Financial institutions on the RTP® network already know that the rise in digital transactions makes doing business a lot easier. But it has also led to an increased number of account numbers being stored in locations outside the banking system. This makes account information a potentially vulnerable target for hacking. If account numbers are improperly accessed, they can be used to initiate unauthorized debits in the ACH or to create fraudulent checks.

Enhanced Security with Account Tokenization Capability

Secure Token Exchange is a new capability available for payments on the RTP® network that issues tokens for financial institutions’ account numbers. These tokens are used like real account numbers in the RTP network, which helps to reduce financial institutions’ account numbers from being stored outside the banking system. An RTP payment that uses a token is sent through the network in the usual way.

RTP Account Tokenization

Tokens are random numbers to stand in for a customer’s account number so that the real number does not need to be used to send or receive a payment.

Even if compromised, the token is of limited or no use to cybercriminals.

Compliance Heads Up for All RTP Participating Financial Institutions

All RTP participants, whether choosing to have tokens issued for their account numbers or simply receiving RTP payment instructions from their customers or payments from the network in which the other financial institution’s account numbers is a token, need to verify that compliance practices, such as AML monitoring and reporting, can accommodate tokenized account numbers. As part of its RTP account tokenization capability, The Clearing House will support translation of a counterparty participant’s tokens to real account numbers for compliance purposes as needed.