

# BakerHostetler

## Baker&Hostetler LLP

312 Walnut Street  
Suite 3200  
Cincinnati, OH 45202-4074

T 513.929.3400  
F 513.929.0303  
www.bakerlaw.com

Craig A. Hoffman  
direct dial: 513.929.3491  
cahoffman@bakerlaw.com

October 6, 2025

### VIA E-MAIL (CONSUMER@AG.IOWA.GOV)

Consumer Protection Division  
Security Breach Notifications  
Office of the Attorney General of Iowa  
1305 E. Walnut Street  
Des Moines, IA 50319-0106

*Re: Incident Notification*

Dear Sir or Madam:

I am writing on behalf of my client, AppFolio, Inc. (“AppFolio”), to notify you of a third-party data security incident involving Iowa residents.

On August 22, 2025, AppFolio was made aware of a security incident affecting Salesloft, a provider of sales enablement software, and one of AppFolio’s vendors. This incident, which reportedly impacted hundreds of organizations, allowed unauthorized access to records in AppFolio’s CRM system between August 8 to August 18, 2025. Upon learning of the security incident, AppFolio promptly disabled all Salesloft integrations and launched an investigation. The investigation confirmed that the unauthorized access involved requests to retrieve data from the CRM system. AppFolio then worked to determine what requests were made by the unauthorized actor and what data was returned in response to the requests. The investigation confirmed that the unauthorized access involved requests to retrieve data from AppFolio’s hosted CRM system from a specific location that contained personal information; however, the investigation was not able to identify the specific records or information returned. On September 18, 2025, the investigation determined the records accessed by the unauthorized actor may have contained the names and Social Security numbers of 799 Iowa residents.

On October 6, 2025, AppFolio began mailing notification letters via United States Postal Service First-Class mail to the Iowa residents whose information may have been involved, in accordance with Iowa Code § 715C.1-2. A sample copy of the notification letter is enclosed. AppFolio is offering all notified individuals one year of complimentary credit monitoring and identity

October 6, 2025

Page 2

protection services. AppFolio has also established a dedicated, toll-free call center to answer questions that individuals may have.

To prevent a similar incident in the future, AppFolio has been in close contact with Salesloft to understand the steps it has taken to address this incident and prevent future occurrences.

Please do not hesitate to contact me if you have any questions regarding this matter.

A handwritten signature in blue ink, appearing to read "Craig Hoffman". The signature is stylized and includes a long horizontal line extending to the right.

Craig Hoffman  
Partner

Enclosure



October 6, 2025

Dear

AppFolio, Inc. (“AppFolio,” “we,” or “our”) is writing to notify you of a recent security incident that occurred through a third-party vendor that may have involved your personal information. We want to provide you with the details of this incident and the steps we are taking to address it, including offering you complimentary credit monitoring and identity theft protection.

**What Happened?** On August 22, 2025, we were made aware of a security incident affecting Salesloft, a provider of sales enablement software and one of our vendors. This incident, which reportedly impacted hundreds of organizations, allowed unauthorized access to records in AppFolio’s hosted CRM system .

Upon learning of the security incident, we promptly disabled all Salesloft integrations and launched an investigation. Our investigation confirmed that the unauthorized access involved requests to retrieve data from our hosted CRM system. One such request obtained approximately 0.13% of the records from a specific location that contained personal information; however, our investigation was not able to identify the specific records or information that were part of the 0.13%.

**What Information Was Involved?** The records accessed by the unauthorized actor contained information that included names, addresses, dates of birth, and Social Security numbers. Although our investigation could not definitively determine whether a record with your personal information was part of the approximately 0.13% of records accessed, there is a small chance your personal information was accessed.

**What We Are Doing?** AppFolio’s contract with Salesloft requires Salesloft to use appropriate security measures. We have been in close contact with Salesloft to understand the steps it has taken to address this incident and prevent future occurrences.

In addition, we are offering you the option (at no cost to you) to enroll in credit monitoring and identity theft protection services provided by Cyberscout, a TransUnion company. This product helps detect possible misuse of your information and provides you with identity protection solutions focused on prompt identification and resolution of identity theft. Activating this product will not hurt your credit score.

**What You Can Do?** For more information on the credit monitoring and identity theft services available to you, including instructions on how to activate such services, please see the additional information provided with this letter. If you have questions, please call 1-833-866-9539, Monday through Friday, from 8:00 am to 8:00 pm Eastern Time (excluding U.S. holidays).

Sincerely,

AppFolio, Inc.

## ENROLLMENT INSTRUCTIONS FOR CYBERSCOUT IDENTITY FORCE SERVICES

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 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:



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.

### **ADDITIONAL STEPS YOU CAN TAKE**

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 1000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.identitytheft.gov](http://www.identitytheft.gov)

### **Fraud Alerts and Credit or Security Freezes:**

**Fraud Alerts:** There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud--an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

**Credit or Security Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That is because most creditors need to see your credit report before they approve a new account. If they cannot see your report, they may not extend the credit.

*How do I place a freeze on my credit reports?* There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)
- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 160, Woodlyn, PA 19094, [www.transunion.com](http://www.transunion.com)

You will need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

*How do I lift a freeze?* A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

AppFolio, Inc.'s corporate headquarters is located at 70 Castilian Dr., Goleta, CA 93117, and can be contacted by phone at (866) 648-1536.

**Additional information for residents of the following states:**

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, [www.ct.gov/ag](http://www.ct.gov/ag)

District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 400 6<sup>th</sup> Street NW, Washington, DC 20001, 1-202-727-3400, [www.oag.dc.gov](http://www.oag.dc.gov)

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, [www.marylandattorneygeneral.gov/](http://www.marylandattorneygeneral.gov/)

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov)



Rhode Island: This incident involves 188 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, [www.riag.ri.gov](http://www.riag.ri.gov)

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

**A Summary of Your Rights Under the Fair Credit Reporting Act:** The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to [www.consumerfinance.gov/learnmore](http://www.consumerfinance.gov/learnmore) or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.