



In care of ID Experts  
10300 SW Greenburg Road, Suite 570  
Portland, OR 97223

March 6, 2015

[Name]  
[Address1]  
[Address2]  
[City, State Zip]

Dear [First Name] [Last Name],

I write to inform you about a potential data incident at The Painted Turtle that may have involved some of your personal information.

The Painted Turtle is a non-profit organization that offers a fun, safe camp environment to thousands of children with life-threatening diseases and their families each year free of charge. Prospective campers and their families submit an online application in order to attend camp sessions at The Painted Turtle.

The incident involved an error in the database supporting The Painted Turtle's online application system for campers and volunteers. Because of this error, there is a chance that information that you provided in your online camper/family member application to The Painted Turtle may have been viewable by individuals you listed as a Medical Provider or Emergency Contact. If it was viewable, it would have included your name, address, personal medical information, and health insurance information. The online application did not request your Social security number, driver's license number, bank account number or credit card information and that information was therefore not viewable.

Your information would not have been viewable unless a specific chain of events occurred. Specifically: (1) you would have had to identify someone as a Medical Provider or Emergency Contact in your application in 2013–2014, *and* (2) that person would have had to begin filling out an application as well, *and* (3) while that person's application (and your application) was still pending, (4) they would have had to access their pending application and click "show related profiles" and your name. Again, your information would not have been accessible to anyone outside of the persons you listed as Medical Providers or Emergency Contacts in your application.

We became aware of this issue on January 12, 2015. As soon as this error was brought to our attention, we began taking steps to address and mitigate the risk to you. We immediately brought the database offline to prevent anyone from being able to access your records. Also, in

an effort to prevent similar data breaches in the future, before bringing the system back online we updated our database's code to prevent the issue from occurring again.

At this time, there is no evidence that your information has been misused. Nevertheless, we regret any adverse impact this incident may have on you and hope this notification will allow you to take action along with our own efforts to minimize or eliminate any potential harm to you.

We are working with ID Experts®, the data breach and recovery experts. Representatives from ID Experts have been fully versed on this incident and can answer questions or concerns you may have regarding protection of your personal information by calling 866-486-4814. ID Experts is available Monday through Friday from 6 am – 6 pm Pacific Time.

Sincerely,

A handwritten signature in black ink, appearing to read "Blake Maher", with a long horizontal flourish extending to the right.

Blake Maher  
The Painted Turtle

(Enclosure)

## Recommended Steps to Help Protect Your Information

**1. Telephone.** Contact ID Experts at 866-486-4814 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

**2. Protect Your Medical and Health Insurance Information.** We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please notify your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider or plan and request them to send such statements following the provision of services in your name or number.

Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your plan to serve as a baseline.

**3. Review your credit reports.** We recommend that you remain vigilant by monitoring your credit report for any medical bills that you do not recognize. Under federal law, you are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

When you receive your credit report, look it over carefully. Look for accounts that you did not open and medical bills that you do not recognize. If you discover any suspicious items call the credit reporting agency at the phone number on the report.

**Important note for minors:** In most cases, minors under the age of 18 may not have a credit file established yet. That being said, you will be able to pull copies of their reports to review. If you suspect someone is using your child's information, please contact TransUnion at [childidtheft@transunion.com](mailto:childidtheft@transunion.com).

**4. Right to file police report.** You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. Get a copy of the police report. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement, the Attorney General, or to the Federal Trade Commission.

**5. Place Fraud Alerts** with the three credit bureaus. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

### Credit Bureaus

Equifax Fraud Reporting  
1-800-525-6285  
P.O. Box 740241  
Atlanta, GA 30374-0241  
[www.alerts.equifax.com](http://www.alerts.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
Fraud Victim Assistance Division  
P.O. Box 6790  
Fullerton, CA 92834-6790  
[www.transunion.com](http://www.transunion.com)

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. A fraud alert lasts 90 days. You can keep the fraud alert in place by calling again after 90 days.

**6. Security Freeze.** If you are concerned that you may be a victim of identity theft, you may place a security freeze on your credit files. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze varies by the state you live in and for each credit reporting agency. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.

**7. For more information about child identity theft,** please visit <http://www.consumer.ftc.gov/articles/0040-child-identity-theft>.

**8. You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

**For California Residents:**

Visit the California Office of Privacy Protection ([www.privacy.ca.gov](http://www.privacy.ca.gov)) for additional information on protection against identity theft

**For Maryland Residents:**

Office of the Attorney General of Maryland  
Consumer Protection Division  
200 St. Paul Place  
Baltimore, MD 21202  
[www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer)  
Telephone: 1-888-743-0023

**For all US Residents:**

Identity Theft Clearinghouse  
Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
[www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)  
1-877-IDTHEFT (438-4338)  
TDD: 1-202-326-2502

**For Kentucky Residents:**

Office of the Attorney General of Kentucky  
700 Capitol Avenue, Suite 118  
Frankfort, Kentucky 40601  
[www.ag.ky.gov](http://www.ag.ky.gov)  
Telephone: 1-502-696-5300

**For North Carolina Residents:**

Office of the Attorney General of North Carolina  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
[www.ncdoj.com/](http://www.ncdoj.com/)  
Telephone: 1-919-716-6400