

KIM — WLC ✓

COPY

North Carolina Security Breach Reporting Form Pursuant to the Identity Theft Protection Act of 2005

Name of Business Owning or Licensing Information Affected by the Breach: MILITARY OFFICERS ASSN. OF AMERICA
Address: 201 N. WASHINGTON ST. ALEXANDRIA, VA 22314
Telephone: 1-800-234-6622
Fax: 703-838-8173
Email: wylie@maa.org

PLEASE SUBMIT FORM TO: Consumer Protection Division NC Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001 Telephone: (919) 716-6000 Toll Free in NC: (877) 566-7226 FAX: (919) 716-6050

Date Security Breach Reporting Form submitted: 9 NOV 2007
Date the Security Breach was discovered: 1 NOV 2007 (REPORTED TO MAAA 4 NOV)
Estimated number of affected individuals: 259,497
Estimated number of NC residents affected: 9,540 9,813

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b)): CONVIO, BLDG. 5, SUITE 200, 11400 BURNET ROAD, AUSTIN, TEXAS 78758

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: PLEASE SEE ATTACHED E-MAIL FROM CONVIO, DESCRIBING THEM

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner: YES If so, please describe the security measures protecting the information: PLEASE SEE ATTACHED E-MAIL FROM CONVIO

Describe any measures taken to prevent a similar Security Breach from occurring in the future: PLEASE SEE ATTACHED E-MAIL FROM CONVIO

Date affected NC residents were/will be notified: 9 NOV 2007

If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (c): DELAY DUE TO DETERMINING TO WHOM THE E-MAIL ADDRESSES AND PASSWORDS BELONGED

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the written request or the contemporaneous memorandum.

How NC residents were/will be notified? (pursuant to N.C.G.S. § 75-65(e))
Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.
[X] written notice
[X] electronic notice (email)
[] telephone notice
[] substitute notice

Signature: P. Wylie Date: 9 NOV 2007
Contact Person, Title: PETER C. WYLIE, SEC'Y & GEN. COUNSEL
Address: SAME AS ABOVE
Telephone: 1-800-234-6622, EXT. 166 Fax: 703-838-8173 Email: wylie@maa.org

Pete Wylie

From: Gene Austin [client-communication@info.convio.com]
Sent: Tuesday, November 06, 2007 7:32 PM
To: Julie Huebsch
Subject: Convio Security Update and Constituent Support Information



Dear Julie,

To begin, let me thank you for your understanding and the many words of support both to me and to your dedicated team of account managers. We certainly understand the anxiety and frustration that have resulted from this incident, and we take it very seriously. I plan to provide you with regular updates on this incident to ensure you have the information you need to address its consequences within your organization as well as with your constituents.

We are still investigating the details of the intrusion, but we can share that the attack was perpetrated by an outside party commandeering the account of a Convio staff member. Working as an authorized administrator, the intruder was then able to access client data. We are working with the FBI and have hired forensics experts to help us undertake a complete evaluation of how the intruder was able to compromise the staffer's account. We will share as much information as possible in the coming weeks.

We are implementing additional measures to strengthen our security. Below are some of the steps we've already taken:

- Reset all system level account passwords and will reset passwords for all client administrative accounts (see detailed information below signature),
- Restricted administrative access to our systems to corporate IP addresses,
- Scanned all systems for any remnants of the intrusion,
- Revised security procedures across the company, and
- Accelerated planned investments in additional technical and human security systems that will help reduce the risk of future breaches.

Below the password reset information at the bottom of this email, you will find a sample paragraph that we recommend you place into your normal communications. The information directs constituents to a Web site with consumer-friendly tips that help with this incident, but also provide more information to your constituents in helping protect their online privacy. That site is www.convio.com/onlinesecurity.

Beginning tomorrow at 12:00 p.m. (noon) Central, we will be staffing a toll-free number that you can provide to your constituents who might have questions. Please understand that the staff on the phone lines will be providing online tips to help make people more secure, not answering questions specific to your organization and technical detail. That number is **1-800-501-8193**.

