



Stacy A. Cole

D: 513.579.6463

scole@kmlaw.com

February 19, 2025

BY EMAIL ONLY TO IDTHEFT@OAG.STATE.MD.US

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

Re: Incident Notification

Dear Sir/Madam:

We are writing on behalf of our client, Hartson-Kennedy Inc. (“**Hartson-Kennedy**”), to notify the Office of the Maryland Attorney General of a recently discovered security incident that impacts one (1) Maryland resident.

On October 9, 2024, Hartson-Kennedy was alerted to a dark web posting by an attacker claiming to have accessed and removed data from its IT systems. Upon learning of the incident, Hartson-Kennedy immediately worked to successfully contain the intrusion and began its investigation with the help of legal and computer forensics teams. Through its investigation, Hartson-Kennedy learned the attacker accessed its systems starting on June 24, 2024, as a result of an employee clicking a malicious advertisement in an attempt to download a Web browser. As a result, the attacker was able to gain access to parts of Hartson-Kennedy’s network and view and take certain files relating to its current and former employees and their spouses and dependents.

Due to the large volume of data involved, Hartson-Kennedy engaged in months-long comprehensive data mining work, which was recently completed. On December 9, 2024, Hartson-Kennedy mailed notifications to the individuals it initially identified as potentially impacted. Thereafter, data mining uncovered additional impacted individuals, including one (1) Maryland resident. On February 20, 2025, Hartson-Kennedy will be mailing letters in the same form as the enclosed to these additional impacted individuals.

The information that may have been viewed or taken includes contact information, such as current and former employees, spouse, and dependent names, addresses, dates of birth, phone numbers, and emails, plus one or more of the following: healthcare-related information (only for individuals notified on December 9, 2024), Social Security number, driver’s license or state or other ID number, and/or financial account information.

Keating Muething & Klekamp PLL

Attorneys at Law

One East Fourth Street | Suite 1400 | Cincinnati, Ohio 45202

P: 513.579.6400 | F: 513.579.6457 | kmlaw.com

Hartson-Kennedy is providing 24 months of free single-bureau credit monitoring and fraud assistance services to all affected individuals, and has representatives available to take calls and answer questions related to the incident.

Please do not hesitate to contact us should you have any questions regarding this notification or the incident.

Sincerely,

KEATING MUETHING & KLEKAMP PLL

By: 
Stacy A. Cole

Enclosures

Hartson-Kennedy, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



P



February 11, 2025

Re: Notification of data breach at Hartson-Kennedy, Inc. Please read this letter in its entirety.

Dear [REDACTED]

Hartson-Kennedy, Inc. is committed to protecting the privacy of our employees' information. We take privacy very seriously, and it is important to us that you are made fully aware of a privacy issue involving your information.

What Happened?

We at Hartson-Kennedy, on our own behalf and on behalf of the Hartson-Kennedy Inc. Group Benefit Plan, are writing to notify you of a security incident. On October 9, 2024, we were alerted to a dark web posting by an attacker claiming to have accessed and removed data from our IT systems. We immediately began our investigation with the help of legal and computer forensics teams. We learned the attackers accessed our systems starting on June 24, 2024, through a malicious advertisement. As a result, the attacker was able to gain access to parts of our network and view and take certain files relating to our employees, among other types of information. Part of our investigation has included a comprehensive review of the impacted data to identify individuals who may have been affected by this incident.

While we have no evidence that any of your personal information has been misused for identity theft or fraud, we are treating this matter with an abundance of caution to help protect your financial security and alleviate concerns you may have.

What information was involved?

The information that may have been viewed or taken includes contact information, such as your name, address, date of birth, phone number, and email, plus one or more of the following: Social Security number, driver's license or state or other ID number, and/or financial account information. The data that may have been seen or taken may differ from person to person, and not all the information listed above may have been impacted for you.

What are we doing to address this situation?

Hartson-Kennedy fully investigated this incident with its forensic service provider and legal team, and has made immediate enhancements to our systems, security, and practices. Additionally, we have engaged appropriate experts to assist us in conducting a full review of our security practices and systems to ensure that enhanced security protocols are in place going forward so an incident like this does not happen again. In particular, we are improving our systems and processes for records relating to employees and our health plan. We are also enhancing our employee training to increase awareness and prevent future security incidents.

We are committed to helping those who may have been impacted by this situation, and are providing you with access to **Single Bureau Credit Monitoring** services at no charge. These services provide you with alerts for **twenty-four (24) months** from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED] In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What can I do to protect myself?

Please review the enclosed information at the end of this letter entitled "Other Steps You Can Take to Protect Yourself."

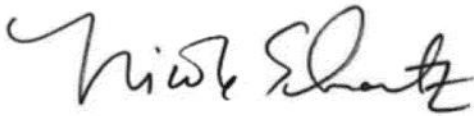
What if I want to talk to someone about this incident?

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern Time, Monday through Friday, excluding holidays. Please call the help line **833-799-3971** and supply the fraud specialist with your unique code listed above.

While representatives should be able to provide thorough assistance and answer most of your questions, you may still feel the need to speak with Hartson-Kennedy regarding this incident. If so, please call us at 765-668-8144 Ext. 126 from 9:00 am to 5:00 pm Eastern Time, Monday through Friday.

We take our responsibilities to protect your personal information very seriously. We apologize for any inconvenience resulting from this incident.

