

Dual Control: A Best Practice to Safeguard against Electronic Payments Fraud

As evidenced in recent news, there are growing concerns across the industry about Internet fraud. Additionally, the FDIC continues to warn companies of increased electronic funds transfer (EFT) fraud. Most incidents of EFT fraud are a result of compromised login credentials and are perpetrated using malicious software, key loggers or illicit email messages; however, EFT fraud can also be perpetuated internally by employees who have access to initiating and approving EFT transactions without additional safeguards.

The U.S. Treasury Department has reported increased incidents of wire transfer fraud and of fraud targeting ACH batch transfers. You can greatly reduce your company's exposure to electronic payments fraud by instituting the best practice of dual control approval for initiating and releasing wire and ACH transactions.

How dual control works

By selecting dual control you are separating the duties of your iTreasury users.

- An administrator or user who enters or creates a payment (ACH batch, wire transfer) will not be allowed to release that payment without the input of a second administrator or user to release or approve the transaction
- A second administrator or user is then required to review the payment and release it

It is important to note that dual control is applicable for your company's iTreasury administrator as well once established, because the administrator cannot act alone to both initiate and release payments.

The benefit of dual control

If for some reason an administrator's or user's credentials are compromised and a fraudulent Wire or ACH is created, those compromised credentials cannot be used to release the payment; rather, another user with different credentials is required to release the payment. This is especially important if the compromised credentials belong to a systems administrator, since the administrator has the ability to create and change user entitlements. The administrator's compromised credentials could be used to grant the ability to any user – including their self-- to create and release transactions. However, this would be impossible with dual control in place, as the payment could not be released using the administrator's compromised credentials.

As the systems administrator, it is important that you identify who in your company will have the ability to create payments and who will have the ability to release payments and establish those permissions within iTreasury.

Contact us today to enroll

Protect your company. Set up dual control for your iTreasury payments today. There is no additional charge for this important safeguard.

Contact your Regions Treasury Management Officer to request enrollment, or call Client Services at 1-800-787-3905 to be directed to your Treasury Management Officer.