fraud or identity theft, we are offering a complimentary one-year membership to Experian's IdentityWorks. This product helps detect possible misuse of your personal information. To register, please:

- Ensure that you **enroll by:** <<b2b_text_6 (activation deadline)>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code:** <<activation code s_n>>

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at (877) 288-8057 by September 6, 2024, and provide them engagement number <<b2b_text_1 (engagement number)>>.

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov/databreach.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. A security freeze is free. You can obtain more information about them by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission

600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax

P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian

P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

Maryland

Attorney General

200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

New York

Attorney General

The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

North Carolina

Attorney General

9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

Washington, DC

Attorney General

400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<last_name>>

FCCI Insurance Group is writing to inform you of an incident involving potential unauthorized access to your information that we obtained in connection with insurance that we offer or provide to you or another person or business. Earlier this year, we detected an incident involving unauthorized access to a limited number of our emails. We promptly began investigating, and we recently determined some of your personal information was contained in those emails. FCCI Insurance Group is providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED

An unauthorized third party had access to a small number of our emails between December 2023 and February 2024. Once we discovered the unauthorized activity, we promptly began investigating. We identified the affected files and engaged a data-review firm to analyze their contents. We received those results in May and have been working since then to ensure we have accurate contact information for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED

Based on the investigation, we determined that the third party who accessed our systems was likely attempting to create fraudulent payment requests rather than gather information on individuals. But, in the course of doing so, the third party may have accessed emails that potentially included your name, contact information, date of birth, and government identification (such as a Social Security number or driver's license number). We collected this information in connection with insurance we offer or provide to you or another person or business.

WHAT WE ARE DOING

We hired third-party experts to address this situation, to perform an investigation into the unauthorized activity, and to further secure our systems.

WHAT YOU CAN DO

We currently have no evidence that the unauthorized third party has, or will, use this information to harm you. Nonetheless, we encourage you to remain vigilant for any signs of unauthorized financial activity. Please also review the next page for steps you can take to protect yourself against fraud and identity theft.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at [TFN](#), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

A handwritten signature in black ink that reads "Jessica Markun".

Jessica Markun
VP, Risk, Audit & Administrative Services

ADDITIONAL STEPS YOU CAN TAKE

Activate your complimentary credit monitoring – To help protect you from fraud or identity theft, we are offering a complimentary one-year membership to Experian's IdentityWorks. This product helps detect possible misuse of your personal information. To register, please:

- Ensure that you **enroll by:** <<b2b_text_6 (activation deadline)>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code:** <<activation code s_n>>

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at (877) 288-8057 by September 6, 2024, and provide them engagement number <<b2b_text_1 (engagement number)>>.

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov/databreach.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. There is no charge for requesting a security freeze. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission

600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax

P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian

P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

Maryland

Attorney General

200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

New York

Attorney General

The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

North Carolina

Attorney General

9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

Washington, DC

Attorney General

400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.

Review the Fair Credit Reporting Act – You also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit: <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<last_name>>

FCCI Insurance Group is writing to inform you of an incident involving potential unauthorized access to your information that we obtained in connection with insurance that we offer or provide to you or another person or business. Earlier this year, we detected an incident involving unauthorized access to a limited number of our emails. We promptly began investigating, and we recently determined some of your personal information was contained in those emails. FCCI Insurance Group is providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED

An unauthorized third party had access to a small number of our emails between December 2023 and February 2024. Once we discovered the unauthorized activity, we promptly began investigating. We identified the affected files and engaged a data-review firm to analyze their contents. We received those results in May and have been working since then to ensure we have accurate contact information for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED

Based on the investigation, we determined that the third party who accessed our systems was likely attempting to create fraudulent payment requests rather than gather information on individuals. But, in the course of doing so, the third party may have accessed emails that potentially included your name, date of birth, and contact information as well as limited health information about you. We collected this information in connection with insurance we offer or provide to you or another person or business.

WHAT WE ARE DOING

We hired third-party experts to address this situation, to perform an investigation into the unauthorized activity, and to further secure our systems.

WHAT YOU CAN DO

We currently have no evidence that the unauthorized third party has, or will, use this information to harm you. Nonetheless, we encourage you to remain vigilant for any signs of unauthorized financial activity. Please also review the next page for steps you can take to protect yourself against fraud and identity theft.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at [TFN](#), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

A handwritten signature in black ink that reads "Jessica Markun".

Jessica Markun
VP, Risk, Audit & Administrative Services

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov/databreach.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. There is no charge for requesting a security freeze. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission

600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax

P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian

P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

Maryland Attorney General

200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

New York Attorney General

The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

Washington, DC Attorney General

400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.



