



Akliz, Inc.
464 Common Street, Suite 101
Belmont, MA 02478
617-475-3266
www.akliz.net

January 4, 2012

The Honorable Tom Miller
Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319

Dear Attorney General Miller,

Please be advised that we, AKLIZ, Inc. ("AKLIZ"), experienced a data breach on December 27, 2011 when our customer billing system was the victim of what appears to be international computer hackers. AKLIZ has notified affected customers by email and is in the process of sending physical letters.

It appears that an attacker was able to gain access to one of the internal servers that hosts AKLIZ's billing system. That system contains customer names, phone numbers, email addresses, usernames and passwords. If customers paid online with a credit card, their credit card information was stored on the system as well. Sensitive information, such as credit card information and account passwords, was stored in an encrypted form. However, the incident involved an attempt by the attacker to access the keys used to decrypt the data, so AKLIZ cannot be certain that the data remains encrypted.

As explained in the enclosed letter, AKLIZ has initiated a full security lockdown, and implemented a number of technical and procedural changes to enhance security across its entire network generally, and with its billing system specifically. AKLIZ has also begun revising its billing and login processes to prevent a recurring incident. The notification letter to customers includes additional information regarding how they can safeguard and monitor their personal information.

AKLIZ filed a report with law enforcement, and an investigation is underway. Should we become aware of any significant developments we will inform your office. Please let us know if you require any additional information regarding this matter.

Yours respectfully,

Lawrence Chan
Founder and CEO
Akliz, Inc.

Enclosure

CONSUMER PROTECTION DIV.

12 JAN 10 AM 1:45

RECEIVED



Akliz, Inc.
464 Common Street, Suite 101
Belmont, MA 02478
617-475-3266
www.akliz.net

Dear [[CUSTOMER NAME]],

We believe that one of our internal servers was compromised on December 27, 2011. We discovered this incident during a routine examination of our server logs, and have received no reports of any harm to our customers associated with this incident. However, we are continuing to investigate the matter, and wanted to inform you of the situation as soon as possible.

What Happened

It appears that an attacker was able to gain access to one of the internal servers that hosts our billing system. That system contains information you provided when you created an account with us, such as your name, phone number, email address, username and password. If you paid online with a credit card, your credit card information was stored on our system as well.

The billing system we use is a popular and sophisticated one. Sensitive information, such as credit card information and account passwords, was stored in an encrypted form. However, the incident involved an attempt by the attacker to access the keys used to decrypt the data, so we cannot be certain that the data remains encrypted.

What We've Done

Immediately after detecting the breach, we initiated a full security lockdown, and implemented a number of technical and procedural changes to enhance security across our entire network generally, and with our billing system specifically.

In addition to these internal steps, we will be revising our billing and login processes to prevent any similar incident from ever happening again. For example, we immediately redirected all credit card billing to an external billing provider. Customers can no longer enter credit card information on our system; they must use PayPal. All customers will also be asked to reset their usernames and passwords. Passwords stored on the system will be stored in an encrypted state.

In an effort to assist in the possible apprehension of the attacker, we filed a report with law enforcement. An investigation is underway and we will be cooperating with law enforcement officials.

What You Can Do

Akliz is committed to minimizing any inconvenience this situation could have for our customers. The attack appears to be an isolated incident that occurred for the first time yesterday. We discovered it the same day, and took steps immediately to prevent a recurrence. However, there are also steps you can take to minimize any impact this incident could have.

We encourage you to follow security best practices and continue to use unique and secure passwords that are updated regularly. The next time you log in to your account with us, you will be prompted to select a new password and you will receive an email from us at support@akliz.net, confirming that you have done so. If you receive such an email before you have changed your password, contact us by telephone immediately so we can confirm your identity and reset your account. Also, if you use your Akliz password on other accounts, you may wish to change your password on those accounts as well.

If you have a game server password, you will need to reset its control panel password as well. You can reset the game server password by logging onto www.akliz.net/manage, and going to "My Services." Once in "My Services," click on the green arrow next to the service, and enter a new password.

Customers who used a credit card with us may wish to contact your issuing bank and have a new card number assigned. In addition, examine your next credit card statement carefully for unauthorized charges, and inform the issuing bank immediately if you become aware of any suspicious activity. Report all suspected identity theft to local law enforcement.

You may also want to contact one of the three nationwide credit monitoring agencies as soon as possible in order to add a fraud alert to your credit report and to remove your name from lists of pre-approved credit applications for a period of time. You only need to alert one of the three agencies, as they will share your information with the others.

Equifax
P.O. Box 740241
Atlanta, GA 30374
800-685-1111
www.equifax.com

Experian
P.O. Box. 2002
Allen, TX 75013
888-397-3742
www.experian.com/consumer

TransUnion
P.O. Box 1000
Chester, PA 19022
800-888-4213
www.transunion.com

In addition, the Federal Trade Commission ("FTC") offers consumer assistance services. The FTC can be reached at www.ftc.gov, or by calling 877-438-4338.

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

You are entitled to a free copy of your credit report at www.annualcreditreport.com.

Our Apology and Our Commitment

We apologize about any inconvenience that this event might have caused. We are committed to providing our customers with the best possible hosting experience, and part of that is ensuring that our customers' data is as safe and secure as possible.

If you have any questions or concerns, please do not hesitate to contact us.

Sincerely,

Lawrence Chan
Founder and CEO
Akliz, Inc.
privacy@akliz.net