



Richard Aponte-Boyd
Office: (267) 930-4888
Fax: (267) 930-4771
Email: raponte@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

October 29, 2025

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Magenta Holdco GP, LLC dba GreenSky, LLC (“GreenSky”) located at P.O. Box 2730, Alpharetta, Georgia 30023, and write to notify your office of an incident that may affect the security of certain personal information relating to fourteen (14) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, GreenSky does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or around August 21, 2025, GreenSky received a report of a possible security issue affecting the Salesloft Drift application used by thousands of customers of the Salesforce cloud-based platform, including GreenSky. On August 29, 2025, Salesloft provided GreenSky with additional information regarding the security issue. Based on this information, GreenSky launched an investigation and determined that between August 13, 2025, and August 18, 2025, several customer-related GreenSky databases were accessed by an unauthorized actor. GreenSky then conducted a comprehensive review of the information accessed by the unauthorized actor within the affected databases to determine to whom the information relates for purposes of providing notice. This review was recently completed.

The information that could have been subject to unauthorized access includes name, and Social Security number.

Notice to New Hampshire Residents

On or about October 29, 2025, GreenSky provided written notice of this incident to fourteen (14) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, GreenSky moved quickly to investigate and respond to the incident, assess the security of GreenSky systems, and identify potentially affected individuals. Additionally, GreenSky notified federal law enforcement regarding the event, is working to implement additional safeguards and training to its employees, and is providing access to credit monitoring services for two (2) years, through Cyberscout, a TransUnion company, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Further, GreenSky is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank, information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

GreenSky is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4888.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Richard Aponte-Boyd".

Richard Aponte-Boyd of
MULLEN COUGHLIN LLC

RAB/azd
Enclosure

EXHIBIT A



Magenta Holdco GP, LLC dba GreenSky, LLC
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS2095



NOTICE OF SECURITY INCIDENT

Dear

Magenta Holdco GP, LLC dba GreenSky, LLC (“GreenSky”), through its subsidiaries and affiliates, acts as a bank-directed program administrator and technology and services provider to federally insured, federally- or state-chartered banks (the “Banks”) that offer consumer loans to finance the purchase of goods and services from merchants. As part of that process, GreenSky maintains certain information related to businesses that are merchants or apply to become merchants. GreenSky writes to notify you of a recent incident involving a former GreenSky service provider that may impact the privacy of some of your information. Although we have no evidence of misuse of your information, we are providing you with this notice in an abundance of caution, to inform you of the incident, our response, and steps you can take to help protect against the possible misuse of your information, should you feel it appropriate to do so.

What Happened. On August 21, 2025, GreenSky received a report of a possible security issue affecting the Salesloft Drift application used by thousands of customers of the Salesforce cloud-based platform, including GreenSky. On August 29, 2025, Salesloft provided us with additional information regarding the security issue. Based on this information, GreenSky conducted a forensic investigation, with the assistance of third-party cybersecurity specialists, to determine if any of our systems were impacted and what data might have been involved. Our investigation found that between August 13, 2025, and August 18, 2025, several customer-related GreenSky databases were accessed by an unauthorized actor. We then conducted a comprehensive review of the affected databases to determine what, if any, sensitive information was at risk of unauthorized access. We recently completed this review, and we are notifying you because the investigation determined that certain information related to you was contained in the affected databases.

What Information Was Involved. The investigation confirmed that your
were present in the databases that were accessed by an unauthorized actor.

What We Are Doing. GreenSky takes this incident and the security of the information in our care seriously. Upon learning that the Salesloft Drift application was affected by a cybersecurity issue, we promptly terminated our relationship with Salesloft and took steps to confirm the security of GreenSky systems. We also engaged third-party cybersecurity specialists to investigate the activity to determine what occurred. As part of our ongoing commitment to the privacy of information in our care, we are also reviewing our policies, procedures and processes related to the storage and access of sensitive information to reduce the likelihood of a similar future incident.

As an added precaution, we are offering you _____ months of complimentary access to credit monitoring and identity monitoring services through Cyberscout, a TransUnion company. If you wish to receive these services, you must enroll by following the below activation instructions, as we are unable to activate these services on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your bank and credit card statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. Please also review the information contained in the enclosed *Steps You Can Take To Help Protect Your Information*. There, you will also find more information on the complimentary credit monitoring services we are making available to you.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance, please call our assistance line at 1-866-936-0602, Monday through Friday 8 am EST – 10 pm EST, Saturday 8 am EST – 8 pm EST, and Sunday 10 am EST – 8 pm EST. You may also write to GreenSky at P.O. Box 2730, Alpharetta, GA 30023.

Sincerely,

GreenSky, LLC

Steps You Can Take To Help Protect Your Information

Enroll in Credit Monitoring

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 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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a fraud alert or a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to your bank or credit card company and law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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. We encourage consumers to review their 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.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 7 Rhode Island residents that may be impacted by this event.