<<Date>> (Format: Month Day, Year)

Parent or Guardian of

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>

<<address_1>>

<<address_2>>

<<city>>, <<state_province>> <<postal_code>>

<<country>>

Notice of Data Breach

To the Parent or Guardian of <<first_name>> <<last_name>>,

FCCI Insurance Group is writing to inform you of an incident involving potential unauthorized access to your child's information that we obtained in connection with insurance that we offer or provide to you, your child, or another person or business. Earlier this year, we detected an incident involving unauthorized access to a limited number of our emails. We promptly began investigating, and we recently determined some of your child's personal information was contained in those emails. FCCI Insurance Group is providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED

An unauthorized third party had access to a small number of our emails between December 2023 and February 2024. Once we discovered the unauthorized activity, we promptly began investigating. We identified the affected files and engaged a data-review firm to analyze their contents. We received those results in May and have been working since then to ensure we have accurate contact information for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED

Based on the investigation, we determined that the third party who accessed our systems was likely attempting to create fraudulent payment requests rather than gather information on individuals. But, in the course of doing so, the third party may have accessed emails that potentially included your child's name, contact information, date of birth, and government identification (such as a Social Security number) as well as limited health information. We collected this information in connection with insurance we offer or provide to you, your child, or another person or business.

WHAT WE ARE DOING

We hired third-party experts to address this situation, to perform an investigation into the unauthorized activity, and to further secure our systems.

WHAT YOU CAN DO

We currently have no evidence that the unauthorized third party has, or will, use this information to harm you or your child. Nonetheless, we encourage you to remain vigilant for any signs of unauthorized financial activity. Please also review the next page for steps you can take to protect you and your child against fraud and identity theft.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at [TFN](#), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

A handwritten signature in dark ink that reads "Jessica Markun". The signature is fluid and cursive.

Jessica Markun
VP, Risk, Audit & Administrative Services

ADDITIONAL STEPS YOU CAN TAKE

Activate your complimentary credit monitoring – To help protect your child from fraud or identity theft, we are offering a complimentary one-year membership to Experian's IdentityWorks. This product helps detect possible misuse of your child's personal information. To register, please:

- Ensure that you **enroll by:** <<b2b_text_6 (activation deadline)>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/minorplus
- Provide your **activation code:** <<activation code s_n>>

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at (877) 288-8057 by September 6, 2024, and provide them engagement number <<b2b_text_1 (engagement number)>>.

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov/databreach.

- You should confirm that your child's credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your child's credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your child's credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your child's credit file to notify companies extending your child credit that they should take special precautions to verify your child's identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your child's credit report, which makes it harder for someone to open an account in your child's name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your child's full name, Social Security number, date of birth, and current and previous addresses. There is no charge for requesting a security freeze. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you or your child are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission

600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax

P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian

P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.



<<Date>> (Format: Month Day, Year)

Parent or Guardian of

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>

<<address_1>>

<<address_2>>

<<city>>, <<state_province>> <<postal_code>>

<<country>>

Notice of Data Breach

To the Parent or Guardian of <<first_name>> <<last_name>>,

FCCI Insurance Group is writing to inform you of an incident involving potential unauthorized access to your child's information that we obtained in connection with insurance that we offer or provide to you, your child, or another person or business. Earlier this year, we detected an incident involving unauthorized access to a limited number of our emails. We promptly began investigating, and we recently determined some of your child's personal information was contained in those emails. FCCI Insurance Group is providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED

An unauthorized third party had access to a small number of our emails between December 2023 and February 2024. Once we discovered the unauthorized activity, we promptly began investigating. We identified the affected files and engaged a data-review firm to analyze their contents. We received those results in May and have been working since then to ensure we have accurate contact information for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED

Based on the investigation, we determined that the third party who accessed our systems was likely attempting to create fraudulent payment requests rather than gather information on individuals. But, in the course of doing so, the third party may have accessed emails that potentially included your child's name, contact information, and date of birth as well as limited health information. We collected this information in connection with insurance we offer or provide to you, your child, or another person or business.

WHAT WE ARE DOING

We hired third-party experts to address this situation, to perform an investigation into the unauthorized activity, and to further secure our systems.

WHAT YOU CAN DO

We currently have no evidence that the unauthorized third party has, or will, use this information to harm you or your child. Nonetheless, we encourage you to remain vigilant for any signs of unauthorized financial activity. Please also review the next page for steps you can take to protect you and your child against fraud and identity theft.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at [TFN](#), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

A handwritten signature in cursive script that reads "Jessica Markun".

Jessica Markun
VP, Risk, Audit & Administrative Services

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov/databreach.

- You should confirm that your child's credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your child's credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your child's credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your child's credit file to notify companies extending your child credit that they should take special precautions to verify your child's identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your child's credit report, which makes it harder for someone to open an account in your child's name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your child's full name, Social Security number, date of birth, and current and previous addresses. There is no charge for requesting a security freeze. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you or your child are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax
P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.