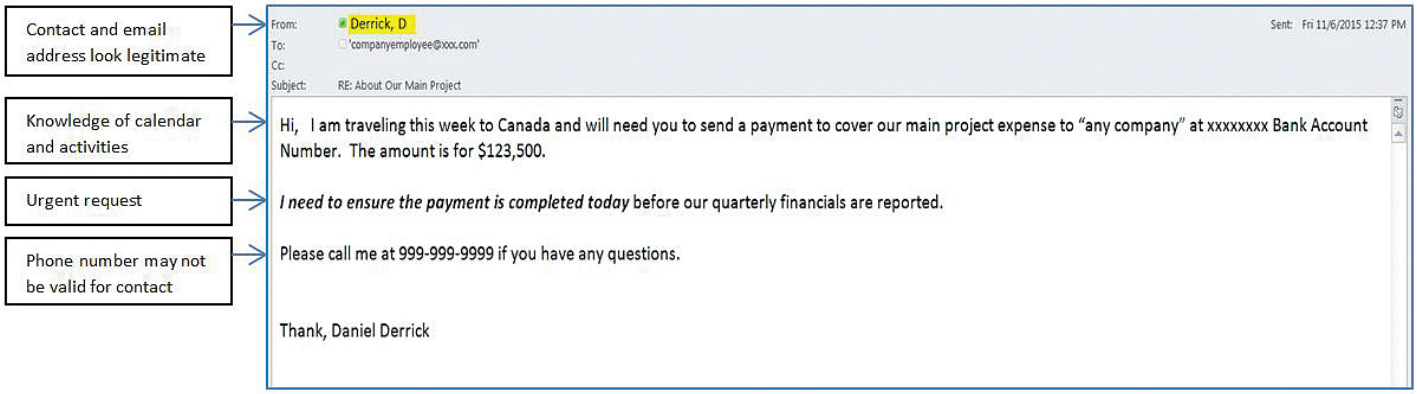
BB&T Payment Solutions

2015 CashManager OnLine Fraud Protection Update

Dear Client:

BB&T is committed to educating our clients and helping to mitigate fraud. As part of that commitment, BB&T recognizes the value of routinely updating our clients on developments relevant to you and your accounts.

In 2015, business email compromise, also called masquerading, has become more prevalent. This fraud involves the use of email or phone in which the cyber-criminal pretends to be a business partner or executive and requests a company employee to send funds typically by ACH or Wire. These requests look real and are urgent in nature. Sometimes, the fraudster even has knowledge of the travel calendar and activities of the individual they are impersonating. Please review this sample masquerading email.



Fortunately, there are effective, common sense steps you can take to mitigate fraud. For masquerading and email fraud, mitigation steps include contacting the sender to validate payment by an alternate method, along with utilizing dual control for payment initiation and regular training of your staff. For additional details, please read the enclosed BB&T Intellectual Capital series, *Fraudulent Emails: What You Need to Know.*

Also, continue to be vigilant in your security procedures and training for associates when accessing BB&T CashManager OnLine and any other financial platforms utilized by your company. Today's threats constantly adapt to circumvent mitigation methods. Commercial account fraud is not covered by Regulation E and is the responsibility of your company.

We recommend your company security officer and CashManager OnLine administrator review the features and recommendations included in our BB&T CashManager OnLine Standard Security Protocol. The enclosed protocol list describes features considered optimal for user access and security. Additionally, the following checklist of highly recommended security measures and sound business practices can provide guidance as you assess your company policies, procedures and training.

While nothing guarantees the prevention of fraud, the standard CashManager OnLine security features are recognized industry best practices. Upon reviewing this information, we invite you to contact your payments consultant if you have any questions.

BB&T is committed to a partnership with you, including education for online financial security. We invite you to contact your Treasury Consultant, your Relationship Manager or call our Treasury Support Team at 800-774-8179 if you have any questions or comments. Thank you for choosing BB&T and using CashManager OnLine to make banking convenient, safe and efficient for your business.

