May 26, 2015

VIA FEDERAL EXPRESS

Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Potential Security and Data Breach Involving Protected Information

Dear Sir/Madam:

We have recently learned that the personal information of certain clients and/or potential clients held by Unity Recovery Group, Inc. and/or its affiliated companies, including Starting Point Detox, LLC, Lakeside Treatment Center, LLC, Changing Tides Transitional Living, LLC, and Unity Recovery Center, Inc. (collectively "Unity"), was improperly disclosed to one or more recovery and/or rehabilitation service providers, unaffiliated with Unity, without prior written consent from the respective client or potential client. Unity's facilities operate in the State of Florida and provide alcohol and drug rehabilitation services to individuals from across the United States.

In April 2015, Unity learned that the personal information of the affected individuals disclosed to the unaffiliated recovery and/or rehabilitation service providers may include an individual's name, address, date of birth, address, telephone number, social security number, e-mail address, insurance information, and/or certain health-related information. The incidents giving rise to this notice occurred between April 2014 and March 2015, however, our investigation has revealed that the disclosure included less than 1,000 individuals' personal information. The individuals affected reside in several states, none of which includes more than 500 affected individuals. While we have not received any indication that the information disclosed has been accessed or used for any other purpose, we are required to obtain prior written consent before disclosing personal information, with limited exception.

Unity has notified the Secretary of the U.S. Department of Health and Human Services, as required by the rules implementing the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and is continuing to investigate how this breach happened in light of our Privacy Policy, Client Confidentiality Policy, Conflict of Interest Policy, and IT security policies (together "Unity's Policies"). To protect against future incidents, we have undertaken additional technological security measures and implemented additional training of our employees to ensure compliance with Unity's Policies. We have also hired outside legal counsel to assist us with our

investigation and Forensic Data Services, Inc., a technology forensics firm, to enhance the security of our IT systems.

A notification of the data security breach will be sent on May 26, 2015 to the four (4) affected individuals residing in the State of New Hampshire. An example notification letter sent to affected consumers is enclosed with this letter. For those individuals for whom Unity does not have valid contact information, Unity will post the form of the notification letter on its primary websites: www.unityrehab.com and www.unityrecovery.com for a period of 90 days pursuant to HIPAA.

In keeping with our commitment to patient privacy, we have arranged to provide potentially affected individuals with a complimentary one-year subscription to ID Experts®, a leading identity and credit protection service. Unity is not affiliated in any way with ID Experts, however, their services have come highly recommended. For those individuals who opt-in to the services offered, ID Experts will assist them with placing a "Fraud Alert" on their credit reports and provide 12 months of credit and CyberScan monitoring, a $20,000 insurance reimbursement policy, Healthcare Identity Protection Toolkit™, exclusive educational materials and complete access to their fraud resolution representatives. With this protection, ID Experts will help individuals to resolve issues if their identity is compromised.

Unity also enclosed an information sheet in its notification to potentially affected individuals called "**What You Can Do To Protect Yourself**" which outlines steps individuals can take now to protect themselves.

A call center has been set up at 1-888-262-4479 to answer questions related to this incident. Written inquiries may be directed to Steve Kolb, Unity's Chief Operations Officer, via e-mail at contact@urgmanagement.com.

We sincerely apologize for any difficulties or inconvenience that may be caused by this incident.

Sincerely,

Jason Ackner, CEO

Unity Recovery Group, Inc.
630 US Highway 1, Floor 4
North Palm Beach, FL 33408

SAMPLE
NOTIFICATION
LETTER

May 26, 2015

We have recently learned that your personal information, held by Unity Recovery Group, Inc. and/or its affiliated companies, including Starting Point Detox, LLC, Lakeside Treatment Center, LLC, Changing Tides Transitional Living, LLC, and Unity Recovery Center, Inc. (collectively "Unity"), was improperly disclosed to one or more recovery and/or rehabilitation service providers, unaffiliated with Unity, without your prior written consent.

At Unity, we take patient privacy very seriously and it is important to us that you are made fully aware of a potential privacy issue that may affect you. In April 2015, we learned that your personal information, which may include your name, address, date of birth, address, telephone number, social security number, e-mail address, insurance information, and/or certain health-related information, was impermissibly disclosed. The incidents giving rise to this notice occurred between April 2014 and March 2015 and involved the disclosure of your personal information to one or more unaffiliated recovery and/or rehabilitation service providers, without your prior written consent. While we have not received any indication that the information disclosed has been accessed or used for any other purpose, we are required to obtain your prior written consent before disclosing your personal information, with limited exception.

We are complying with our regulatory notice obligations and continue to investigate how this breach happened in light of our Privacy Policy, Client Confidentiality Policy, Conflict of Interest Policy, and IT security policies (together "Unity's Policies"). To protect against future incidents, we have undertaken additional technological security measures and implemented additional training of our employees to ensure compliance with Unity's Policies. We have also hired outside legal counsel to assist us with our investigation and Forensic Data Services, Inc., a technology forensics firm, to enhance the security of our IT systems. We will notify you if there are any significant developments that may affect you.

