RENKIM CORPORATION
13333 Allen Road
Southgate MI 48195-2294
734.374.8300 ♦ Fax 734.374.8323

<<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>> <<middle_name>> <<last_name>> <<suffix>>,

We are contacting you about a security incident that concerns some of your personal information. We are reaching out to provide you information on what happened and an opportunity to enroll in free credit monitoring.

WHO WE ARE

Renkim provides print and electronic communications solutions that help companies deliver messages efficiently to many individuals at once. In order for us to provide these services, companies will provide us with the necessary information so that we can process and send out the communications. We received your information as part of this process.

WHAT HAPPENED

On March 3, 2025, we detected suspicious activity on our network. We immediately responded to terminate that activity and secure our network environment. We also launched an investigation with the assistance of third-party experts and notified law enforcement of the incident. Based on the investigation, the suspicious activity started on March 2, 2025, and we believe that an unauthorized third party may have obtained files including your personal information.

WHAT INFORMATION WAS INVOLVED

The information in our systems that was related to you was limited to the information to process and create these mailings. This included a limited amount of your <<b2b_text_2 (personal information or personal health information)>>, which consisted of your: <<b2b_text_3 (data types)>>.

WHAT WE ARE DOING

We hired third-party experts to address this situation, investigate the unauthorized activity, and further secure our systems to protect your information. We also notified law enforcement.

WHAT YOU CAN DO

Enclosed with this letter you will find steps you can take to protect yourself. In addition, we are offering a complimentary <<Monitoring Term Length (Months)>> month membership to Experian IdentityWorks. This product helps detect possible misuse of 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: https://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 <<b2b_text_6(activation deadline)>> and provide them engagement number <<b2b_text_5 (Engagement #)>>.

FOR MORE INFORMATION

Should you have any questions, you can contact us at 1-866-461-3496, between 9:00 am and 6:30 pm Eastern Time, Monday through Friday, excluding major U.S. holidays, and one of our representatives will be happy to assist you.

Sincerely,

Clifton Stephens
President & CEO

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.

- 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. There is no charge for requesting a fraud alert. 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 www.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, (877) 438-4338, www.ftc.gov
- **Equifax,** P.O. Box 740241, Atlanta, GA 30374, (866) 349-5191, 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, (800) 888-4213, www.transunion.com

For Maryland Residents – The Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov.

For North Carolina Residents – The North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents – The New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; 1-800-771-7755; www.ag.ny.gov.

For Rhode Island Residents – The Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; (401) 274-4400; www.riag.ri.gov. This incident impacted [#] Rhode Island residents.

For Washington, D.C. Residents – The Washington, D.C. Attorney General may be reached at: 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/sites/default/ files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

This notice was not delayed by a law enforcement investigation.

RENKIM CORPORATION
13333 Allen Road
Southgate MI 48195-2294
734.374.8300 ♦ Fax 734.374.8323

<<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>> <<middle_name>> <<last_name>> <<suffix>>,

We are contacting you about a security incident that concerns some of your personal information. We are reaching out to provide you information on what happened, what you can do, and what we are doing in response.

WHO WE ARE

Renkim provides print and electronic communications solutions that help companies deliver messages efficiently to many individuals at once. In order for us to provide these services, companies will provide us the necessary information so that we can process and send out the communications. We received your information as part of this process.

WHAT HAPPENED

On March 3, 2025, we detected suspicious activity on our network. We immediately responded to terminate that activity and secure our network environment. We also launched an investigation with the assistance of third-party experts and notified law enforcement of the incident. Based on the investigation, the suspicious activity started on March 2, 2025, and we believe that an unauthorized third party may have obtained files including your personal information.

WHAT INFORMATION WAS INVOLVED

The information in our systems that was related to you was limited to the information to process and create these mailings. This included a limited amount of your <<b2b_text_2 (personal information or personal health information)>>, which consisted of your: <<b2b_text_3 (data types)>>.

