faegredrinker.com

Kathryn R. Allen
Associate
kathryn.allen@faegredrinker.com
+1 612 766 7116 direct

Faegre Drinker Biddle & Reath LLP
2200 Wells Fargo Center
90 South Seventh Street
Minneapolis, Minnesota 55402
+1 612 766 7000 main
+1 612 766 1600 fax

February 27, 2021

VIA E-MAIL (SECURITYBREACH@ATG.WA.GOV.)

Re: Data Security Incident Notification

Dear Attorney General Bob Ferguson:

Our firm represents Fastcase, Inc. ("Fastcase"), which recently acquired Casemaker, LLC and Lawriter, LLC (collectively, "Casemaker"). Casemaker recently experienced a data incident and we are hereby formally notifying you of this event pursuant to Washington Statute § RCW 19.255.010. By providing this notice, we do not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington notification security breach statute, or all/any other applicable laws (including those pertaining to personal jurisdiction).

On January 5, 2021, Casemaker announced its merger with Fastcase. On January 28, 2021, while laying the groundwork for consolidating the Fastcase and Casemaker platforms, Fastcase learned of a potential security issue with the Casemaker Libra platform ("Casemaker Libra"). Upon learning of the incident, Fastcase quickly notified its Casemaker counterparts and engaged a third-party forensic firm and outside counsel to investigate the matter. While the investigation was ongoing, the Casemaker team took the Casemaker Libra product offline for security maintenance. Ultimately, the third-party forensic investigators found that attackers used malicious code with the capability of taking user tables on Casemaker Libra, apparently seeking to copy data from Casemaker Libra database tables. Although it is possible that the attacks could have gone back further, the forensic team found evidence indicating that the bulk of unauthorized access occurred between July and October 2020, before the merger.

Casemaker sent notifications to the potentially affected individuals on February 26, 2021. The notice contains a description of what happened and the personally identifiable information (PII) that could have potentially been accessed, including an individual's name, street address, email address and Casemaker Libra password. For your reference, we have attached a sample letter of the individual notice, attached hereto as Exhibit A. Casemaker sent this notice to the one thousand six hundred and ninety (1690) Washington residents identified by the third-party forensics team. Casemaker s providing individuals with a toll-free number to call with any questions.

/
/
/
/
/
/
/

As remedial or containment measures, Casemaker prompted password changes, conducted a code review, conducted security scans of the Casemaker platform, and installed security features on Casemaker platforms to help mitigate against malicious attacks in the future. Fastcase also accelerated the migration of Casemaker Libra users to the Casemaker 4 platform as an interim security step. If you have any questions regarding this matter, please do not hesitate to contact me at 612-766-7116 or Kathryn.Allen@faegredrinker.com.

Very truly yours,
Kathryn R. Allen

EXHIBIT A
Sample Notice Letter

[[DATE]]

[[NAME]]
[[ADDRESS]]
[[CITY]], [[STATE]] [[ZIP]]

RE: Notice of Data Security Incident

Dear [[NAME]]:

We are writing to notify that Casemaker, LLC and Lawriter, LLC (collectively, "Casemaker"), had a security incident that may have involved some of your personal information. We take the protection and proper use of your information very seriously; therefore, we are contacting you to explain the incident and measures taken to protect your information.

What Happened?

On January 5, 2021 Casemaker announced its merger with Fastcase, Inc. ("Fastcase"). One purpose of the merger was to consolidate various Casemaker and Fastcase legal research platforms to improve user experience. On January 28, 2021, during the groundwork for this consolidation, Fastcase learned of a potential security issue with the Casemaker Libra platform ("Casemaker Libra"). Upon learning of the incident, Fastcase quickly notified its Casemaker counterparts and engaged a third-party forensic firm and outside counsel to investigate the matter. While the investigation was ongoing, the Casemaker team took the Casemaker Libra product offline for security maintenance. Ultimately, the third-party forensic investigators found that attackers used malicious code with the capability of taking user tables on Casemaker Libra, apparently seeking to copy data from Casemaker Libra database tables. Although it is possible that the attacks could have gone back further, the forensic team found evidence indicating that the bulk of unauthorized access occurred between July and October 2020, before the merger.

What Information Was Involved?

Based on an extensive investigation, forensic experts determined that the stolen Casemaker Libra data may have contained some of your personal information, including your name, street address, email address and Casemaker Libra password. Although a subset of passwords in the Casemaker Libra platform were exposed, the majority of passwords in Casemaker Libra were encrypted. Forensic investigators did not find any evidence that this incident changed or affected any of the content of reported cases or any other legal reference material in any Casemaker system.

What's Being Done?

