

From: Heck, Zachary S. <zheck@taftlaw.com>
Sent: Friday, October 4, 2024 4:50 PM
To: IDTheft
Cc: Franklin, Zenus; Deime, Karen
Subject: State of Maryland - Notice of Security Breach, 21st Century Solutions, Ltd. dba GoKeyless
Attachments: GoKeyless - SAMPLE Security Incident Notice Letter.pdf
Follow Up Flag: Follow up
Flag Status: Flagged
Categories: Data breach

Good afternoon:

Pursuant to Md. Code Ann. Comm. Law 14-3504, I am providing notice of a security incident and a sample notice letter that will be delivered to affected individuals by my client, 21st Century Solutions, Ltd. d/b/a GoKeyless LLC ("GoKeyless"), on October 4, 2024 via first class U.S. mail. My client is providing this notice as expediently as possible having confirmed the scope of the incident, the number of individuals impacted, and its obligations under applicable state law.

Incident and Security Vulnerability

On or about August 16, 2024, GoKeyless identified what it believed to be unauthorized activity by a threat actor in an effort to access GoKeyless information systems (the "Incident"). The unauthorized access to GoKeyless information systems lasted from on or about June 25, 2024 until access was terminated on August 16, 2024. Once aware of the Incident, GoKeyless promptly took a series of actions to contain the Incident, remediate the issue, and investigate the scope and depth of the Incident's impact. Based on GoKeyless' investigation, it learned that the attack was likely made possible through a user credential compromise. On September 11, 2024, at the conclusion of GoKeyless' investigation, it discovered that personal information may have been impacted by the unauthorized access. Although the investigation did not identify any actual misuse of any personal information, GoKeyless can neither confirm, nor deny, whether the threat actor viewed or removed personal information during the Incident. Therefore, GoKeyless is providing notice to the impacted Maryland resident out of an abundance of caution.

Maryland Individuals Impacted

Upon learning of the Incident and the indication that personally identifiable information may have been accessible, GoKeyless immediately began reviewing files that may have been impacted. GoKeyless confirmed that the personally identifiable information of one (1) Maryland resident may have been impacted. GoKeyless has been working since then to confirm the individuals, addresses of resident, and data risk.

Potentially Compromised Information

As described in the attached sample notice letter, personally identifiable information that could have been potentially accessed or viewed as a result of the Incident may have included: first name and last name; postal address; and credit card with CVV.

Response and Remediation

Once aware of the Incident, GoKeyless engaged trusted third-party forensics and cybersecurity experts to assist with understanding the impacts of the Incident, and promptly took a series of actions to contain and remediate the Incident. GoKeyless has carefully brought impacted information systems back online, and it continues to closely monitor its network and information systems for unusual activity. As part of GoKeyless' remediation of the Incident, it promptly took steps to secure the system by implementing a variety of mitigation steps, including changing user credentials and implementing

new employee training. Based on the forensic and cybersecurity experts' recommendations, GoKeyless also implemented both administrative and technical safeguards to further remediate the Incident and to prevent such an incident from occurring again. Beyond these immediate measures, GoKeyless will continue developing its administrative, technical, and physical safeguards to further improve its security.

Should you have any questions regarding this matter, please do not hesitate to contact me.

Sincerely,
Zachary Heck, Esq., CIPP/US/E, CIPM



Zachary S. Heck

Partner

zheck@taftlaw.com

Dir: 937.641.2053

Tel: 937.228.2838 | Fax: 937.228.2816

40 North Main Street, Suite 1700

Dayton, Ohio 45423-1029

[Download: Taft Privacy and Data Security Mobile App – Google](#)

[Download: Taft Privacy and Data Security Mobile App – Apple](#)

taftlaw.com



Taft expands on Jan. 1, 2025 to the Mountain West region with the addition of Sherman & Howard, a prominent 130-year-old law firm. Learn more **[here](#)**.

This message may contain information that is attorney-client privileged, attorney work product or otherwise confidential. If you are not an intended recipient, use and disclosure of this message are prohibited. If you received this transmission in error, please notify the sender by reply e-mail and delete the message and any attachments.

[Date]

[First Name Last Name]

[Address]

[City, State Zip]

RE: Notification of Data Security Incident

Dear [First Name],

21st Century Solutions, Ltd. d/b/a GoKeyless LLC (“GoKeyless”, “we”, or “our”) takes the security and protection of your personal information seriously. We are writing to inform you of a data security incident in which your personal information may have been accessed by an unauthorized third party. We are providing this letter to you out of an abundance of caution to provide you information about the incident and what you can do to remain vigilant and protect your personal information.

What Happened

On or about August 16, 2024, GoKeyless first became aware of unauthorized activity by a threat actor in an effort to access GoKeyless information systems (the “Incident”). The unauthorized access to GoKeyless information systems lasted from on or about June 25, 2024 until access was terminated on August 16, 2024. Once aware of the Incident, we promptly took a series of actions to contain the Incident, remediate the issue, and investigate the scope and depth of the Incident’s impact. Based on our investigation, we learned that the attack was likely made possible through a user credential compromise. At the conclusion of our investigation, we determined that your personal information may have been impacted by the unauthorized access. Although the investigation did not identify any actual misuse of any personal information, GoKeyless can neither confirm, nor deny, whether the threat actor viewed or removed your personal information during the Incident. Therefore, GoKeyless is providing you this letter out of an abundance of caution.

