

EXHIBIT 1

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, Ansell 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 September 30, 2025 (AEDT), Ansell became aware of claims relating to unauthorized access to certain sets of company data. Immediately following first awareness and containment, with assistance from experts across the cyber industry, Ansell took steps to investigate in line with its obligations to assess suspected data breaches. Recently following an extensive investigation, Ansell was able to validate the claims made. Through its investigation, Ansell determined that the unknown actor gained access to its systems on or around August 9, 2025. Ansell then undertook a review of the files identified as accessed in order to determine what information they contained and to whom the information was related. This review was recently completed and confirmed that the information that could have been subject to unauthorized access includes name and Social Security number.

Notice to Maine Resident

On or about March 10, 2026 Ansell provided notice of this incident to one (1) Maine resident. 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 incident, Ansell moved quickly to investigate and respond to the incident. To date, Ansell has identified personal information provided by Ansell employees during the course of their employment with the company. While Ansell is not yet aware of the impacted data being disclosed online (or any misuse events), out of an abundance of caution, Ansell is currently going through the process of notifying all employees globally about the incident. As part of this process, where available in a jurisdiction, Ansell is offering identity and/or credit monitoring services to all employees and their dependents. Ansell has also set up post-notification support pathways for any employees that have questions and concerns.

Additionally, where necessary, Ansell 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. Ansell is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

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

EXHIBIT A



Return Mail Processing
PO Box 999
Suwanee, GA 30024

7 3 1923 *****AUTO**ALL FOR AADC 085

SAMPLE A. SAMPLE - L01



APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



March 10, 2026

NOTICE OF [Extra2]

Dear Sample A. Sample:

Ansell Healthcare Products LLC USA (“Ansell”) is writing to inform you of a recent event that may impact the privacy of some of your information. We note some of you may have already received a notification from us in relation to the event. This letter contains further information about our response and resources available to you to help protect your personal information, should you feel it appropriate to do so.

What Happened? On September 30, 2025 (AEDT), Ansell became aware of claims relating to unauthorized access to certain sets of company data (the “Event”). Upon becoming aware of the Event, with the assistance of third-party cyber security specialists, Ansell promptly took steps to investigate the nature and scope of the Event. Following an extensive investigation, Ansell determined that an unknown actor gained access to Ansell’s systems on or around August 9, 2025, and that during that period of unauthorized access, certain files were accessed or copied by the unauthorized actor. Therefore, Ansell undertook a comprehensive and time-intensive review of the impacted data to determine what information was contained therein and to whom it related. That review was recently completed, and we are providing you with this supplementary notification after determining that information related to you was found in the impacted files.

What Information Was Involved? Based on our investigation to date of the impacted dataset, below is a list of the personal data that we have identified for you:

- [Extra1]

What We Are Doing. Ansell takes the confidentiality, privacy, and security of information in its care very seriously. Upon identifying this Event, we immediately commenced an investigation to confirm the nature and scope of the same, and to identify what information could have been affected. As an added precaution, we are also offering you at no cost to you a 12-month subscription to Norton LifeLock identity protection services. A description of the services and instructions on how to request details about this service can be provided to you upon request. Please note that you must complete the enrollment process yourself as we are not permitted to enroll you in these services.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next twelve (12) to twenty-four (24) months. We further encourage you to contact us to receive enrollment instructions regarding the complimentary services being provided by Norton LifeLock.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions please contact us at Response@ansell.com or alternatively at 1-800-800-0444. You may also write to us at 111 S Wood Ave, Iselin, New Jersey 08830

Sincerely,

Nathalie Ahlstrom

Chief Executive Officer

Deanna Johnston

Chief Information Officer

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To activate your subscription at no cost to you, please contact us at Response@ansell.com. Upon receipt, we will provide you with the relevant details to set up your subscription to Norton LifeLock. Please note you will have until **March 31, 2026** to enroll in this service.

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 1-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 credit freeze or fraud alert, 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/data-breach-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, 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, 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 law enforcement and the relevant 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 Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 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.