Sincerely,

W. Bennett Bradley

W. Bennett Bradley
Executive Vice President
President, Payment Solutions Division

BB&T Payment Solutions

Standard Security Protocol for BB&T CashManager OnLine®

Criminal attempts to access bank accounts and steal from businesses are becoming more sophisticated. Malicious attempts to steal cash and/or information that can be converted to cash are increasingly common. In addition to direct financial loss, your business could suffer lost productivity, legal costs and reputational loss. As a result, any user access and activity can expose your business to fraud. It's critical every employee with access to CashManager OnLine use all standard security features.

Liability

As a user of CashManager OnLine, you have an obligation to safeguard your credentials and account information from physical or electronic theft, including theft by malware on any/all computers used to conduct business by CashManager OnLine. Under the terms of your company's agreement with BB&T, we are authorized to process payments upon receipt of your CashManager OnLine credentials. Furthermore, losses are not covered under Regulation E. Your company, therefore, is liable for any loss of information or funds due to payments originated with stolen credentials. BB&T closely monitors its systems to ensure only valid credentials are used to initiate funds transfers. Failure to safeguard your credentials physically or electronically can result in fraudulent access to your CashManager OnLine account, unauthorized funds transfers, and financial loss to your company. It is critical to protect your credentials and computer systems by following Standard Security Protocol.

BB&T provides the following standard CashManager OnLine security features:

- Logon Credentials. Company system administrators (CSAs) are provided logon credentials. CSAs then create credentials for company users. A temporary password is created for each user who is subsequently prompted to change it at initial log in. Passwords expire every 30 days – new passwords should contain a mix of uppercased and lowercased letters and numbers, no special characters, and be at least eight characters in length.
- Security Token. BB&T provides CSAs with security tokens for distribution to all company CashManager OnLine users. A security token is a small, connectionless device that generates a one-time passcode to use at log in. Once activated, every time a user logs in to CashManager OnLine, the token code allows BB&T to authenticate each user and validate each user is logging in to a legitimate BB&T CashManager OnLine session. Additionally, company users who have release authority for account transfers, wire transfers or ACH transactions must further authenticate those transactions by performing the security token passcode process each time those transactions are submitted for release.
- Trusteer Rapport. Trusteer Rapport software protects your company's financial assets and business data during every CashManager OnLine banking session. BB&T will automatically prompt all company users to download Rapport by an in-browser message and hyperlink. Users should consult their IT or system administrator as necessary. Failure to download Rapport on all PC/Mac devices used for CashManager OnLine will result in discontinued access after a period of 30 days from initial user prompt.
- Dual Approval for Payments. Dual Approval for Payments requires one user to initiate a payment and a second user, with a second set of credentials and using a second computer, to approve the release of the payment.
- User Entitlements. Users should be entitled to only those functions and accounts necessary to perform their normal activities. These entitlements should be reviewed regularly.
- Payment Limits. A maximum wire transfer payment limit is assigned by BB&T based on your company's needs. This limit, along with other payment limits you have established for your company and individual users, should be routinely reviewed.
- Event Notification Service. Event notification allows users to receive messages through their selected delivery method when account payment activity occurs and when changes are made to a user's entitlements or profile. Notifications of unexpected activity enable action to be taken more quickly. Certain notifications – Administrative Alerts – are automatic to alert the company administrator(s) and/or affected user(s) of potentially suspicious activity. These include: new user set up, user modified or deleted, modifications to a user's security privileges, changes in a user's email address, change in a user's mobile data or carrier's text delivery, password changes, changes to a user's service entitlements, account list or screen settings. (Note: "user" in these descriptions also includes administrator.)

While Standard Security Protocol will not guarantee the prevention of fraud or change your liability if fraud occurs, these featured components are recognized best practices. Rejecting the use of any component will put your company at greater risk for fraud. BB&T monitors anomalous activity and behavior. You may be periodically asked to validate transactions.

BB&T Payment Solutions

Highly Recommended Security Measures and Sound Business Practices

BB&T recommends you review these measures routinely.