Our entire team is committed to your continued success — from the account managers and technical support team, to the executive team. We look forward to working with you through this challenge.

11/9/2007

We will continue to provide you updates through your account management team and via appropriate email communications.

Regards,



Gene Austin
CEO, Convio, Inc.

Password reset notification

As a result of the recent security incident on the GetActive platform, we are taking the purely precautionary step of resetting all client administrative passwords. Beginning Wednesday morning, the next time you sign on to access your GetActive dashboard, your old password will not work and you will see a link to reset your password. After clicking that button, you will receive a system-generated email with a personalized link to re-establish a new password. You can then sign on and resume your work. Note: If you already requested that we reset your passwords after the security incident, you will not be asked to change them again.

We realize this is an inconvenience, but we hope you agree that adding this extra step to your next sign-on provides an extra level of comfort in knowing all those who access your data are authorized to do so. We also recommend you regularly review who has access to your GetActive service by going to CONFIGURE from your dashboard and choosing ADMINISTRATORS. If you are an administrative manager, you can add, change, or delete administrators at any time. Otherwise contact Client Support from the HELP section of your dashboard to submit changes to administrative access.

We are committed to keeping the GetActive platform secure. We have taken substantial measures since last week's security incident and we continue to be vigilant. We appreciate your cooperation as we continue to implement measures to enhance the security of your data and the GetActive platform.

Sample communication to constituents/members:

As we continue our push into the digital age, we are seeing a not too surprising rise in phishing and other online scams as criminals migrate their schemes to the Internet. In light of the recent security intrusion against the company we contract with to provide online services, we are encouraging all our members to be more diligent about online security. For a list of tips and suggestions to ensure the safest possible online experience, please visit www.convio.com/onlinesecurity.

Copyright 2007, Convio Inc. All rights reserved.

We respect your time and privacy. To unsubscribe from our mailing list, please [click here](#). Review our [Privacy Policy](#).

Convio is headquartered at 11400 Burnet Rd, Bldg 5, Ste 200, Austin, Texas 78758. Visit us on the Web at <http://www.convio.com>.

11/9/2007

THIS WAS SENT, BY BOTH E-MAIL AND LETTER, TO THE 9,843 PEOPLE IN NS WHO LOST ONLY AN E-MAIL ADDRESS.

Dear MOAA E-Mail Subscriber,

This is a special notice to advise you that MOAA's e-mail contractor, Convio, has informed us that someone illegally gained access to Convio's files and downloaded e-mail addresses from 92 of Convio's clients, one of which was MOAA.

At the outset, let me stress that no information was stolen that we reasonably believe could be used by the data thief to compromise your identity – that is, no Social Security numbers, account numbers, or other financial information. No names were stolen, except to the extent an e-mail address included a person's name.

However, the data thief did obtain thousands of e-mail addresses of MOAA members and some non-members who have used our services or subscribed to our e-mail products – including your e-mail address.

MOAA takes any such illegal activity very seriously – especially if it involves any of our members' data. We want to stress, however, that we believe that any risk to you arising from this data breach is limited. Today's reality is that dedicated "data-mining" individuals and organizations routinely obtain e-mail addresses within minutes from anyone who hooks up a computer and starts an e-mail account. Nevertheless, you should remain vigilant in protecting your identity by reviewing all of your financial account statements regularly and monitoring free credit reports available from national consumer-reporting agencies.

We believe there is a possibility that you may receive some additional "spam" (junk mail) or be targeted with "phishing" e-mails. In "phishing" or similar scams, you may receive an e-mail that appears to be from a well-known or trusted organization, urging you to go to a website and enter personal information. It is likely that you have received such "phishing" e-mails in the past. If you receive such e-mails, you should promptly delete them and you should not respond to them in any way. Reputable firms do not ask for personal information in this manner.

