

CELEBRATING 50 YEARS



5101 Spaulding Plaza Ada, MI 49355-0001

May 6, 2009

New Hampshire Department of Consumer Affairs  
New Hampshire Attorney General's Office  
33 Capitol Street  
Concord, NH 03301

Re: **Reporting of Security Incident**

To Whom It May Concern:

On behalf of Amway Corp. d/b/a Amway Global, I am writing to inform you that on April 28, 2009, Amway Global discovered unauthorized access to some user accounts, including the accounts of five New Hampshire residents, at the AmwayGlobal.com (also known as Quixtar.com) website. Amway Global discovered that some user account passwords and user IDs had been compromised, one or more unauthorized individuals were accessing these accounts and, in some cases, changing deposit bank account information and other account information. Amway Global believes that these acts were performed with the fraudulent intent to divert bonus payments earned by the independent business owners who use the AmwayGlobal.com website and to collect data for identity theft. The intruders were able to view the New Hampshire residents' name, mailing address, telephone number, e-mail address and, in the case of two New Hampshire residents, social security numbers.

Notification letters were sent on May 6, 2009 to those AmwayGlobal.com users whose accounts are believed to have been fraudulently accessed. I am attaching a copy of the form letters that Amway Global is using to notify New Hampshire residents affected by this incident.

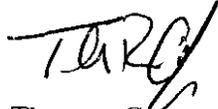
Amway Global is still in the process of investigating this incident, but has found no evidence that the perpetrators of this fraud obtained user names and passwords through any security breach at AmwayGlobal.com. Amway Global does not know where the breach occurred, the date of the breach or the number of individuals affected. Amway Global, however, has scrambled the password and password hint question for those users of its website that are affected and they will have to call Amway Global to reestablish access to their accounts. Amway Global has also modified the site to remove access to social security numbers and is offering credit monitoring services at Amway Global's expense to individuals who had social security numbers accessible to the intruders. Amway Global has notified and is cooperating with the FBI and will continue to provide information to the FBI as Amway Global learns more.

New Hampshire Department of Consumer Affairs  
May 6, 2009  
Page 2

---

If you have any questions about this incident, you may contact me at (616) 787-6304.

Very truly yours,



Thomas Curran  
Associate General Counsel  
Amway Global

cc: Dirk Bloemendaal, Alticor Corporate Government Affairs

## **SUBJECT: Alert: Suspicious Activity on your Account**

Dear \_\_\_\_\_:

Amway Global is investigating unauthorized activity that has impacted the accounts of a small number of Independent Business Owners (“IBOs”). We want to reassure you that based on our investigation to date; the incidents do not appear to involve a breach of the security infrastructure of the Amway Global website nor have any bonus payments been affected. At this time, we do not know where or when the breach occurred, but it appears that one or more intruders obtained a list of identification numbers and passwords for a group of Amway Global IBOs from an unidentified source, and used those same numbers and passwords to gain IBO account access at the Amway Global site.

Although the intruders were only able to access a small number of IBO accounts, yours was one that was accessed. So what does this mean for you? The intruders know your password. According to our records, the intruders gained access to your account and may have modified some of your account information. The intruders may have been able to view and /or change your name, mailing address, e-mail address, telephone number, and other account information at the Amway Global website, and may have been able to change your Bonus method of payment preference.

To protect your account, we scrambled your password and password hint question and answer on May 5, 2009, effectively preventing access by the intruder. If you have not logged on since then, you will find that on your next visit you will need to contact Customer Support at 800 253-6500 to set up a new password and password hint question and answer. Once you regain account access, please check your account information and correct any inaccuracies. We recommend that you do not use your Amway Global website account user ID and password on other websites, but if you have in the past, you should change those, as well.

Amway Global is committed to maintaining the highest level of security and privacy of information submitted to its website. There are many best practices you can follow to help protect your privacy online. On the following pages are some suggestions, guidelines, and resources for your use.

We take this incident very seriously and are diligently continuing our investigation. We have also provided information to the FBI about the incident and will continue to share information with the FBI as we learn more.

