ORIGINATOR EDUCATION - 2025

A checklist approach to payments could help Originators comply with rules and regulations, avoid errors, and reduce fraud. A basic electronic payment checklist might include 10 steps.

Electronic Payment Checklist:

1. Authenticate the requestor when adding or updating a Receiver (i.e. payee).
2. Confirm validity of authorization change request through a separate channel using know contact information.
3. Verify account number of receiver prior to the first payment.
4. Verify routing number of receiver prior to the first payment.
5. Confirm effective date of transaction.
6. Confirm payment-related information.
7. Confirm sufficient funds in funding account.
8. Obtain approval for transaction.
9. Initiate transaction.
10. Require a second person to confirm and release the transaction. (Dual Control)

Some of the steps above are required by rule or law, while others are necessary to route the transaction appropriately. When any step goes wrong, the error decreases the efficiency of the payment process. It can even cause a transaction to be misrouted, possibly without opportunity for recovery. The checklist offers a low-cost guide that can provide value to a financial institution's payment initiation customers while increasing the quality of transactions the institution receives from its customers. These steps merely provide a starting point for customizing a checklist to fit a particular need. The usefulness of a checklist derives from the fact that creating an electronic transaction involves a series of steps. Any step can be missed. Consistent use of a checklist may help payment initiators to ensure each transaction complies with rules, is free of errors, and reaches the intended recipient.

The last steps in the Electronic Payment Checklist are particularly important. They constitute a traditional fraud mitigation activity called "dual control." Originally designed to thwart internal fraud, dual control has a renewed relevance in an age of identity theft, imposter fraud, and business email compromise and corporate account takeover.