



Harter Secrest & Emery LLP

ATTORNEYS AND COUNSELORS

[WWW.HSELAW.COM](http://www.hselaw.com)

October 4, 2022

VIA EMAIL (SecurityBreach@atg.wa.gov)

Office of the Attorney General
1125 Washington St SE
PO Box 40100
Olympia, WA 98504

Re: Kaye-Smith Enterprises, Inc.

To Whom It May Concern:

Harter Secrest & Emery LLP represents Kaye-Smith Enterprises, Inc., with its principal place of business at 4101 Oakesdale Ave SW, Renton, Washington, 98057. Reference is respectfully made to Kaye Smith's earlier letter dated July 25, 2022, which provided notice that Kaye-Smith had been the victim of a sophisticated ransomware attack.

This supplemental notice is being provided by Kaye-Smith on behalf of Kaye-Smith's customer, Washington Federal Bank, dba WaFd Bank. WaFd Bank determined that a breach occurred with regard to customer information on August 5, 2022. On or about September 16, 2022, 36,119 customers that are also Washington residents received written notice in the form attached hereto, which advised them that certain of their personal information, specifically, name, address, telephone number, and account number, may have been impacted in the incident. All recipients of said notice will be receiving an offer of complementary credit monitoring and identity theft services, which are described in the letter.

The investigation into the incident has determined that the time frame of exposure was from May 18, 2022 through June 2, 2022. The incident was discovered on June 2, 2022. Upon discovery of the incident, Kaye-Smith moved quickly to investigate and secure its environment. It notified federal law enforcement and has deployed enhanced security measures and endpoint monitoring and detection.

Kaye-Smith's investigation into the scope of the incident remains ongoing, and, if necessary, Kaye-Smith will supplement this notice accordingly.

Thank you.

Very truly yours,
Harter Secrest & Emery LLP

A handwritten signature in blue ink, appearing to read 'F. Paul Greene', with a long horizontal flourish extending to the right.

F. Paul Greene
DIRECT DIAL: 585.231.1435
EMAIL: FGREENE@HSELAW.COM

Kaye-Smith
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

Dear <<Name 1>>,

Kaye-Smith is providing notice of a recent incident affecting certain personal information it processes. We process your personal information as a mailing service provider for Washington Federal Bank, dba WaFd Bank. The confidentiality, privacy, and security of personal information in Kaye-Smith's systems is very important to Kaye-Smith, and Kaye-Smith takes this incident seriously. This notice provides information on the incident and what we are doing in response, to keep the personal information we process safe and secure.

What Happened?

In June 2022, Kaye-Smith engaged outside experts to help investigate suspicious activity relating to its operating environment. A detailed investigation into the matter ultimately confirmed that a discrete number of files were compromised as part of a ransomware attack by a bad actor, with available logs identifying the first suspicious activity in late May 2022. Subsequently, we completed a thorough review of the files to identify the information compromised.

What Information Was Involved?

On August 5, 2022, we identified the following sensitive information about you in the files compromised during the incident: your name, mailing address, and account number. For some individuals, we also identified a phone number present in the data.

What We Are Doing

Through our investigation we confirmed the scope of this incident, the security of our environment and that our systems are not otherwise currently at risk. In order to prevent any further unauthorized access, we have enhanced our security measures and monitoring and we will continue to work closely with WaFd Bank to ensure the continued security of our systems. We are also providing a complimentary credit monitoring service for you, which you can find more information about below.

What You Can Do

You may wish to take some or all of the below actions to help reduce your risk of identity theft:

- Remain vigilant, especially over the next 12-24 months, and review your bank accounts, credit card bills and free credit reports for unauthorized activity. Promptly report any suspected identity theft to your local law enforcement agency, the U.S. Federal Trade Commission, your State Attorney General, your financial institution, and to the Fraud Alert phone line of a consumer reporting agency. You can obtain information about fraud alerts and security freezes by contacting the three national reporting agencies below:
 - **Equifax**, P.O. Box 740256, Atlanta, GA 30374, www.equifax.com, 1-800-525-6285;
 - **Experian**, P.O. Box 4500, Allen, TX 75013, www.experian.com, 1-888-397-3742; and
 - **TransUnion**, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016, www.transunion.com, 1-800-680-7289.
- Periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted.
- Place a fraud alert on your credit file by contacting any of the three credit reporting agencies listed above. A fraud alert temporarily, for a period of 90 days, requires potential creditors to take additional steps to verify your identity before issuing credit in your name.