- ☐ Dual Approval for Administrative Changes. Dual Approval for Administrative Changes provides you with added security by requiring a second "administrator of record" (an additional CSA registered with BB&T rather than a user entitled to security privileges) approve all user profiles, entitlements, settings, and account changes. These multiple administrators of record are maintained by BB&T and must have identical entitlements, settings, and accounts. This added security impedes fraudster attempts to gain administrative control. To establish Dual Approval for Administrative Changes, please contact BB&T Treasury Management Client Support at 800-774-8179.
- ☐ Activity Limits and User Entitlements. Implement limits on activities, payments, and active session thresholds by user and company.
- ☐ Review Accounts Daily. Notify BB&T immediately of unusual activity.
- ☐ Employ Positive Pay and ACH Control. These features are widely recognized best practices for preventing unauthorized paper and electronic payments.
- ☐ Use a Stand-Alone Computer. Designate one computer exclusively for online banking. Limit Internet access and prohibit email to minimize exposure to malware.
- ☐ Sign Off and Power Down. Always sign off from your CashManager OnLine session. And, to ensure you are availing your computer of the most current Trusteer updates, always power down your computer at the end of your work period.
- ☐ Exercise Sound Password Management. Prohibit the sharing of passwords, require strong passwords with a mix of characters and cases, use a different password for each website accessed, and regularly change passwords. Do not store passwords on your computer in case it is compromised.
- ☐ User Education. Aware and alert CashManager OnLine users are an effective defense against payments fraud. Establish an online fraud awareness program and conduct regular training sessions. Conduct periodic risk assessments. Train all employees to recognize and prevent online fraud. BB&T regularly provides fraud prevention webinars for CashManager OnLine users, administrators, and company executives. Contact BB&T Treasury Management Client Support at 800-774-8179 to register. For current security information, please visit BBT.com/security.
- ☐ Remain Alert. BB&T will never ask for your login credentials, including requests to respond to or click on a link within an event notification message.
- ☐ Report Immediately. If you experience fraud, stop, quarantine your computer, and immediately contact BB&T Treasury Management Client Support at 800-774-8179.
- ☐ Insurance. Cyber theft occurring with the use of valid credentials is not covered by the bank. Discuss cyber liability with your insurance provider.

Understanding the Threat

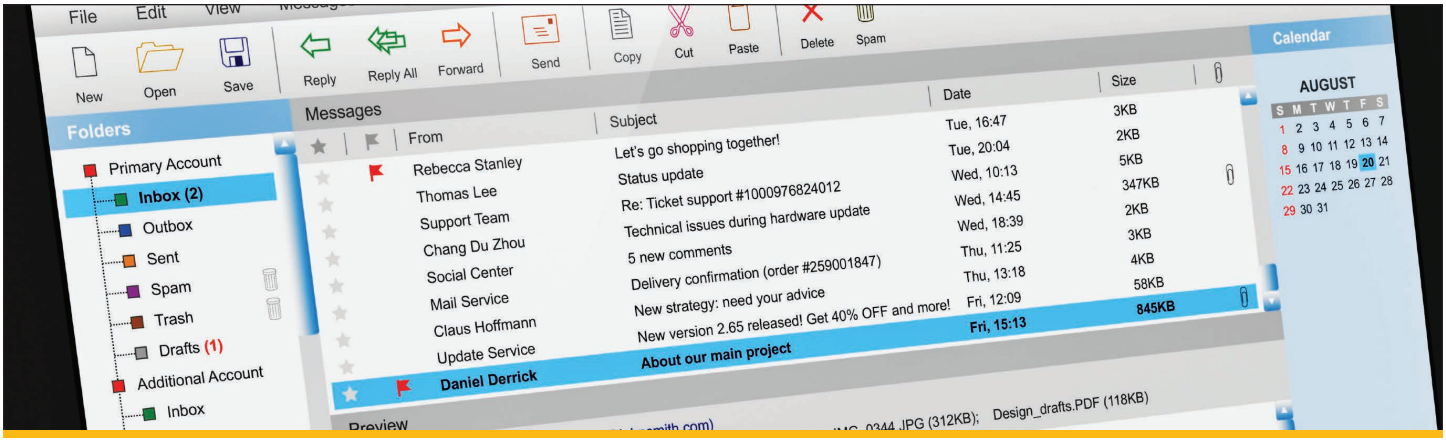
The goal of online thieves is to trick you into providing your password, user ID, and token code(s) so they can access your CashManager OnLine account and steal money. To obtain your credentials, a thief may send you an email purportedly from a trusted source such as a government agency, business, or bank. The email may ask for your credentials directly or ask you to click on a link that secretly downloads malicious software to your computer. Malware may even be loaded on your computer by visiting seemingly innocent websites or through fake security updates. It is important to protect your computer as the malware can activate when you attempt to visit your online banking website and hijack your session, log your key strokes, or insert fake login pages into your browser. The malware can transmit your credentials to the thief for illicit use. The latest threats may not be detected by anti-virus software.