Sincerely,

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 AmwayGlobal.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 password 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 you can 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](http://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 <a href="http://www.equifax.com">www.equifax.com</a>	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: <a href="http://www.equifax.com/cs/Satellite?c=EFX_ContentRoot&amp;cid=1165203975981&amp;pagename=5-1%2F5-1_Layout">http://www.equifax.com/cs/Satellite?c=EFX_ContentRoot&amp;cid=1165203975981&amp;pagename=5-1%2F5-1_Layout</a>	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 <a href="http://www.experian.com">www.experian.com</a>	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: <a href="http://www.experian.com/consumer/security_freeze.html">http://www.experian.com/consumer/security_freeze.html</a>	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 <a href="http://www.transunion.com">www.transunion.com</a>	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: <a href="http://www.transunion.com/corporate/personal/fraudIdentityTheft/preventing/securityFreeze.page">http://www.transunion.com/corporate/personal/fraudIdentityTheft/preventing/securityFreeze.page</a>	No more than \$20 (plus any applicable tax)  For more information about costs in your state, visit the TransUnion security freeze information page.

## **SUBJECT: Alert: Suspicious Activity on your Account**

Dear \_\_\_\_\_:

Amway Global is investigating unauthorized activity that has impacted the accounts of a small number of Independent Business Owners (“IBOs”). We want to reassure you that, based on our investigation to date, the incidents do not appear to involve a security breach at the Amway Global website nor have any bonus payments been affected. At this time, we do not know where or when the breach occurred, but it appears that one or more intruders obtained a list of identification numbers and passwords for a group of Amway Global IBOs and used those same numbers and passwords to gain IBO account access at the Amway Global site.

Although the intruders were able to access only a small number of IBO accounts, yours was one that was accessed. So what does this mean for you? The intruders know your password. The intruders may have been able to view and /or change your name, mailing address, e-mail address, telephone number, and other account information at the Amway Global website, and may have been able to change your Bonus method of payment preference. Also, the intruders were able to access your registration form, which includes your social security number.

To protect your account, we scrambled your password and password hint question and answer on May 5, 2009, effectively preventing access by the intruders. If you have not logged on since then, you will find that on your next visit you will need to contact Customer Support at 800 253-6500 to set up a new password and password hint question and answer. Once you regain account access, you should check your account information and correct any inaccuracies. We recommend that you do not use your Amway Global website account user ID and password on other websites, but if you have in the past, you should change those, as well.

Because the intruders were able to access your social security number, Amway Global is making available to you a credit monitoring service at no cost to you for a period of one year. If you would like to take advantage of this service, please call Customer Support and ask to speak with Gail Playford, Manager of Accounts Receivable, to discuss the options that Amway Global is making available to you. To view information about these options, please visit <http://www.identitytheflubs.com/>. On the following pages are some additional suggestions, guidelines and resources for your use.

We take this incident very seriously and are diligently continuing our investigation. We have also provided information to the FBI about the incident and will continue to share information with the FBI as we learn more.

Sincerely,

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 AmwayGlobal.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 password 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 you can 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](http://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 <a href="http://www.equifax.com">www.equifax.com</a>	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: <a href="http://www.equifax.com/cs/Satellite?c=EFX_ContentRoot&amp;cid=1165203975981&amp;pagename=5-1%2F5-1_Layout">http://www.equifax.com/cs/Satellite?c=EFX_ContentRoot&amp;cid=1165203975981&amp;pagename=5-1%2F5-1_Layout</a>	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 <a href="http://www.experian.com">www.experian.com</a>	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: <a href="http://www.experian.com/consumer/security_freeze.html">http://www.experian.com/consumer/security_freeze.html</a>	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 <a href="http://www.transunion.com">www.transunion.com</a>	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: <a href="http://www.transunion.com/corporate/personal/fraud/identityTheft/preventing/securityFreeze.page">http://www.transunion.com/corporate/personal/fraud/identityTheft/preventing/securityFreeze.page</a>	No more than \$20 (plus any applicable tax)  For more information about costs in your state, visit the TransUnion security freeze information page.