WHAT WE ARE DOING

We hired third-party experts to address this situation, investigate the unauthorized activity, and further secure our systems to protect your information. We also notified law enforcement.

WHAT YOU CAN DO

We encourage you to remain vigilant for any signs of unauthorized financial activity and to review the **Additional Steps You Can Take** guidance on the next page.

FOR MORE INFORMATION

Should you have any questions, you can contact us at 1-866-461-3496, between 9:00 am and 6:30 pm Eastern Time, Monday through Friday, excluding major U.S. holidays, and one of our representatives will be happy to assist you.

Sincerely,

Clifton Stephens
President & CEO

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.

- 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. There is no charge for requesting a fraud alert. 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 www.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, (877) 438-4338, www.ftc.gov
- **Equifax,** P.O. Box 740241, Atlanta, GA 30374, (866) 349-5191, 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, (800) 888-4213, www.transunion.com

For Maryland Residents – The Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov.

For North Carolina Residents – The North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents – The New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; 1-800-771-7755; www.ag.ny.gov.

For Rhode Island Residents – The Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; (401) 274-4400; www.riag.ri.gov. This incident impacted [#] Rhode Island residents.

For Washington, D.C. Residents – The Washington, D.C. Attorney General may be reached at: 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/sites/default/ files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

This notice was not delayed by a law enforcement investigation.

RENKIM CORPORATION
13333 Allen Road
Southgate MI 48195-2294
734.374.8300 ♦ Fax 734.374.8323

<<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>> <<middle_name>> <<last_name>> <<suffix>>,

We are contacting you about a security incident that concerns some of your personal information. We are reaching out to provide you information on what happened, what you can do, and what we are doing in response.

WHO WE ARE

Renkim provides print and electronic communications solutions that help companies deliver messages efficiently to many individuals at once. In order for us to provide these services, companies, such as <<b2b_text_1 (Name of Reporting Entity)>>, will provide us the necessary information so that we can process and send out the communications. We received your information as part of this process.

WHAT HAPPENED

On March 3, 2025, we detected suspicious activity on our network. We immediately responded to terminate that activity and secure our network environment. We also launched an investigation with the assistance of third-party experts and notified law enforcement of the incident. Based on the investigation, the suspicious activity started on March 2, 2025, and we believe that an unauthorized third party may have obtained files including your personal information.

WHAT INFORMATION WAS INVOLVED

The information in our systems that was related to you was limited to the information to process and create these mailings. This included a limited amount of your <<b2b_text_2 (personal information or personal health information)>>, which consisted of your: <<b2b_text_3 (data types)>>.

WHAT WE ARE DOING

We hired third-party experts to address this situation, investigate the unauthorized activity, and further secure our systems to protect your information. We also notified law enforcement.

WHAT YOU CAN DO

We encourage you to remain vigilant for any signs of unauthorized financial activity and to review the **Additional Steps You Can Take** guidance on the next page.

FOR MORE INFORMATION

Should you have any questions, you can contact us at 1-866-461-3496, between 9:00 am and 6:30 pm Eastern Time, Monday through Friday, excluding major U.S. holidays, and one of our representatives will be happy to assist you.

Sincerely,

Clifton Stephens
President & CEO

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.

- 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. There is no charge for requesting a fraud alert. 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 www.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, (877) 438-4338, www.ftc.gov
- **Equifax,** P.O. Box 740241, Atlanta, GA 30374, (866) 349-5191, 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, (800) 888-4213, www.transunion.com

For Maryland Residents – The Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov.

For North Carolina Residents – The North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents – The New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; 1-800-771-7755; www.ag.ny.gov.

For Rhode Island Residents – The Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; (401) 274-4400; www.riag.ri.gov. This incident impacted [#] Rhode Island residents.

For Washington, D.C. Residents – The Washington, D.C. Attorney General may be reached at: 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/sites/default/ files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

This notice was not delayed by a law enforcement investigation.