- Place a security freeze on your consumer report. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. However, a security freeze may delay your ability to obtain credit. Please contact one of the three credit reporting agencies listed above for further information.
- Request and carefully review your free annual consumer credit report by visiting www.annualcreditreport.com or by calling 1-877-322-8228.
- Enroll in the free credit-monitoring service we are providing – see more information below.

You can also contact the Federal Trade Commission to obtain information about preventing identity theft and, specifically, setting up fraud alerts and security freezes. The contact information for the Federal Trade Commission is as follows: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, www.ftc.gov, 1-877-382-4357.

OTHER IMPORTANT INFORMATION

Kaye-Smith is providing Equifax Credit Watch Gold as a result of this incident.

Your Activation Code: <<ACTIVATION CODE>>

Your Enrollment Deadline: <<Enrollment Deadline>>

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <<ACTIVATION CODE>> then click “Submit” and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click “Continue”.

If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

¹ WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers’ personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers’ personal information is at risk of being traded.

² The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

³ Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer’s identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

⁴ The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

FOR MORE INFORMATION

We apologize for any concern or inconvenience this incident may cause. If you have questions, please contact our call center at 877-560-8603, 6am to 6pm Pacific Time. Our mailing address is 4101 Oakesdale Ave SW, Renton, WA 98057.

Thank you.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For 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 violators. 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. We encourage you to 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.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

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

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street,

Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

For Vermont Residents, if you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General’s Office at 802-656-3183 (800-649-2424 toll free in Vermont only).



Harter Secret & Emery LLP

ATTORNEYS AND COUNSELORS

WWW.HSELAW.COM

July 25, 2022

VIA EMAIL (SecurityBreach@atg.wa.gov)

Office of the Attorney General
1125 Washington St SE
PO Box 40100
Olympia, WA 98504

Re: Kaye-Smith Enterprises, Inc.

To whom it may concern:

Harter Secret & Emery LLP represents Kaye-Smith Enterprises, Inc., with its principal place of business at 4101 Oakesdale Ave SW, Renton, Washington, 98057. Kaye-Smith is a marketing execution and supply chain company that services business clients across a wide range of industries. On or about June 2, 2022, Kaye-Smith discovered that it had been the victim of a sophisticated ransomware attack. Kaye-Smith has since worked diligently to restore and safeguard the integrity of its systems as well as investigate the scope of the incident.

As is now common in ransomware attacks, certain data processed by Kaye-Smith was exfiltrated as part of the attack. Kaye-Smith's investigation into the scope of the incident continues and a thorough review of exfiltrated files is being undertaken to identify the number of individuals potentially affected and the information involved. At this point, Kaye-Smith has not yet confirmed the number of Washington residents whose information may have been potentially affected by this incident, but it is currently anticipated that Washington residents will receive notice, whether directly through Kaye-Smith or through one or more of its customers.

Once the incident was discovered, Kaye-Smith immediately took steps to address it. Working with outside experts, Kaye-Smith deployed industry-leading incident response tools and techniques and has no reason to believe that its systems are currently at risk.

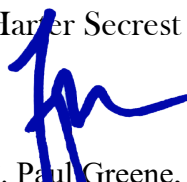
July 25, 2022
Page 2

Pursuant to Wash. Rev. Code Ann. § 19.255.010(7)(b), HSE on Kaye-Smith's behalf will provide updated information with respect to the information required under § 19.255.010(7)(a) when such information becomes known. Should you have questions in the meantime, please contact me.

Thank you.

Very truly yours,

Harter Secrest & Emery LLP



F. Paul Greene, CIPP/US, CIPP/E, CIPM, FIP
DIRECT DIAL: 585.231.1435
EMAIL: FGREENE@HSELAW.COM

FPG:meh