Sincerely,



Nicole Schwartz
General Manager

Other Steps You Can Take to Protect Yourself

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. Hearing impaired consumers can access their TDD service at 1-877-730-4204. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

Upon receipt of your credit report, we recommend that you review it carefully for any suspicious activity. Be sure to promptly report any suspicious activity by calling the help line number included above and providing your unique code listed in this letter.

Police Report. You also 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 evidence 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.

Fraud Alerts. You can also 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:

Experian (1-888-397-3742) P.O. Box 4500 Allen, TX 75013 www.experian.com	Equifax (1-800-525-6285) P.O. Box 740241 Atlanta, GA 30374 www.equifax.com	TransUnion (1-800-680-7289) P.O. Box 2000 Chester, PA 19016 www.transunion.com
--	---	--

No one can place a fraud alert on your credit report except you.

Credit 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.

Additional Information. You can obtain additional information about how 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. You can contact the FTC at <https://consumer.ftc.gov>; 1-877-IDTHEFT (438-4338); TTY 1-866-653-4261; or Attn: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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.



00001020280000

P

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: 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: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400.

P



February 11, 2025

Re: Notification of data breach at Hartson-Kennedy, Inc. Please read this letter in its entirety.

Dear Parent/Guardian of [REDACTED]

Hartson-Kennedy, Inc. is committed to protecting the privacy of our employees' information. We take privacy very seriously, and it is important to us that you are made fully aware of a privacy issue involving your information.

What Happened?

We at Hartson-Kennedy, on our own behalf and on behalf of the Hartson-Kennedy Inc. Group Benefit Plan, are writing to notify you of a security incident. On October 9, 2024, we were alerted to a dark web posting by an attacker claiming to have accessed and removed data from our IT systems. We immediately began our investigation with the help of legal and computer forensics teams. We learned the attackers accessed our systems starting on June 24, 2024, through a malicious advertisement. As a result, the attacker was able to gain access to parts of our network and view and take certain files relating to our employees, among other types of information. Part of our investigation has included a comprehensive review of the impacted data to identify individuals who may have been affected by this incident.

While we have no evidence that any of your child's personal information has been misused for identity theft or fraud, we are treating this matter with an abundance of caution to help protect their financial security and alleviate concerns you may have.

What information was involved?

The information that may have been viewed or taken includes contact information, such as your child's name, address, date of birth, phone number, and email, plus one or more of the following: Social Security number, driver's license or state or other ID number, and/or financial account information.

The data that may have been seen or taken may differ from person to person, and not all the information listed above may have been impacted for your child.

What are we doing to address this situation?

Hartson-Kennedy fully investigated this incident with its forensic service provider and legal team, and has made immediate enhancements to our systems, security, and practices. Additionally, we have engaged appropriate experts to assist us in conducting a full review of our security practices and systems to ensure that enhanced security protocols are in place going forward so an incident like this does not happen again. In particular, we are improving our systems and processes for records relating to employees and our health plan. We are also enhancing our employee training to increase awareness and prevent future security incidents.

We are committed to helping those who may have been impacted by this situation and are providing the parents of impacted minor dependents with access to **Cyber Monitoring** services for you and your minor child for **twenty-four (24) months** at no charge. Cyber monitoring will look out for your and your child's personal data on the dark web and alert you if your personally identifiable information or your child's is found online. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Cyber Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED] Once you have enrolled yourself, click on your name in the top right of your dashboard and select "Manage Family Protection" then "Add Family Member" to enroll your child. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and an email account and will require enrollment by parent or guardian first. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity and your child's.

What can I do to protect my child?

Please review the enclosed information at the end of this letter entitled "Other Steps You Can Take to Protect Yourself."

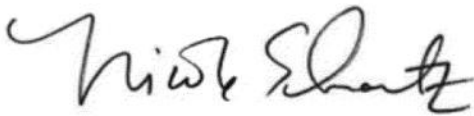
What if I want to speak with someone about this incident?

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern Time, Monday through Friday. Please call the help line at **833-799-3971** and supply the fraud specialist with your unique code listed above.

While representatives should be able to provide thorough assistance and answer most of your questions, you may still feel the need to speak with Hartson-Kennedy regarding this incident. If so, please call us at 765-668-8144 Ext. 126 from 9:00 am to 5:00 pm Eastern Time, Monday through Friday.

We take our responsibilities to protect your personal information and your child's very seriously. We apologize for any inconvenience resulting from this incident.

Sincerely,



Nicole Schwartz
General Manager

Other Steps You Can Take to Protect Yourself

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. Hearing impaired consumers can access their TDD service at 1-877-730-4204. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

Upon receipt of your credit report, we recommend that you review it carefully for any suspicious activity. Be sure to promptly report any suspicious activity by calling the help line number included above and providing your unique code listed in this letter.

Police Report. You also 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 evidence 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.

Fraud Alerts. You can also 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:

Experian (1-888-397-3742)
P.O. Box 4500
Allen, TX 75013
www.experian.com

Equifax (1-800-525-6285)
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

TransUnion (1-800-680-7289)
P.O. Box 2000
Chester, PA 19016
www.transunion.com

No one can place a fraud alert on your credit report except you.

Credit 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.

Additional Information. You can obtain additional information about how 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. You can contact the FTC at <https://consumer.ftc.gov>; 1-877-IDTHEFT (438-4338); TTY 1-866-653-4261; or Attn: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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.



00001020280000

P

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: 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: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400.