

1873349 Ontario, Inc.  
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>>

## Notice of Data Breach

Dear <<Name 1>>:

1873349 Ontario, Inc. understands the importance of protecting payment card information. We are writing to inform you of a recent security incident that may have involved your payment card information used to place an order on our website, [www.1800Flowers.ca](http://www.1800Flowers.ca) (the “Canadian Website”). The incident did not involve orders placed on the 1800Flowers.com website. This letter explains the incident, measures we have taken to remediate the incident, and steps you can take in response.

### What Happened?

Our security team was made aware of suspicious activity on the Canadian Website. We immediately began an investigation with the assistance of a leading computer security firm and disabled the website. On October 30, 2018, the investigation identified unauthorized access to payment card data from cards used to make purchases on the Canadian Website from August 15, 2014 to September 15, 2018.

### What Information Was Involved?

Findings from the investigation suggest that the information collected included your first and last name, payment card number, expiration date, and card security code. We are notifying you because you may have placed an order on the Canadian Website between August 15, 2014 and September 15, 2018 using a payment card ending in <<variable data – 4 digit CC #>>.

### What We Are Doing.

We take the security of our customers’ personal information very seriously. To help prevent a similar incident from occurring in the future, we have redesigned the Canadian Website and implemented additional security measures. We are also working with the payment card networks so that banks and other entities that issue payment cards can be made aware.

### What You Can Do.

We encourage you to closely review your payment card statements for any unauthorized charges. You should immediately report any such charges to the bank, credit union or credit card company that issued your card because payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported. The phone number to call is usually located on the back of your payment card. Also, please review the following page for more information on steps you can take.

**For More Information.**

If you have any questions, please call 888-842-3152, Monday through Friday, from 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

A handwritten signature in black ink, appearing to read "WES - E Shea". The signature is fluid and cursive.

William E. Shea  
Vice President  
1873349 Ontario, Inc.

## ADDITIONAL STEPS YOU CAN TAKE

We remind you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you detect any unauthorized activity on financial accounts, you should immediately contact your financial institution. We also recommend that you make your financial institution aware of this incident and take their advice on steps to protect your bank account. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

*Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742  
*TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800  
*Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

*Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)