



Top things our business customers can do to reduce the risk of online identity theft

- Initiate ACH and wire transfer payments under dual control. For example: One person authorizes the creation of the payment file; a second person authorizes the approval of the file.
- Restrict transfer capabilities by User or transfer type. For example, a transfer that should never exceed a certain dollar amount should be locked down to prevent it from exceeding that amount or restricting an ACH/Wire template so funds can only be sent to a specific recipient.
- Most Current Anti-Virus. Ensure that all anti-virus and security software and mechanisms for all computer workstations and laptops that are used for online banking and payments are up-to-date.
- Restrict functions for computer workstations and laptops that are used for online banking and payments. For example, a workstation used for online banking should not be used for general Web browsing and social networking; A better solution is to conduct online banking and payments activity from a dedicated computer that is not used for other online activity, and/or is not connected to an internal network.
- Monitor transactions and reconcile accounts daily. Many small business clients do not reconcile their bank accounts on a regular basis, and therefore may not recognize fraudulent activity until it is too late to take action.
- Use very different passwords for each system you access. In the event that one of your passwords is compromised, the sites you access will be limited to the ones you use for that specific password.
- Utilize strong passwords that contain a combination of letters, numbers and symbols. Avoid common words, your name, family names, pets names, etc.
- Change your passwords often. When choosing a new password, use a completely different naming convention and different letters/numbers/word. Repetitive uses of the same passwords are easily guessed by the thieves.
- [Click here for additional tips.](#)

Some of the steps that North Valley Bank takes to protect their business customers:

- Deploy multi-factor authentication for business accounts that are permitted to initiate funds transfers.
- Restrict user access to only those functions and time periods that are appropriate to the customer's business process and review periodically for accuracy.
- Authorized Administrator which allows access to accounts at the direction of the business customer's authorized administrator(s) only.
- Dual control provides the option for our business customers to initiate payments under dual control, with distinct responsibility for transaction origination and authorization.
- User Control provides the option for our business customers to designate transfer limits by User or template
- Limits to establish and monitor exposure limits that are related to customers' activities.
- Tools which provide products to further automate the monitoring process such as Positive Pay which helps prevent your internal checks from fraudulent activity and e-Alerts which assist in early detection of possible fraudulent activity.

Of course, we encourage you to call us should you become a victim of malicious activity so that we can answer any questions you have regarding your online banking accounts. The Customer Resource Center is available Monday through Friday 7:00 am to 7:00 pm, or Saturday from 9:00 am to 2:00 pm at 866.869.MORE (6673).

Get More.



Call 1-866-869-MORE (6673)  go online at www.novb.com ■ Member FDIC