PoliceOne.com News

Police Products > Police Press Releases

To P1 Forums Users: An Update on PoliceOne Forums Data Breach

Feb 7, 2017

Notice of Data Breach

Dear PoliceOne Member,

***What Happened*.** On Friday, February 3, 2017, we were notified that the content of our PoliceOne Forum was the subject of unauthorized access and acquisition. The incident occurred in our forums, which are run on third party software and are entirely separate from our main PoliceOne member database and other systems, which have not been compromised. We have become aware of a security incident in our PoliceOne Forums that allegedly occurred in 2015. We are aggressively addressing the matter and want to make you clear on the scope of the issue and its potential impact to you. Security is

incredibly important to us and we've worked hard to protect your information over the past 17 years.

What Information Was Involved. The information accessed was limited, and included email addresses, user names and hashed and salted passwords (a protected version of the password you use). It did not include forums posts or other content.

What You Can Do. As a user of the PoliceOne forums, your account may have been among those included in the incident, and we want to make sure you have all of the information regarding what happened, what we are doing to address it, and what you'll be asked to do as a result. Here's what you need to know:

> As soon as we became aware of the potential incident, we took down the forums and set any new member login to require a password reset via email for potentially affected accounts
>
> On your next PoliceOne login, you will automatically receive an email with a link to change your password. **We strongly recommend you go to our login page and initiate a password change immediately.**
>
> If you use your same PoliceOne password and email combination for any other sites, we **highly recommend** changing your password on those sites
>
> In general, it is a best practice to change any online password every 6 months to 1 year due to the increase in hacking activity

What We are Doing. We are currently in the process of completing a full security review and confirm updates to prevent future incidents. We are confident this was an isolated incident specific to our forums that has since been resolved. This notice was not delayed as a result of a law enforcement investigation.

For More Information. Thank you for your attention and we apologize for any inconvenience. For more information on this matter, please read our notice. If you have any questions about this matter not addressed by this email, please contact our Customer Service department at **1-888-765-4231**.

Sincerely,

— *PoliceOne Team*

Exhibit C

Notice of Data Breach

Dear PoliceOne Member,

We have become aware of a security incident in our PoliceOne Forums that we were told occurred in 2015. While our investigation is ongoing, we are addressing the matter and want to make you clear on the issue and its potential impact to you. Security is incredibly important to us and we've worked hard to protect your information over the past 17 years.

***What Happened*.** On Friday, February 3, 2017, we were notified that the content of our PoliceOne Forum was the subject of unauthorized access and acquisition.

What Information Was Involved. The information accessed included email addresses, user names, MD-5 hashed passwords, and potentially your date of birth. While the passwords were also salted (a type of protection), the salt was also compromised.

What You Can Do. You are receiving this email because your account may have been among those included in the incident, and we want to make sure you have information regarding what happened, what we are doing to address it, and what you'll be asked to do as a result. Here's what you need to know:

- As soon as we became aware of the potential incident, we took down the forums and set any new member login to require a password reset via email for potentially affected accounts
- On your next PoliceOne login, you will automatically receive an email with a link to change your password. **We strongly recommend you go to our login page and initiate a password change immediately.**
- If you use your same PoliceOne user name or email address and password for any other sites, we **highly recommend** changing your password on those sites
- In general, it is a best practice to change any online password every 30 to 60 days due to the increase in hacking activity.

What We are Doing. While our investigation is ongoing, we are currently in the process of completing a security review. This notice was not delayed as a result of a law enforcement investigation.

For More Information. Thank you for your attention and we apologize for any inconvenience. If you have any questions about this matter not addressed by this email, please contact our Customer Service department at **1-888-765-4231**.

Sincerely,

— *PoliceOne Team*

PRIVACY SAFEGUARDS

You may take action directly to protect against possible identity theft or financial loss. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files.

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;

6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft; and
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit file report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-685-1111 (NY residents please call 1-800-349-9960) http://www.freeze.equifax.com	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion PO Box 2000 Chester, PA 19022-2000 1-888-909-8872 www.transunion.com/securityfreeze

You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/idtheft, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. **For Rhode Island residents**, the Attorney General's office can be contacted at http://www.riag.ri.gov/index.php, consumers@riag.ri.gov or (401) 274-4400. Approximately 715,000 accounts were affected, including an unknown number of Rhode Island residents.

Exhibit D

PoliceOne Provides Notice of Data Security Incident Related to PoliceOne Forums

San Francisco, California, March 21, 2017 – PoliceOne announced that a recent data security incident has compromised the security of PoliceOne Forums users' email addresses, user names, a small number of dates of birth and MD-5 hashed and salted passwords. Although there is no indication of actual or attempted misuse of this information nor was PoliceOne's central database compromised, PoliceOne is notifying users whose information may have been subject to unauthorized access and acquisition and providing these users with information and resources that can be used to better protect against the possibility of identity theft or fraud if they feel it is appropriate to do so.

"We take this incident and user privacy very seriously as we have over the past 17 years," Alex Ford, CEO of PoliceOne stated. "We have fully reviewed our forums, confirming the vulnerability had already been addressed, and continue to review our processes, policies, and procedures that address data security to prevent any future incidents."

What Happened: On Friday, February 3, 2017, we were notified that the content of our PoliceOne Forum was the subject of unauthorized access and acquisition. The access and acquisition allegedly occurred in 2014, but was just brought to our attention.

What Information Was Involved: The information accessed included email addresses, a small number of dates of birth, user names, and MD-5 hashed passwords. The passwords were also salted, which adds another layer of security; however, the salt was also accessed.

What PoliceOne Users Can Do: We want to make sure you have information regarding what happened, what we are doing to address it, and what you'll be asked to do as a result. Here's what you need to know:

- As soon as we became aware of the potential incident, we took down the forums and set any new member login to require a password reset via email for potentially affected accounts
- On your next PoliceOne login, you will automatically receive an email with a link to change your password. **We strongly recommend you go to our login page and initiate a password change immediately.**
- If you use your same PoliceOne user name or email address and password for any other sites, we **highly recommend** changing your password on those sites.
- In general, it is a best practice to change any online password every 30 to 60 days due to the increase in hacking activity.

What We are Doing: While our investigation is ongoing, we are currently in the process of completing a security review.

For More Information: We apologize for any inconvenience. If you have any questions about this incident, please contact our Customer Service department at **1-888-765-4231**.

General Consumer Information Regarding Fraud

You may take action directly to protect against possible identity theft or financial loss. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, list or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files.

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;

4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft; and
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit file report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
(NY residents please call 1-800-349-9960)
http://www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
PO Box 2000
Chester, PA 19022-2000
1-888-909-8872
www.transunion.com/securityfreeze

You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/idtheft, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. **For Rhode Island residents**, the Attorney General's office can be contacted at http://www.riag.ri.gov/index.php, consumers@riag.ri.gov or (401) 274-4400. An unknown number of Rhode Island residents may be affected by this incident.