In an effort to keep you safe and informed, Lincoln Savings Bank offers updates and reminders regarding the ACH network and best-practices. The information included herein is intended as informative only. Please consider your own internal guidance, policies, or procedures, as well as legal advice that your business has received as well.

Are You Using all Your Tools?

Jon Parker, AAP
1st VP, Business Banking and Services Manager

It turns out that "Bad Actors" are out there just looking for ways to access business, consumer, and financial accounts and information. This is simply the reality of the world we live in. The problem is that there desire to access information and the counter-measures that are generally put in place to prevent undesirable access run opposite to how humans prefer to interact.

That is to say that the best line of defense is a robust, multi-layered and complex entry and verification flow. However, we (myself included) really like things to be easy. We want to just be logged into our favorite streaming services without having to do anything. We've grown accustomed to the ease of online shopping and "1-click" purchases. Because we are surrounded with a focus on ease, we occasionally find frustration when a process deviates from that expected norm, even though our logic tells us that there is a reason to deviate.

This is one of our perpetual struggles at Lincoln Savings Bank as we strive to deliver a first in class customer experience through all of our channels and services. The customer experience is of great importance, but we cannot sacrifice your security in that desire. As a bank, we are directed by very specific and encompassing regulation and guidance that tells us the very minimum we need to achieve in areas, such as online banking security. In addition, we take additional guidance from industry peers, security experts, and good old fashioned common sense to strike the balance with ease and security.

As a business who utilizes some of our advanced "Treasury Management" services, you have access to a greater wealth of capabilities at scale than most any single consumer user. With that in mind, we absolutely treat you a little bit differently, but please note, it's only because we live by the belief that your financial security, and that of all of our customers, is of the greatest importance.

Businesses with access to higher risk services like ACH and Wire origination fall into a specific security role within our environment as a baseline with additional measures added from there. For example, we require every user with access to these (or like) systems to enter a "Temporary Access Code" at every login. This code is a single-use number that is issued by request and valid for a short period of time to a device other than e-mail. This helps ensure that even if a Bad Actor were able to infect your machine with a key-logger, and have access to your user-name and password, there would be an additional out of band authentication measure that they would not have access to.

Next, we utilize data driven end-point analytics to flag suspected logins from unknown or new machine types. Then, our system analyzes transactions that are initiated to send funds out from your account to determine if it meets a level of expectation based on prior performance. If it does not rise to the level of confidence, then you will be receiving a call from on of our friendly staff to verify with you directly that a transaction is valid. Don't be alarmed, or frustrated by this process, it's simply one of our attempts to live up to our belief that your financial security is priority one.

In addition to these standard measures, we have a myriad of tools and solutions to assist in creating a place of financial safety. Some of these options are already in place, but I would encourage you to reach out to us to learn more if any of these are of interest to you, or if you question how your security environment is presently constructed.

- Dual Approval of Transactions
- Temporary Access Code Required for Approval
- Tiered Approval Requirements based on Transaction Size or Type
- Segregation of Duties and Rights
- User Level Enforcement of Rights, Entitlements, and Limits
- IP address Restrictions
- Day/Hour Restrictions
- Location Restrictions
- System Alerts (text and email)
- Positive Pay
- ACH Block
- Account Reconciliation Assistance

LSBpro Support can be reached at:
Email - lsbprosupport@mylsb.com
Phone - 515-777-7940