STATEMENT OF SECURITY

EVERYTHINGCU.COM DATA SECURITY

The safety and security of your member data is our paramount concern. To that end, we have developed a number of security features into our products. In addition to the three layers of data encryption security outlined on the following page, here are our other security pledges to you:

Member data policy

EverythingCU does not use your sensitive member data for any purpose other than to display it to your own designated CU staff within the product itself. We do not transfer the member information to any other alternate storage medium besides the encrypted database as outlined on the next page. This applies to all of our products including LoanStreamer, Loan Switch, KickStart, Credit Check Plus, eSwitchKit, and Premium Online Switch Kit.

Member data purged after set time period

In addition, some of our services utilize an expiration date system, whereby after a pre-determined time, which is set by the credit union within a minimum and maximum range, the member's account and information is automatically deleted after the number of days has been reached. This feature erases the information permanently. This is a further safeguard of your members' data.

Timely notification

EverythingCU's servers reside in an extremely secure co-location facility. This facility has both physical security as well as data security. In the extremely unlikely event that there is a data breach, EverythingCU will notify all affected clients immediately.

DATA ENCRYPTION LEVELS ON NEXT PAGE...

STATEMENT OF SECURITY

From a technical standpoint, here are our **three levels of data encryption security:**

1.) 128-bit Secure Socket Layer(SSL)/Hypertext Transfer Protocol Secure (HTTPS):

All EverythingCU.com products are created in such a way that data can only be transmitted over the 128-bit Secure Socket Layer (128-bit SSL). This system is the one that creates the familiar "Lock" symbol in your browser. Any attempt to access an EverythingCU product that is not via 128-bit SSL is automatically rejected.

More information can be found at: http://en.wikipedia.org/wiki/HTTPS

2.) Access security of the EverythingCU database:

In addition to the 128-bit SSL transmission security, all calls to the EverythingCU.com database are secure using the ColdFusion database security procedures. This insures that only the EverythingCU program can insert and retrieve data.

For more information on this system visit: https://learn.adobe.com/wiki/display/coldfusionen/Data+Source+Management+for+ColdFusion#DataSourceManagementforColdFusion-AddingdatasourcesintheAdministrator

3.) Advanced Encryption Standard (AES) of all sensitive data within the database:

In addition to the 128-bit SSL transmission security and database access security described above, all sensitive member data is encrypted using AES, the Advanced Encryption Standard as specified by the National Institute of Standards and Technology (NIST) FIPS-197 [view 42-page PDF on this standard]. This third layer of security is yet an additional safeguard since only the EverythingCU server can initiate decryption of the database items using the AES encryption/decryption key, and this only happens when the authorized Credit Union personnel view the data in their administrative control panel.

More about this database encryption/decryption process can be found here: http://livedocs.adobe.com/coldfusion/8/htmldocs/help.html?content=functions_e-g_01.html

In addition to the above, the co-location facility in which the EverythingCU.com servers reside is maintained to the highest security standards as well, including SSAE-16 certification.

FOR FURTHER INFORMATION

More information about EverythingCU.com security, please contact Morriss M. Partee, Chief Experience Officer at morriss@everythingcu.com or 413-535-0621.