Enhanced Liberty Security Update

E*TRADE ADVISOR SERVICES

On July 26, 2019, we are making a change to enhance our application security. To help mitigate credential stuffing attacks we have implemented a web application firewall (WAF).

What are we changing?
We are implementing a WAF to help prevent traffic from known bad actors. This WAF will sit in front of any web pages that handle logon for our Liberty web application. The WAF determines that the customer's log-on attempt is legitimate using a large list of criteria, such as the IP address, log-on ID, location, and MAC address of your laptop, just to name a few. This collection of information forms a fingerprint that uniquely identifies the user. Any fingerprints from known bad actors or odd behavior that hits our log-on pages will be redirected to a log-on error page.

How will this affect you?
1) Liberty will be more secure after this update.
2) There is a possibility that false positives will be experienced—in other words, legitimate users that the WAF may mistake as bad traffic. These users will be sent to the log-on error page and will need to be white-listed by the WAF.

How do we white-list users?
The workflow for white-listing a user will be as follows.
1) The end user will encounter the log-on error page (a sample is attached). This error page contains an error number (the user's IP address) and a message for the user to contact their registered investment advisor (RIA).
    a. This log-on attempt does not imply a failed log-on attempt, as the log-on request will never hit our system: The WAF has provided a buffer.
    b. However, the end user will likely assume that it is a failed log-on attempt.
2) The RIA will verify the user's identity just as they would as if the user forgot their password.
3) The RIA will contact their relationship manager (RM) and provide the error number/IP address.
4) The RM will contact our WAF provider via email (soc@shapesecurity.com) and request a white-list exception for the specific user. The RM will provide the user's log-on ID and error number (IP address) to Shape (the WAF provider).
5) The resolution time is roughly 10 minutes after a white-list exception is submitted.
6) After the user is white-listed, they should be able to log on without issue.

How many people will experience a false positive log-on attempt?
We anticipate the number will be very small, perhaps as little as one to two per month—but that's just a guess. Modern WAFs are very good at identifying bad vs. good Log-on attempts.

Please contact your relationship manager to discuss any questions you have.