What Information Was Involved

Although GoKeyless has confirmed unauthorized access to the its information systems between June 25, 2024 and August 16, 2024, there is no conclusive evidence that the intruder has used any of the accessible personal information. At this point in our investigation, we can neither confirm nor deny that any personal information was successfully exfiltrated by the threat actor. In an abundance of caution, we are informing you that the intruder may have accessed, viewed, or removed from our systems, the following categories of personal information:

First and last name	Postal Address	Credit Card Number and CVV
Driver’s license number	Passport Number	Social Security Number

What We Are Doing

Once aware of the Incident, we engaged trusted third-party forensics and cybersecurity experts to assist with understanding the impacts of the Incident, and promptly took a series of actions to contain and remediate the Incident. We have carefully brought impacted information systems back online, and we continue to closely monitor our network and information systems for unusual activity. As part of our remediation of the Incident, we promptly took steps to secure the system by implementing a variety of mitigation steps, including changing

user credentials and implementing new employee training. Based on the forensic and cybersecurity experts' recommendations, we also implemented both administrative and technical safeguards to further remediate the Incident and to prevent such an incident from occurring again. Beyond these immediate measures, GoKeyless will continue developing its administrative, technical, and physical safeguards to further improve its security.

What You Can Do

While we have received no reports or indication of such activity, the risks related to unauthorized use of a Social Security number, government identification number, or financial information may include identity theft, financial fraud, and tax fraud. Please be vigilant about monitoring your personally identifiable information, in particular your credit report information and financial accounts, to protect against fraudulent activity. Please also take care and attention when submitting tax returns to protect against possible fraudulent submissions made on your behalf.

If you have concerns about identity theft, you can contact local law enforcement and file a police report. You can also contact your state's Attorney General, as well as the Federal Trade Commission or one of the credit bureaus for more information about how to protect your identity.

For More Information

If you are concerned about identity theft, you can place an identity theft/fraud alert, get credit freeze information for your state, or order a free credit report by calling any of the following credit bureaus at one of the phone numbers listed below or by visiting their respective websites.

Equifax PO Box 740241 Atlanta, GA 30374 800-525-6285 www.equifax.com	Experian PO Box 4500 Allen, TX 75013 888-397-3742 www.experian.com	TransUnion PO Box 2000 Chester, PA 19016 877-322-8228 www.transunion.com
--	--	--

Credit Reports. You can request credit reports from all three credit bureaus be sent to you free of charge. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

Fraud Alerts. You can place a fraud alert with the credit bureaus free of charge. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year. You may also place an extended fraud alert, which lasts up to seven years unless you cancel it sooner. Additionally, you can provide a phone number instructing lenders to contact you if someone applies for credit in your name, and you will get an instant alert to the potential fraud.

Security Freeze. Under state law, a security freeze (or credit freeze) prohibits a credit bureau from releasing any information from a consumer's credit report without written authorization. There is no fee associated with freezing or thawing your credit. The process of freezing your credit takes only a few minutes. You must contact each credit bureau individually to freeze your credit with each bureau. The credit bureaus have one (1) business day after your request to place a security freeze if made by telephone or secure electronic means. If the request is made by mail, the credit bureaus have three (3) business days. The credit bureaus must also send written confirmation to you within five (5) business days. To place a security freeze, you may need to provide the following information:

1. Your full name;

2. Social Security number;
3. Date of birth;
4. Mobile number;
5. Current postal address;
6. Email address; and
7. Any other information that the credit bureau may require.

To lift the security freeze, in order to allow a specific entity or individual access to your credit report, you must apply online, call, or send a written request to the credit bureaus by mail. When you contact a credit bureau to lift the security freeze, you will need to include proper identification (name, address, and Social Security number) and the PIN number or password that was provided to you (if provided) when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. If you request a credit thaw online or by phone, the credit bureaus are required by law to complete the request within one hour. If you request the thaw by regular mail, the credit bureaus have three business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

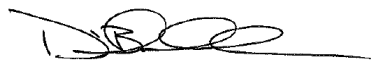
The Federal Trade Commission (FTC) provides more information about how to protect your identity at either <https://www.ftc.gov/> or <https://www.identitytheft.gov/>. You may also find additional information on any applicable rights under the Fair Credit Reporting Act. You can also contact the FTC at: Federal Trade Commission, Bureau of Consumer Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-202-326-2222.

<u>For Maryland Residents:</u> You may also contact the Maryland Attorney General's Office for more information about how to protect your identity by using the information below: Attorney General's Office 200 St. Paul Place Baltimore, MD 21202 Phone: 410-528-8662 Website: https://www.marylandattorneygeneral.gov/	<u>For New York Residents:</u> You may also contact the New York Attorney General's Office for more information about how to protect your identity by using the information below: Attorney General's Office Toll Free Phone Number: (800) 771-7755 Website: https://ag.ny.gov/
--	--

Again, we sincerely regret that this incident has occurred. If you have any questions, please contact us at:

Contact: Dan Isenbarger
Email: dan.isenbarger@Gokeyless.com
Telephone: 937.672.3170
Address: 21st Century Solutions, Ltd. d/b/a GoKeyless LLC
955 Mound Rd
Miamisburg, OH 45342

Sincerely,



Dan Isenbarger, Vice President of Finance