QUIXTAR
NORTH AMERICA
Amway
GLOBAL

June 11, 2008

Ms Kelly A. Ayotte, Attorney General
Department of Justice
33 Capitol Street
Concord, NH 03301

Re: **Reporting of Security Incident**

Dear Ms. Ayotte:

On behalf of Quixtar Inc., I am writing to inform you that six New Hampshire residents are receiving a notification of a security incident that was identified on Quixtar.com on May 27, 2008. Quixtar discovered that some Quixtar.com user account passwords and user IDs had been compromised, that someone was accessing these accounts and, in some cases, changing deposit bank account information. Quixtar believes that these acts were performed with the fraudulent intent to divert bonus payments earned by the independent business owners who use the Quixtar.com website. Notification letters were sent on June 11, 2008 to those Quixtar.com users whose accounts are believed to have been fraudulently accessed.

Quixtar is still in the process of investigating this incident, but has found no evidence that the perpetrators of this fraud obtained user names and passwords through any security breach at Quixtar.com. Moreover, even though these fraudsters were able to access some user accounts, they were not able to view social security, bank account, credit card or drivers license number information.

Quixtar does not believe that this incident has triggered any duty of notification under New Hampshire law, but Quixtar thought it prudent to alert Quixtar.com website users of the incident. As a courtesy, I am notifying you of the incident and including copies of the letters that have been sent to the IBOs. Quixtar has also alerted the FBI about the incident and is cooperating in the FBI's investigation.

5101 Spaulding Plaza, Ada, Michigan 49355

If you have any questions about this incident, you may contact me at (616) 787-6742.

Very truly yours,

Jon A. Sherk
Director and Associate General Counsel
International / Core Legal

cc: Dirk Bloemendaal, Alticor Corporate Government Affairs

QUIXTAR
NORTH AMERICA
Amway
GLOBAL

COPY

June 11, 2008

Dear IBO,

On May 30 we sent out email communications and posted a "What's New" article at Quixtar.com explaining that Quixtar had discovered some fraudulent activity involving compromised user IDs and passwords of some Independent Business Owners. Since then we have placed calls to Independent Business Owners we know were affected by this incident, including you.

We have determined that an intruder was able to access your Quixtar account using your IBO identification number and password combination, which we believe were obtained from an external web site. The intruder then changed the bank account information in an effort to divert your Quixtar bonus income. We assure you that the security of Quixtar.com has not been compromised nor was this person able to access your credit card, bank account or social security numbers, as this information is not viewable on our web site. Also, please be assured that no bonus payments have been lost and that you will receive all payments to which you are entitled. We are taking the precaution this month of issuing paper checks for any IBO whose banking deposit information has changed in any way since March.

To protect your account, we scramoled your password on June 4, 2008, effectively barring access to your account by the intruder. If you have not logged on since then, you will find that on your next visit you will need to create a new password following the prompts provided. We apologize for the inconvenience this may cause, but we wanted to do all we could to protect your account information.

Unfortunately, criminal activity on the Internet means that we all have to use caution. On the following pages are some suggestions, guidelines, and resources for your use.

We take this incident very seriously and will continue investigating. We also have provided information to the FBI about the incident and are cooperating with their investigation. In the coming weeks, you may notice some changes to the Quixtar site as we implement additional protections to safeguard your personal information.

If you have any questions, please contact Customer Support at 800-253-6500 Monday through Friday 8 a.m. to Midnight and Saturday 8:30 a.m. to 5 p.m. ET.

Sincerely,

S C Lieberman

Steve Lieberman
Managing Director

SUGGESTIONS & RESOURCES TO PROTECT YOUR PERSONAL INFORMATION

- Make sure you have up-to-date anti-virus, anti-spyware and firewall software on computers you use to access Quixtar.com or conduct other transactions. After running scans using this software, you should delete any viruses found, and then you may want to again change your password and verify that all account information is accurate.

- You should use separate passwords at different sites, so that if that information is discovered at one site, it does not put you at risk at all other sites where you also use those passwords. Use strong passwords that include numerals and upper and lower case alphabetical characters. It is advised that you change your passwords every 30 to 90 days.

- Be cautious about websites that you visit and any attachments to e-mail messages you receive, even when they appear to be from people you trust. These attachments or linked websites may appear legitimate but may actually contain malicious code that exploits vulnerabilities in operating systems that are not kept up to date. Some sites can plant malicious software on your computer that can track your every keystroke. Also, you should be suspicious of any e-mail that asks you to click on a link and provide user name, password, or account information.

- If you have children who use these computers, talk to them about the risks of downloading "free" games, using file-sharing programs, or clicking on pop-up messages. A good source of information about how to protect yourself from these kinds of risks can be found at http://www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm, provided by the Federal Trade Commission.

- Remain vigilant for identity fraud. You should monitor your bank and credit card statements and you may want to periodically review your credit report. You are entitled to a free copy of your credit report every 12 months from each of the three national credit bureaus, and if you stagger these reports, you can obtain a free report every four months. To request a free report, please visit the annual credit report website at www.annualcreditreport.com, or call 877-322-8228. See the attached credit bureau information sheet for more information about each credit bureau.

- If you suspect someone may be trying to use your personal information to commit fraud, you should report such activity to your local law enforcement agency and to the Federal Trade Commission. If police reports have been filed in connection with such activity, you may have a right under your state's law to obtain copies of such reports. You may also obtain a security freeze on your credit file by sending a written request to one of the credit bureaus – see the attached credit bureau information sheet for more information. The security freeze will prohibit third parties from accessing your credit report without your authorization.

