

EXHIBIT 1

This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Style Crest does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about December 15, 2021, Style Crest identified suspicious activity related to a Style Crest employee's email account. In response, Style Crest quickly took steps to secure its network, and began an investigation, which was aided by third-party forensic specialists, to determine the nature and scope of the activity. The investigation confirmed that certain Style Crest email accounts were accessed without authorization for limited periods between May 20, 2021 and December 15, 2021.

Given that certain email accounts were accessed without authorization, Style Crest then undertook a comprehensive and time-intensive review of the contents of the affected email accounts to understand the specific data present and to whom it related for purposes of providing notification to potentially impacted individuals. After this comprehensive review, which was again aided by third-party specialists, was complete, Style Crest worked diligently to review its internal records and leverage third-party resources to identify and confirm complete and accurate contact information for potentially impacted individuals in furtherance of providing notification. These efforts were completed on or around June 22, 2022, after which Style Crest worked to begin notifying potentially impacted individuals as quickly as possible.

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

Notice to Maine Residents

On July 22, 2022, Style Crest began providing written notice of this incident to potentially impacted individuals, which includes approximately two (2) Maine residents. Written notice is being provided in substantially the same form as the letter attached hereto as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, Style Crest moved quickly to investigate and respond to the incident, assess the security of Style Crest systems, and identify potentially affected individuals. Moreover, in response to the event, Style Crest instituted additional security measures to better protect against future similar incidents and is reviewing and enhancing its existing policies and procedures related to data protection and security, and providing additional training to employees regarding the importance of safeguarding data.

Additionally, as an added measure, Style Crest is providing access to credit monitoring services for twelve (12) months, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. Style Crest is also notifying other relevant regulatory authorities, as required.

Style Crest is also providing impacted individuals with guidance on how to better protect against identity theft and fraud, including providing individuals with 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.

EXHIBIT A



Return Mail Processing
PO Box 999
Suwanee, GA 30024

July 22, 2022

5 1 693 *****SNGLP

SAMPLE A. SAMPLE - L01

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



Re: Notice of Data [Extra3]

Dear Sample A. Sample:

Style Crest Enterprises, Inc. (“Style Crest”) writes to notify you of a recent event that may affect the security of some of your personal information. Please know that we take the privacy of your information very seriously. While we have no evidence that any of your information was used for identity theft or fraud as a result of this event, we are writing to provide you with information about the event, our response to it, and steps you may take to better protect your personal information, should you feel it appropriate to do so.

What Happened? On or about December 15, 2021, Style Crest identified suspicious activity related to a Style Crest employee’s email account. In response, we promptly launched an investigation to assess the security of our systems and to confirm the full nature and scope of the activity. This investigation revealed certain Style Crest email accounts were accessed for limited periods between May 20, 2021 and December 15, 2021. Given that certain accounts were accessed without authorization, Style Crest, with the assistance of data review specialists, undertook a comprehensive and time-intensive review of the contents of the affected email accounts to understand the specific data present and to whom it related for purposes of providing notification to potentially impacted individuals. This detailed review, which required several rounds of analysis was completed on or around June 22, 2022. Thereafter, we worked diligently to reconcile the information with our internal records in furtherance of identifying appropriate contact information so that notification to potentially impacted individuals could commence. We are notifying you because your information was present in the impacted email account(s), and therefore may have been accessed during this incident.

What Information Was Involved? The investigation determined the following types of your information were contained in an impacted email account(s): your name and [Extra1].

What We Are Doing. Safeguarding the privacy of information held in our care and the security of our network are among Style Crest’s highest priorities. Upon learning of this event, we promptly took steps to secure our environment, including resetting all passwords in our email tenant and conducted a thorough investigation. Further, as part of our ongoing commitment to the privacy of information in our care, we implemented additional technical security measures designed to mitigate recurrence of this type of incident. We are also reviewing and enhancing our existing data privacy policies and procedures, and providing additional training to employees regarding the importance of safeguarding data. Style Crest is also notifying relevant regulatory authorities, as required.

As an added precaution, Style Crest is also offering you access to twelve (12) months of credit monitoring and identity restoration services at no cost to you through Experian. Additional information regarding this offering and enrollment instructions are enclosed with this letter.

What You Can Do. As noted, **we have no evidence that any of your information was used for identity theft or fraud as a result of this event.** However, Style Crest encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity and to detect errors. Please also review the enclosed *Steps You Can Take to Help Protect Personal Information* for useful information on what you can do to better protect against possible misuse of your information. We also encourage you to enroll in the free credit monitoring services we are providing to you, as we are unable to take action on your behalf to enroll you.

For More Information. We recognize you may have questions not addressed by this letter. If you have additional questions, you may contact our dedicated assistance line at **(833) 420-2850** (toll free), which is available Monday through Friday, 9 a.m. to 11 p.m. EST; Saturday and Sunday, 11 a.m. to 8 p.m. EST, excluding major U.S. holidays.

We sincerely regret any inconvenience or concern this may have caused you.

Sincerely,

Style Crest Enterprises, Inc.

2450 Enterprise St.

Fremont, OH 43420

Steps You Can Take to Help Protect Personal Information

Enroll in Credit Monitoring Services

To help protect your identity, we are offering a complimentary 12-month membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: October 31, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(833) 420-2850** by **October 31, 2022**. Be prepared to provide engagement number **B058118** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **(833) 420-2850**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor 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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide 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, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or 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	1-833-395-6938
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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact

information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Style Crest is located at 2450 Enterprise Street, Fremont, OH 43420.

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 bureaus 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 violator. 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 https://files.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.