The Casemaker team has worked with third-party forensic investigators to enhance many security measures across our platforms. We prompted password changes, conducted a code review, conducted security scans of the Casemaker platform, and we installed security features on Casemaker platforms to help mitigate against malicious attacks in the future. We also accelerated the migration of Casemaker Libra users to the Casemaker 4 platform as an interim security step.

What Can You Do?
As a best practice in today's world of cybercrime, we recommend that you continue to remain vigilant and report any suspicious activity on your accounts. Many password managers help users set strong passwords and will notify you if your passwords have been compromised. Please promptly change your password or take other appropriate steps to protect all online accounts for which you have used the same password as the one potentially compromised in this attack. Finally, we recommend that you review the attachment called *Preventing Identity Theft and Fraud* for more information on ways to protect yourself and your data.

For More Information
We regret any inconvenience this incident may cause you. Should you have any further questions or concerns regarding this matter, you may contact Casemaker at 855-919-2743. Please be ready to provide engagement number DB25627 to the agent.

Sincerely,

Satish Sheth
CEO of Casemaker

PREVENTING IDENTITY THEFT AND FRAUD

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Immediately report any suspicious activity to your bank or credit union. If you do find suspicious activity on your credit reports or other statements, call your local police or sheriff's office or state Attorney General and file a report of identity theft. You have a right to a copy of the police report, and you may need to give copies of the police report to creditors to clear up your records and also to access some services that are free to identity theft victims.

Under the U.S. Fair Credit Reporting Act and other laws, you have certain rights that can help protect yourself from identity theft. Many of these are explained in this document and at www.identitytheft.gov /Know-Your-Rights. For example, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, call toll-free, 1-877-322-8228, or visit www.annualcreditreport.com. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can have these credit bureaus place a short-term or an extended "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069 Atlanta, GA 30348-5069 (800) 525-6285 www.equifax.com	P.O. Box 9554 Allen, TX 75013 888-397-3742 www.experian.com	P.O. Box 2000 Chester, PA 19016-2000 800-680-7289 www.transunion.com

You may also place a security freeze on your credit reports, free of charge. A security freeze, also known as a "credit freeze," prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. But unlike a fraud alert, you must separately place a security freeze on your credit file at **each** bureau. You can use the following addresses and contact information to place a security freeze with each major credit bureau:

Equifax Security Freeze. 1-800-685-1111. P.O. Box 1057881, Atlanta, GA 30348-0241. www.equifax.com/personal/credit-report-services/credit-freeze/;

Experian Security Freeze. 1-888-EXPERIAN or 1-888-397-3742. P.O. Box 9554, Allen, TX 75013. www.experian.com/freeze/center.html; or

TransUnion. 1-800-680-7289. Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022-2000. www.transunion.com/credit-freeze

In order to request a security freeze, you may need to supply your full name (including middle initial, as well as Jr., Sr., II, III, etc.), date of birth, Social Security number, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement to show proof of your current address. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning your identity theft.

The credit reporting agencies must place a security freeze on your credit report within one (1) business day after receiving a request by phone or secure electronic means, and within (3) business days after receiving your request by mail. The credit bureaus must then send written confirmation to you within five (5) business days of placing the security freeze, along with information about how to remove or lift the security freeze in the future.

You can further educate yourself regarding identity theft, fraud alerts, freezes, and the steps you can take to protect yourself by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission encourages those who discover their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement or your state Attorney General as well.

The Federal Trade Commission can be reached at:

Federal Trade Commission
Consumer Resource Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.identitytheft.gov or www.ftc.gov

OTHER IMPORTANT INFORMATION
You may also file a report with your local police or the police in the community where the identity theft took place. Further, you are entitled to request a copy of the police report filed in this matter.

For California residents:
You can visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For Iowa residents:
You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Maryland residents:
You may obtain information about avoiding identity theft at: Office of the State of Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.marylandattorneygeneral.gov.

For North Carolina residents:
You may obtain information about avoiding identity theft at: North Carolina Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001 919-716-6400 www.ncdoj.gov.

For New Mexico residents:
The Fair Credit Reporting Act provides certain rights in addition to the right to receive a copy of your credit report (including a free copy once every 12 months), including the right to ask for a credit score, dispute incomplete or inaccurate information, limit "prescreened" offers of credit and insurance, and seek damages from violators. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Rhode Island residents:
You may obtain information about preventing and avoiding identity theft from Rhode Island's Attorney General Office: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, Phone: (401) 274-4400 http://www.riag.ri.gov.

For Washington D.C. residents:
You may obtain information about avoiding identity theft at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 202-727-3400, https://oag.dc.gov/.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).