QUIXTAR
NORTH AMERICA
Amway
GLOBAL

COPY

June 11, 2008

Dear IBO,

On May 30 we sent out email communications and posted a "What's New" article at Quixtar.com explaining that Quixtar had discovered some fraudulent activity involving compromised User IDs and passwords of some Independent Business Owners.

We have determined that an intruder was able to access a small number of IBO accounts and unfortunately yours was one affected. This intruder gained access to your Quixtar account using your IBO identification number and password combination, which we believe were obtained from an external web site linked to Quixtar. So what does this mean? It does not appear that any fraudulent activity occurred on your account. No information about your account was changed by the intruder, nor was this person able to access your credit card, bank account or social security numbers, as this information is not viewable on our web site. The intruder however, knows your passcodes.

Because your account was at risk, however, on June 4, 2008, we scrambled your password. If you have not logged on since then, you will find that on your next visit you will need to create a new password, following the prompts provided. We apologize for the inconvenience this may cause, but we wanted to do all we could to protect your account information.

Unfortunately, criminal activity on the Internet means that we all have to use caution. On the following pages are some suggestions, guidelines, and resources for your use.

We take this incident very seriously and will continue investigating. We also have provided information to the FBI about the incident and are cooperating with their investigation. In the coming weeks, you may notice some changes to the Quixtar site as we implement additional protections to safeguard your personal information.

If you have any questions, please contact Customer Support at 800-253-6500 Monday through Friday 8 a.m. to Midnight and Saturday 8:30 a.m. to 5 p.m. ET.

Sincerely,

S C Lieberman

Steve Lieberman
Managing Director

5101 Spaulding Plaza, Ada, Michigan 49355

SUGGESTIONS & RESOURCES TO PROTECT YOUR PERSONAL INFORMATION

- Make sure you have up-to-date anti-virus, anti-spyware and firewall software on computers you use to access Quixtar.com or conduct other transactions. After running scans using this software, you should delete any viruses found, and then you may want to again change your password and verify that all account information is accurate.

- You should use separate passwords at different sites, so that if that information is discovered at one site, it does not put you at risk at all other sites where you also use those passwords. Use strong passwords that include numerals and upper and lower case alphabetical characters. It is advised that you change your passwords every 30 to 90 days.

- Be cautious about websites that you visit and any attachments to e-mail messages you receive, even when they appear to be from people you trust. These attachments or linked websites may appear legitimate but may actually contain malicious code that exploits vulnerabilities in operating systems that are not kept up to date. Some sites can plant malicious software on your computer that can track your every keystroke. Also, you should be suspicious of any e-mail that asks you to click on a link and provide user name, password, or account information.

- If you have children who use these computers, talk to them about the risks of downloading "free" games, using file-sharing programs, or clicking on pop-up messages A good source of information about how to protect yourself from these kinds of risks can be found at http://www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm, provided by the Federal Trade Commission.

- Remain vigilant for identity fraud. You should monitor your bank and credit card statements and you may want to periodically review your credit report. You are entitled to a free copy of your credit report every 12 months from each of the three national credit bureaus, and if you stagger these reports, you can obtain a free report every four months. To request a free report, please visit the annual credit report website at www.annualcreditreport.com, or call 877-322-8228. See the attached credit bureau information sheet for more information about each credit bureau.

- If you suspect someone may be trying to use your personal information to commit fraud, you should report such activity to your local law enforcement agency and to the Federal Trade Commission. If police reports have been filed in connection with such activity, you may have a right under your state's law to obtain copies of such reports. You may also obtain a security freeze on your credit file by sending a written request to one of the credit bureaus – see the attached credit bureau information sheet for more information. The security freeze will prohibit third parties from accessing your credit report without your authorization.

CREDIT BUREAU INFORMATION SHEET

Credit Bureau	Phone	Address for requesting security freeze	Information needed to request security freeze	Cost of security freeze
Equifax	800-685-1111 www.equifax.com	Equifax Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	Name, address, date of birth, Social Security Number, proof of current address (such as a current utility bill), payment of any applicable fees. If you are a victim of identity theft, you must also include a copy of police report, identity theft report, or other government law enforcement agency report For more information, visit the Equifax security freeze information page at: http://www.equifax.com/cs/Satellite?c=EFX_ContentRoot&cid=1162203975981&pagename=5-1%2F5-1_Layout	No more than $20 (plus any applicable tax) For more information about costs in your state, visit the Equifax security freeze information page
Experian	888-397-3742 www.experian.com	Experian Attn: Experian Security Freeze P.O. Box 9554 Allen, TX 75013	Full name, Social Security number, date of birth; current address and previous addresses for the past two years, a copy of a government issued identification card, such as a drivers license, state or military ID card; a copy of a utility bill, bank or insurance statement; plus any applicable fee or a valid investigative or incident report or complaint with a law enforcement agency For more information, visit the Experian security freeze information page at: http://www.experian.com/consumer/security_freeze.html	No more than $20 (plus any applicable tax) For more information about costs in your state, visit the Experian security freeze information page
TransUnion	800-916-8800 www.transunion.com	TransUnion Attn: TransUnion Fraud Victim Assistance Department P.O. Box 6790 Fullerton, CA 92834	Name, address, Social Security number, proof of current address (such as state issued identification card or driver's license), and a credit card number and expiration date to pay any applicable fee For more information, visit the TransUnion security freeze information page at http://www.transunion.com/corporate/personal/fraudIdentityTheft/preventing/securityFreeze.page	No more than $20 (plus any applicable tax) For more information about costs in your state, visit the TransUnion security freeze information page