



Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
VIA EMAIL
idtheft@oag.state.md.us

November 13, 2023

Orrick, Herrington & Sutcliffe LLP

222 Berkeley Street
Suite 2000
Boston, MA 02116-3740
+1 617 880 1800
orrick.com

Heather Helen Egan
E hegan@orrick.com
D +1 617 880 1830
F +1 617 880 1801

RE: The Clorox Company – Notice of Security Incident

Dear Attorney General,

I am writing on behalf of our client, The Clorox Company (“Clorox”), to notify you of a cybersecurity event.

On August 11, 2023, Clorox identified that an unauthorized actor had accessed some of its IT systems. After becoming aware of the access, Clorox immediately began taking steps to stop and remediate the access, including taking certain systems offline. An investigation was then launched with assistance from external cybersecurity experts. Clorox subsequently discovered the unauthorized actor had accessed and/or acquired files containing personal information. Clorox also notified law enforcement.

Once Clorox was able to identify the affected files, Clorox began a process to determine who was affected and the types of information that was affected. On October 21, 2023, Clorox determined that the personal information associated with 3 Maryland residents was in the files. These individuals are current Clorox employees or employee relatives, dependents or beneficiaries. Depending on the individual, the types of personal information that were in the affected files include one or more of the following: home address, Social Security number, driver’s license number, bank account or routing number, username and passwords, PINs, or other access codes, or medical information.

Clorox began notifying these individuals on November 13, 2023, via email or U.S. First Class Mail. While Clorox is not aware of any evidence that personal information has been misused as a result of this incident, Clorox is offering each of these individuals two years of free credit monitoring and identity protection services from Experian.

Prior to the incident, Clorox had a number of cybersecurity measures in place, including endpoint detection and response tools across the environment. As Clorox brought systems back online, they took a series of steps to further strengthen their security controls.



A sample notice is attached as Attachment A to this letter. If your office requires any further information in this matter, please contact me at (617) 880-1830 or hegan@orrick.com.

Sincerely,

A handwritten signature in blue ink, appearing to be "HEG", with a stylized flourish at the end.

Heather Egan
Partner, Orrick Herrington & Sutcliffe LLP



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

November 13, 2023

K3034-L04-0000002 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L04 E
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



Re: Notice of Data Breach

Sample A. Sample:

We are writing to inform you that some of your personal information was recently involved in a cybersecurity incident. Please read this notice carefully, as it provides up-to-date information on what happened and what we are doing, as well as information on how you can obtain complimentary credit monitoring.

What happened?

On August 11, 2023, the Clorox Company ("Clorox") identified that an unauthorized actor had accessed some of our IT systems. After becoming aware of the access, we immediately began taking steps to stop and remediate the access, including taking certain systems offline. An investigation was then launched with assistance from external cybersecurity experts. We subsequently discovered the unauthorized actor had accessed and/or acquired files containing personal information. We also notified law enforcement.

What personal information was involved?

Once Clorox identified the accessed and/or acquired files, we began a process to determine what types of personal information were affected and to whom it relates.

Your personal information that was accessed and/or acquired included: [Extra2].

What we are doing:

Prior to the incident, Clorox had a number of cybersecurity measures in place, including endpoint detection and response tools across the environment. As we brought systems back online, we took a series of steps to further strengthen our security controls.

At this time, we are not aware of any evidence that personal information has been misused as a result of this incident. However, Clorox is offering you a complimentary 24-month membership to Experian's® IdentityWorksSM. This product provides you with 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**: February 1, 2024 (Your code will not work after this date.)
Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
Provide your **activation code**: **ABCDEFGHI**

Please see Attachment A for additional details regarding these services. **You must enroll by February 1, 2024, to receive these services.**

What you can do:

It is always a good idea to remain vigilant against threats of identity theft or fraud and to regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity. You can also enroll in the credit monitoring service being offered to you. Additional information about how to protect your identity and personal information is contained in Attachment B to this mailing.

For more information:

If you have questions, you can call the dedicated call center toll free Monday through Friday 6 a.m. – 8 p.m. PT, or Saturday and Sunday from 8 a.m. – 5 p.m. PT (excluding major U.S. holidays) at 800-630-9470. Please be prepared to provide engagement number B108206.

Sincerely,

Kirsten Marriner
Executive Vice President and Chief People and Corporate Affairs Officer

Encs. Attachment A
Attachment B

**Attachment A – ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN
IDENTITYWORKS MEMBERSHIP**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 800-630-9470 by February 1, 2024. Be prepared to provide engagement number B108206 as proof of eligibility for the Identity Restoration services by Experian.

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, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* 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.



Attachment B – More Information about Identity Protection

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

You can contact the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware 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. A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax	Experian	TransUnion
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
(888) 766-0008	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone +1 (877) 382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general, or the FTC.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023; or www.marylandattorneygeneral.gov.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the cybersecurity event. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; +1 (877) 566-7226 (Toll-free within North Carolina); +1 (919) 716-6400; or www.ncdoj.gov.

Oregon Residents: The Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; +1 (877) 877-9392 (toll-free in Oregon); +1 (503) 378-4400; or www.doj.state.or.us/.

For California, Iowa, Montana, New York, North Carolina, Oregon, Washington, and West Virginia 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).