



Kevin J. Murphy
Division Vice President
Information Security and
Data Privacy

Corning Incorporated
One Riverfront Plaza
Corning, NY 14831
Address

t 607 974 9000
MurphyKJ@corning.com
corning.com

VIA FIRST CLASS MAIL AND EMAIL TO DOJ-CPB@DOJ.NH.GOV

April 12, 2019

New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
E-Mail: DOJ-CPB@doj.nh.gov

RE: Notice of Data Security Breach

Dear Sir or Madam:

Pursuant to N.H. Rev. Stat. § 359-C:20, we write to notify your office of an incident that may affect the security of personal information relating to one (1) New Hampshire resident. Corning's investigation into this event is ongoing and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Corning does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On March 12, 2019, Corning learned that on or about January 29, 2019, at least one dormant email account of an employee of an entity acquired by Corning was "spoofed" and was thereafter accessible by, and initiated later emails on behalf of, an unauthorized third party. That email account contained personally identifiable information provided to Corning by employees in connection with their employment. Although Corning has no evidence to suggest that private information was misused, the possibility that emails and/or attachments in the account were viewed by the unauthorized party could not be ruled out.

Corning takes data privacy and this incident very seriously. Immediately upon becoming aware of the incident, Corning took steps to block access to the account by resetting passwords and hired a leading forensics firm to help investigate. Through that investigation and following an extensive programmatic and manual review of the emails and attachments, Corning determined that an unauthorized party had access to records which may have included employee names, addresses, email addresses, and Social Security numbers.

Notice to New Hampshire Resident

On or about April 12, 2019, Corning mailed written notice of this incident to one (1) New Hampshire resident affected in the incident, in substantially the same form as the letter attached hereto and labeled as **Exhibit A**.

Other Steps Taken and To Be Taken

Upon discovering this incident, Corning immediately launched an investigation to determine the nature and scope of the event, as well as whose data may potentially be affected. Corning is mailing written notice to affected consumers and certain regulators. This notice includes guidance on how to better protect against identity theft and fraud, 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, and a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports. As an added precaution, Corning arranged to have Experian provide the affected individuals twelve (12) months of credit monitoring and identity restoration services at no cost to the individual. Corning is also providing notice of this event to other state and federal regulators as appropriate.

Corning has taken steps to ensure the security of the information it stores. As part of its ongoing efforts to help prevent another incident from occurring in the future, it is re-educating employees on cyber best practices and enhancing existing security measures by implementing two-factor authentication for remote email access for these accounts. Corning also implemented a forced password reset protocol across all affected systems, has removed all outside access to the accounts at issue, and subscribes to an email security program for inbound and outbound filtering and blocking of emails potentially containing personally identifiable information.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact me at (607) 974-4907 or MurphyKJ@corning.com.

Sincerely,

A handwritten signature in black ink, appearing to read "Kevin J. Murphy". The signature is fluid and cursive, with the first name "Kevin" and last name "Murphy" clearly distinguishable.

Kevin J. Murphy
Division Vice President
Information Security and Data Privacy
Corning Incorporated

Exhibit A – Template Notification for New Hampshire Resident

CORNING

Kevin J. Murphy
Division Vice President
Information Security and
Data Privacy

Corning Incorporated
One Riverfront Plaza
Corning, NY 14831

t 607 974 9000
MurphyKJ@corning.com
corning.com

April 11, 2019

[Name]
[Address]
[City, State, Zip]

RE: Important Security Notification. Please read this entire letter.

Dear [Name]:

At Corning, we respect the privacy of your information, which is why, as a precautionary measure, we are contacting you regarding a data security incident that occurred at Corning at the beginning of this year. This incident involved your Social Security Number, email address, and/or other personally identifying information that potentially may have been exposed due to the breach incident. Please be assured that we treat privacy issues with the utmost seriousness and have taken appropriate steps to address the incident.

It has specifically come to our attention that on or about January 29, 2019, at least one dormant email account of an employee of an entity acquired by Corning was “spoofed” and was thereafter accessible by, and initiated later emails on behalf of, an unauthorized third party. We have investigated the breach, and have confirmed that the vulnerability has been eliminated. Our investigation has uncovered no evidence that the unauthorized third party actually accessed any of your personal information. That said, you should not ignore the breach and we encourage you to take advantage of our offer and suggestions below to help ensure the safety of your identity.

We obviously regret this incident occurred. Our professionals have conducted a review of the potentially affected systems at issue, and, while we don’t expect there to be any, will notify you if there are any other significant developments. Corning has implemented additional security measures designed to prevent a recurrence of such an attack, and to protect the privacy of its present and former employees.

What we are doing to protect your information:

In addition to taking the steps necessary to close the vulnerability and minimize the likelihood of future attacks, to help protect your identity, we are offering a complimentary one-year membership of Experian’s® IdentityWorksSM product. 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: **July 31, 2019** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bplus>
- Provide your activation code: [code]

Additional details on Experian’s IdentityWorks product are attached to this letter. 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 1-877-890-9332 by **July 31, 2019**. Be prepared to provide engagement number **DB11773** as proof of eligibility for the identity restoration services by Experian. Please note that this Identity Restoration support is available to you for one year 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 <https://www.experianidworks.com/restoration-terms/>. You will also find self-help tips and information about identity protection at <https://www.experianidworks.com/restoration>.

Additional steps you may take to protect your information:

In addition to our actions and offer above, we recommend you also take steps to help protect yourself. As a first preventive step, we recommend you closely monitor your financial accounts and, if you see any unauthorized activity, promptly contact your financial institution.

As a second step, you may also want to contact the three U.S. credit reporting agencies (Equifax, Experian, and TransUnion) to obtain a free credit report from each by calling 1-877-322-8228 or by visiting www.annualcreditreport.com. Even if you do not see any suspicious activity on your initial credit reports, the Federal Trade Commission recommends that you check your credit reports periodically, as doing so can help you spot problems and address them quickly.

Finally, you may also want to consider placing a security freeze on your credit files, which would prevent an unauthorized person from using your personal identifying information to open new accounts or borrow money in your name. To do so, you would need to contact the three reporting agencies. There may be a fee for each agency to place the freeze, though fees may be waived if you can prove that identity theft has actually occurred. Keep in mind that you would not be able to borrow money, obtain instant credit, or get a new credit card unless you lift the freeze. You can contact the credit reporting agencies to obtain a security freeze or otherwise as follows:

Equifax: 1-888-298-0045; www.freeze.equifax.com

Experian: 1-888-EXPERIAN; www.experian.com/freeze.com

TransUnion: 1-800-680-7289; www.transunion.com/credit-freeze

Should you have questions or concerns regarding this matter, please do not hesitate to contact us using the following information:

Corning Incorporated - Global Data Privacy Office

One Riverfront Plaza

MP-HQ-W1-Z12

Corning, NY 14831

(607) 974-9000 or privacy@corning.com

We sincerely apologize for this incident, regret any inconvenience it may cause you, and thank you for your continued vigilance in helping us minimize its effects.

Sincerely,



Kevin J. Murphy

Division Vice President

Information Security and Data Privacy

Corning Incorporated

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, Equifax and Transunion files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **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.
- **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 [1-877-890-9332](tel:1-877-890-9332). 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).

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

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions