# Welcome to Centennial Bank!

The former Stonegate Bank and Centennial Bank have merged and will complete a system conversion in early 2018. Centennial's Cash Management team is dedicated to continuing the same great service provided to you from Stonegate Bank. Centennial, as did Stonegate, has a history of strong financial performance and has a desire to exceed your expectations.

Outlined below are some of the changes that will occur with the Cash Management online banking system conversion. **Items in bold represent actions that you will need to take or major changes we want to make sure you know about.** Our experienced Cash Management and Treasury professionals offer direct customer service as an additional point of contact to your local bank associates who will continue to be available to serve you. We look forward to getting to know you!

## CASH MANAGEMENT ONLINE BANKING SYSTEM

- Centennial Bank plans to implement your Cash Management online banking system and will be available to train your staff on the new system after the operational conversion on February 12, 2018. Our goal is to impact your day-to-day functions as little as possible. Please contact 844-213-5198 to schedule training.
- Beginning February 12, 2018, you may access the Cash Management login screen by visiting the website https://online.my100bank.com/CM/bankonline or following the steps below:
    - Navigate to www.my100bank.com
    - Hover over Business Banking and click on Cash Management
    - Click on Cash Management Login
    - **Your Username will remain the same as it is today,** ***unless we communicate with you otherwise*****.**
    - **Your Company ID and password will be communicated to you in a separate mailing.**
- **For personalized assistance with Online Banking or other Cash Management questions, please call 844-213-5198**.
- **An authorized signer on your account(s) will receive an agreement package containing tokens for each of your users. Tokens are required for companies originating ACH or Wire transactions. Should you not receive your tokens prior to February 5 please contact 844-213-5198.**
- **Training will be offered in person or via direct phone support. We would like to schedule the setup and training of the Cash Management online banking system as soon as possible. Additional information will be provided when we supply you with your security tokens.**
- **Superuser (Administrators) and User guides are available on our website https://www.my100bank.com/business-banking/cash-management or by request.**
- **You will no longer be able to access Stonegate's online banking system after February 9 at 4:00 pm EST.**

- **The Cash Management system only allows for one Superuser/Administrator per setup. The Superuser/Administrator is responsible for creating users and editing user authorities.**
- **Upon login, our system will require you to setup four security questions. You must select and answer all four questions with different answers; answers are case sensitive and must be at least 3 characters long.**
- **An account cannot be added to multiple Cash Management profiles.**
- **In order to receive electronic notifications or alerts, each user must complete the email verification through the Cash Management system.**
- **Activity Alerts can only be setup to be received via email. The Cash Management system does not send text notifications or alerts.**
- The Cash Management system currently does not have a mobile banking app. Mobile Banking is for consumer logins only at this time. If you wish to use Mobile Banking on your business accounts, please contact your banking office after February 9 to set up a separate Internet Banking login.
- At this time, Centennial does not offer Mobile Remote Deposit Capture in Cash Management, but there are other Remote Deposit Capture services available. To inquire, please contact Cash Management at **CEN-CMOperations@my100bank.com** or 844-213-5198.
- Password Assistance: Your Superuser/Administrator can reset your access or password. Our Cash Management group can assist with questions if needed.
- Scheduled recurring and future dated account-to-account transfers will continue to be available.
- **Due to the data conversion, the last bank statements will be produced as of Friday February 9, 2018 on the Stonegate Bank system. All existing eStatement recipients will receive paper statements via US mail. Please print or save any Stonegate Bank statements that you may need to reference as they will not be available through Centennial's Cash Management system**. All users who wish to continue receiving eStatements will need to enroll for this service in the Cash Management system under Profile > Edit Profile on or after February 12. eStatements are available for 18 months from the date of enrollment and are stored as PDF documents within our Cash Management system under the Documents tab. Please note that enrolling in eStatements will stop the paper statements from being mailed. Once you verify your email address you may use the email notices as verification that your statements are available for viewing. If you have multiple accounts, an email notice will be generated for each account. Analysis statements will not be available as an eStatement and will no longer be mailed monthly.
- **Intuit® Web Connect and Direct Connect will be available after the Centennial system conversion.** A separate communication will be sent to provide instructions on how and when to convert from Stonegate Bank Web Connect and Direct Connect services to Centennial Bank Web Connect and Direct Connect services. In the Cash Management system you can download a QuickBooks®/Quicken®* file format and upload it to QuickBooks®/Quicken®. **It is critical that your transactions are downloaded from Stonegate's system prior to the conversion as a limited amount of history may be available after conversion.**

* QuickBooks® and Quicken® are registered trademarks of Intuit®, Inc.

## ACH ORIGINATION

- **The last day you will be able to originate an ACH batch using the Stonegate service is Thursday, February 8 at 4:00 pm EST. <u>It is important that all ACH batches with effective dates up to February 9 are initiated within the Stonegate system prior to Thursday February 8th at</u>**

**4:00 pm EST.** **Any files with effective dates after February 9 will be cancelled and must be originated using Centennial Bank's ACH service.**

- **Starting Monday, February 12, ACH users will have access to recent ACH file templates. This information converts electronically so we encourage you to print or save your final ACH file details, templates or any historical data prior to Friday, February 9 at 4:00pm EST, as you may need to reference this information at a later date. We will assist customers to import or re-create files, as needed.**
- Recurring ACH origination is available using Centennial Bank's Cash Management system; however it is activated upon request.
- **Customers who import NACHA™ formatted files from another software system will need to update batch header records with Centennial Bank's information and routing number: 082902757. If the funding account offset entry is embedded in files, please also update the routing number to reflect Centennial Bank's routing number: 082902757.**
- **ACH files must be initiated before 5:30 pm EST on any business day. ACH files initiated after this time will be processed the following business day.**
- ACH originators will have the opportunity to schedule ACH files up to 14 business days prior to the effective date.
- ACH originators in Centennial's system require a token to verify ACH batches before they are processed.
- **A hold will be placed on funds in the accounts originating ACH credit files, on the date of initiation. The offsetting debit entry will hard post on the effective date.**
- **Tax payments will no longer be available as an ACH option. Please visit www.eftps.gov for alternative payment options.**

## WIRE TRANSFERS

- **Domestic and International wire templates currently in use in Stonegate's system are expected to be available to Cash Management system users February 12. This information converts electronically. We encourage you to print and save your templates, beneficiary information or any historical information prior to Friday February 9 at 4:00 pm EST; since you may need to reference this information at a later date.**
- Wire notifications are available in various formats for incoming or outgoing wire transfers.
- **The daily deadline for verified wire originations in the Cash Management system is 5:00 pm EST for same day processing.**
- **Wire originators in Centennial's system require a token to verify wires before they will be processed.**

## BILL PAY

All valid pre-scheduled and recurring payments set through the Stonegate Bill Pay system will be paid. If a payee is a Person-to-Person or a Routing/Account Number combination, those payees and corresponding payments will not convert and will need to be re-established on or after February 12.

You will no longer be able to change payments or create any new payments through the Stonegate Bill Pay system after 5 pm EST on Thursday, February 8. In addition, as of 5 pm EST on Thursday, February 8, the Stonegate Bill Pay system will no longer be accessible.

Beginning Monday, February 12, Centennial Bank Bill Pay will be fully available by logging into www.my100bank.com. Business sub-users will need to be reestablished by the business admin on/after Monday, February 12.

**There are five main changes to the way Bill Pay payments will process beginning February 12, 2018:**

- **Your scheduled Bill Payments will be sent without verifying that your account has the funds. To prevent accidentally overdrawing your account, please manage your balance considering your outstanding bill payments;**
- **When Bill Pay processes a payment electronically, the payment will be debited from your account on the delivery date, as opposed to the business day before the delivery date.**
- **When Bill Pay processes a payment with a check, the payment will not be debited from your account until the date the check clears.**
- **Bill payment cutoff time is at 4:00 pm EST. Any payments entered after the cutoff will not process until the following business day.**
- **All payments $5,000 or more will be sent via check.**

## POSITIVE PAY AND ACH BLOCK

**Positive Pay** is designed to provide enhanced security over a commercial customer's check disbursement process. The customer provides an issue file listing check number, date, and amount of each check the company has issued. As checks clear they are matched against the issue file and any checks that attempt to clear without a matching issue are presented to the customer to pay or return.

- **Exceptions must be reviewed and/or marked daily by 11 am EST.**
- **You may pay or return items online using the Cash Management system.**

**ACH Block-** protects commercial accounts from fraudulent electronic ACH debits and/or credits.

- **Existing allowable ACH debits will continue to be honored.**
- **The system will work the same as it does now.**

## ADDITIONAL SERVICES AVAILABLE

Centennial Bank's Treasury Department offers many additional tools to help automate your collections, protect your accounts, and provide valuable information to help you achieve your business goals.

- Zero Balance Accounts – automatically transfers funds from a sub account to a master account or from a master account to a sub account.
- ACH origination is available through the Cash Management system for direct deposit of payroll, preauthorized debits or credits, and cash concentration. Bank approval and underwriting is necessary and may require additional documentation.
- Wire Origination is available through the Cash Management system. Bank approval and underwriting is necessary and may require additional documentation.
- Remote Deposit Capture is available through internet access and requires a scanner. Bank approval and underwriting is necessary and may require additional documentation.
- Lockbox – outsourcing your accounts receivable can save time and money, and can provide a file upload that automatically posts payments to your accounting system.

## COMMITTED SERVICE

- Centennial Bank is dedicated to servicing all of your Cash Management banking, Remote Deposit, and technical Cash Management needs. We are available Monday through Friday, 8:00 am–5:00 pm EST.
- For personalized assistance with Online Banking, Remote Deposit technical support and other cash management questions, please call **844-213-5198**.
- Department email address: **CEN-CMOperations@my100bank.com**. Please feel free to email questions and requests pertaining to Remote Deposit and Cash Management services. Emails are monitored throughout the day and we will respond in a timely manner.
- We appreciate your patience the first few weeks after conversion as business volume will be higher than normal and responses may be delayed.
- We look forward to getting to know you!

# Security Matters!

Centennial Bank is committed to protecting your financial information. It is equally important that you safeguard your information and your computer system. Criminals will always gravitate toward the easiest way to make money. The more barriers that you can put in place, the more likely the criminal will go elsewhere. We strongly recommend that you read and use the following recommendations to stay as safe as possible online.

- **Use and Maintain a Reputable Antimalware Software Program**: Some programs may be better than others in regard to a particular feature, but any one of them is better than no antimalware protection at all. Do not use any antimalware software that advertises itself via unsolicited email or pop-up windows. Configure the software to update its malware definitions daily. It's also important to use antimalware software on mobile devices, such as your tablet or phone.
- **Use a Software Firewall**: If your operating system provides a firewall, enable it. Effective computer security depends on layers of security such as firewalls and antimalware software.
- **Turn on Automatic Software Updates**: This is a feature of some software which allows it to patch itself with very little effort from you. Make sure it's turned on for your operating system, security software, and any applications that have the option.
- **Be Aware of Your Internet Surroundings**: Stay out of "bad" internet neighborhoods. Simply going to a website can download malicious software. If you are not expecting an email from someone, be suspicious if it contains a link or attachment, as they can download malware. Malware can range from something that pops up ads, to a keystroke logger that records the keystrokes as you type your online banking User ID and password. Sharing files on thumb drives can also spread computer malware.
- **Downloading Mobile Applications:** Only download mobile apps from reputable places, such as the Apple® App Store® or Google Play™ store. Malicious software or software that invades privacy is sometimes hidden in free apps.
- **Ensure a Secure Connection When Using a Wireless Network**: Accessing sensitive information over a non-secure network simply leaves the door open for criminals. Even if you aren't visiting a site where you enter an ID and Password, you are still leaving your computer exposed to possible threats.
- **Log Out Properly**: Always click on "Log Out" at the top of the screen to ensure that no one with access to your computer can see your information or gain access to your accounts.
- **Programs Running Slowly or Crashing**: Many types of malware like to piggy-back on other applications, like web browsers, to monitor what they are doing. This can use a lot of your computer's resources, causing it to slow down considerably or crash other applications.
- **Suspicious Network Traffic and Slow Internet Connection:** In your Task Manager window (in Windows™), if your internet network connection shows more than a few percent usage then this could be evidence of something using your internet connection without your knowledge.
- **Security Warnings:** Security software cannot detect all malware, but when it does, the warning is a good indication of an infection, especially if you're not currently browsing the web or copying files. Ensure the security warning you are getting is coming from security software you know about on your computer. Some malware presents itself as a security warning.
- **Internet Browser Redirects:** Infected computers will sometimes be redirected to malicious websites.

**What should you do if your computer or mobile device is infected?** First, stop banking, shopping, or other online activities that involve sensitive information. Confirm that your antimalware software is enabled and up-to-date. Scan your computer for malware. Allow the antimalware software to do its job, cleaning up and deleting malware. Some malware is very sophisticated and can be difficult to remove even with the tools mentioned here. If you suspect that your computer is still infected, you should consider resetting your computer back to its original state. If you don't know how to do that, you should contact a professional who can. Many of the stores that sell computers also have services to repair them. When you have access to a clean computer, consider changing your passwords to websites that contain your sensitive information.

**Security Recommendations for Multiple Users and Businesses:**

- **Monitor Your Account Daily:** Review your transactions for errors and suspicious activity.
- **Maintain Dual Control:** Certain functions within our system allow for two levels of authorization when performing a transaction. Consider the use of dual control to maintain the security of your transactions, the protection of your users, and the integrity of your transactions against simple mistakes.
- **Set Dollar Limits:** Enter reasonable dollar limits for each user for ACH origination, wire transfers and internal transfers. Give access to services (and accounts) only to those users that absolutely need them.
- **Use Positive Pay:** This is a fraud protection service that matches your issued checks to your paid checks every day and over the teller counter.
- **Use ACH Block:** Return all unauthorized ACH debits/credits automatically.
- **Train Users:** Make sure your users understand the services they have been provided and the importance of the systems security outlined in this document.
- **Regularly Consult Your IT Resources:** Ensure that your systems keep up with the latest software versions and are protected against invasion by viruses, malware, Trojan horses, keylogging software, etc.
- **Consider Using a Stand-Alone Computer to Perform Cash Management Activities:** Using a stand-alone, hardened computer that is not used for web-surfing or email will limit the exposure to malware and viruses. Make sure that the computer's antivirus software and security patches are installed and kept current.

Your security is very important to us! Please notify us immediately if you feel that your accounts have been compromised in any way. We can be reached toll free at 844-213-5198 or at CEN-CMOperations@my100bank.com **.**