In keeping with our commitment to patient privacy, we have arranged for a complimentary one-year subscription for you to ID Experts®, a leading identity and credit protection service. Unity is not affiliated in any way with ID Experts, however, their services have come highly recommended. If you seek the benefits of their services, ID Experts will also assist you with placing a "Fraud Alert" on your credit reports. If you would like to receive this service, the ID Experts fully managed recovery services will include: 12 months of credit and CyberScan monitoring, a $20,000 insurance reimbursement policy, Healthcare Identity Protection Toolkit™, exclusive educational materials and complete access to their fraud resolution representatives. With this protection, ID Experts will help you resolve issues if your identity is compromised. We encourage you to contact ID Experts with any questions and to enroll in the free services by calling 1-888-262-4479 or by going to www.idexpertscorp.com/protect. ID Experts is available Monday through Friday from 9:00 AM – 9:00 PM Eastern Time.

If you have not received a notification letter via email or through US Postal Mail and believe you may be an affected individual, we encourage you to contact ID Experts at 1-888-262-4479. If your information was involved, you can call and be enrolled in the services being offered.

Please note, the deadline to call and enroll with ID Experts is August 26, 2015.

If you do not wish to use the services offered through ID Experts, we recommend that you place a fraud alert on your credit files. A fraud alert requires potential creditors to use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. A fraud alert lasts for 90 days. To place a fraud alert, call one of the three credit reporting agencies at the telephone number found below. This will allow you to automatically place an alert with all of the agencies. You will receive letters from all three agencies to confirm the fraud alert and to let you know how to get a free copy of your credit report.

Equifax	TransUnion	Experian
P.O. Box 740241	P.O. Box 2000	P.O. Box 9532
Atlanta, GA 30374-0241	Chester, PA 19022	Allen, TX 75013
1-800-685-1111	1-800-680-7289	1-888-397-3742
www.equifax.com	www.transunion.com	www.experian.com

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquires by creditors that you did not initiate. And look for personal information such as home address or social security number that is not accurate. If you see anything you do not understand or find to be suspicious, call the credit reporting agency on the number listed on the report. Likewise, if you do find suspicious activity on your credit reports, call your local police or Sherriff's office and file a police report of identity theft. Get a copy of the police report. You may need to provide copies of the police report to creditors to clear up your records.

We understand that this may inconvenience you and wish to assure you that Unity is committed to providing quality care, including protecting your personal information. We have enclosed an information sheet for you called "**What You Can Do To Protect Yourself**" which outlines steps you can take now to protect yourself.

A call center has been setup at 1-888-262-4479 to answer your questions related to this incident.

We sincerely apologize for any difficulties or inconvenience that you may experience as a result of this incident.

Sincerely,

Jason Ackner, CEO
Unity Recovery Group, Inc.

What You Can Do To Protect Yourself

✓ **Website and Enrollment.** Go to www.idexpertscorp.com/protect and follow the instructions for enrollment using your Access Code provided above. Once you have completed your enrollment, you will receive a welcome letter by email (or by mail if you do not provide an email address when you sign up). The welcome letter will direct you to the exclusive ID Experts' Member Website where you will find other valuable educational information.

✓ **Activate the credit monitoring** provided as part of your membership with ID Experts. Credit and CyberScan monitoring are included in the membership, but you must personally activate it for it to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, ID Experts will be able to assist you.

✓ **Be vigilant about your credit reports.** Even if you do not find any signs of fraud on your credit reports, we recommend that you check your credit reports periodically. You can keep the fraud alert in place by calling again in 90 days. For more information on identity theft, we suggest you visit the web site for the Office of the Attorney General for the State of Florida at http://myfloridalegal.com/identitytheft. You may also wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft by visiting http://www.ftc.gov/idtheft or by calling 1-877-ID-THEFT (877-438-4338). A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.

You should also contact the fraud department of each of your creditors. Gather the contact information for each of your credit accounts (credit cards, utilities, cable bills, etc.) and call the fraud department for each creditor. Report the incident to each creditor, even if your account at that institution has not been tampered with. Close any accounts that you believe have been compromised. Ask the credit bureaus to place an "alert" on any accounts that remain open.

✓ **Be cautious about your personal security.** Because the information included your home address, we want you to be cautious about your personal security. Once you've taken these precautions, watch for signs that your information is being misused. For example, you may not get certain bills or other mail on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks. Other signs include:

- receiving credit cards that you didn't apply for;
- being denied credit, or being offered less favorable credit terms, like a high interest rate, for no apparent reason; and
- getting calls or letters from debt collectors or businesses about merchandise or services you didn't buy.

If you believe at any time that your information is actually being misused, do the following:

✓ **Close any accounts that you believe have been tampered with or opened fraudulently.** If you discover that someone used your personal information to tamper with bank, credit or utility accounts, or to open new ones, close those accounts immediately. If a thief has made any charges any debts, ask the company to send a fraud dispute form so that you can dispute those charges or debts.

✓ **Call the police.** Get a copy of the police report so that you can show the report to creditors if they ask.

✓ **File a complaint with the Federal Trade Commission (FTC).** Call the FTC's Identity Theft Hotline at 1-877-438-4338. The FTC enters consumer complaints into the Consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and other countries. The FTC counselors will take your complaint and advise you on how to deal with any problems that result from the theft of personal information. For free information on consumer issues, visit *www.ftc.gov* or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261.