We wanted you to know right away of this unauthorized access, and to know also that we find the theft situation totally unacceptable. We have confirmed that Convio has severely tightened its security, and MOAA is reviewing security precautions on all of our data systems, both internally and with our other contractors who may have access to member data in one form or another.

We take very seriously our responsibility to safeguard your personal data, and we pledge that we will continue to take every possible measure to fulfill that responsibility.

I have attached a series of questions and answers about this incident for your review. Should you have any additional questions, please don't hesitate to contact MOAA's Member Service Center toll-free at 1-800-234-6622, or by e-mail at msc@moaa.org.

Sincerely,

Norb Ryan, Jr.

Vice Admiral, US Navy, Retired
President and CEO

Questions and Answers

1. **How many e-mails have been stolen?** MOAA was one of 92 organizations affected by the e-mail contractor's data loss. The theft included e-mail addresses of 260,000 MOAA members, subscribers, and prospects.
2. **What other data has been stolen?** No other personal financial data (SSNs, birthdates, account numbers, etc.) was affected. Website passwords were stolen with regard to a very few individuals, but you did not have a password stolen – only an e-mail address.
3. **How can you be sure what has been taken?** The contractor electronically tracked the data that was downloaded.
4. **How could I be affected personally by this e-mail address theft? What should I do now?** You may receive additional "spam" (junk mail) messages, or you may receive so-called "phishing" messages with official-looking company logos that ask you to log into a website and provide your personal information to "verify" one thing or another. You should immediately delete all such messages and you should not respond.
5. **Should I change my e-mail address?** That is your decision, but it is probably not necessary. As you may know from experience, dedicated "spammers" and "phishers" have ways of obtaining your e-mail address electronically.
6. **Should I enroll in an identity-theft program? Will MOAA or Convio pay for it?** It is your decision, but we don't believe that's necessary. Your e-mail address alone will not allow anyone to steal your identity. MOAA will not pay for you to enroll in an identity-theft program under these circumstances.
7. **How did this breach happen?** A credential belonging to one of the contractor's employees was stolen, which allowed the thief to log onto the contractor's system and access e-mail addresses owned by members of MOAA and members of dozens of other organizations.
8. **What is MOAA doing to prevent a recurrence?** First, Convio contacted the FBI to alert it about the theft. Second, we at MOAA are working with Convio to ensure it reviews and upgrades its data-security protections. Finally, MOAA is initiating an internal review, and similar reviews with all of our other outside contractors, to assess and, where necessary, upgrade the protection accorded all of our members' personal data.
9. **Why does MOAA have to use an outside online service provider? Can't it be done in-house?** Unfortunately, the complexity of e-mail guidelines and anti-spam laws have made it very difficult for organizations like MOAA to keep track of all the rules, outdated e-mail addresses, and unique requirements of the hundreds of different Internet Service Providers like AOL, Yahoo, etc. We must hire contractors who specialize in managing all these requirements

to ensure we can properly deliver MOAA's weekly Legislative Update, News Exchange, and other e-mail communications to those who wish to subscribe to them.

10. Who can I contact if I have questions about this situation? If you have additional questions, please contact MOAA's Member Service Center by calling 1-800-234-6622 or e-mailing the Center at msc@moaa.org.

9. Who can I contact if I have questions about this situation? If you have additional questions, you can contact MOAA's Member Service Center by calling 1-800-234-6622 or e-mailing the Center at msc@moaa.org.

10. Why does MOAA have to use an outside online service provider? Can't this work be done in-house? Unfortunately, the complexity of e-mail guidelines and anti-spam laws have made it very difficult for organizations like MOAA to keep track of all the rules, outdated e-mail addresses, and unique requirements of the hundreds of different Internet Service Providers like AOL, Yahoo, etc. We must hire contractors who specialize in managing all these requirements to ensure we can properly deliver MOAA's weekly Legislative Update, News Exchange, and other e-mail communications to those who wish to subscribe to them.