If you are concerned about the authenticity of a communication or experience unusual system behavior such as failed log ins, timeout, pop-ups, requests to download software (aside from Trusteer Rapport), maintenance screens, or failure to advance to the next screen, this may be a sign of fraudulent activity. **Stop and immediately contact BB&T Treasury Management Client Support at 800-774-8179.**

Checklist Completed By_____ **on** _____

Company Representative **Date**

BB&T recommends you file this assessment with your company security procedures.



BB&T Intellectual Capital Series

Fraudulent Emails: What You Need to Know

Most of us are aware of phishing scams, which use emails that appear to be from trusted individuals or companies to trick recipients into clicking links or opening attachments. Criminals are now taking this approach a step further with potential for severe financial consequences to businesses.

if you have ever received payment instructions from a boss or vendor by email you are at risk. Fraudsters have been very successful at impersonating superiors, peers, and vendors to get businesses to send them wire and ACH transfers information. They have stolen hundreds of thousands of dollars at a time. The bad guys either compromise known parties' emails or create similar looking emails (e.g., johndoe@example.com vs. johndoe@examp1e.com).

This can involve the impersonation or takeover of legitimate email addresses too, as very sophisticated criminals target corporate executives and try to take over their email.

The bad guys will request payments be made or give new account numbers for future payments. The email requests may look like regular correspondence between you and another party or even be inserted into an ongoing conversation. The email requests will often have a sense of urgency, playing on your desire to help your boss or long-time trading partner.

To protect your company's money please do the following:

- *Always verify requests for wire or ACH transfers received by email. Perform call backs to other parties on known numbers to validate all requests received by email.*
- *Match up requests with known invoices.*
- *Use dual approvals for payments.*
- *Don't be afraid to ask questions. A one minute phone call is all it takes to protect your company's money.*

Fraudsters are relying on social engineering, because they know a person at a company is usually going to open an email from an executive or senior manager. Recipients will probably click on any links or open any attachments in that email.

Fraudsters also target other people at a company to try and gain information directly from the messages. There may be sensitive or confidential business information going out from that company so tapping into such information is a treasure trove for criminals, helping them determine the identities of your valued clients.

Employees can now get exploited by emails that appear to contain tapping into this sensitive or confidential business information from trading partners. These criminals anticipate your employees will trust emails from those valued businesses and make sure all invoices are paid. Overall, criminals have found it is much easier to exploit trusted relationships than to hack their way into a company.

Share this information with anyone in your organization authorized to make wire or ACH transfers. As your employees open email messages in their inbox, be sure they are aware of such fraud attempts!

Fraudulent email awareness tips –

- ***Watch for emails that appear to come from a legitimate source like a well-known company, bank, manager or executive, online payment service, or government organization.*** Be wary of what you read – messages can be very convincing. Scammers register domain names similar to real sites and also copy logos, content and supporting links from real sites. The "from" address can be masked, making emails appear legitimate.
- ***Be suspicious of emails that threaten dire consequences to scare you into action or promise a reward.*** Watch for messages that ask you to provide personal or company information. Ask yourself, "Do I know the sender? Am I expecting a message from this company? Did I initiate action that would result in a response from the organization?" If you don't know the sender or were not expecting a message, it's probably phishing.