



## **RAMPING UP PREPARATIONS FOR REAL-TIME PAYMENTS**

Considerations for businesses to adapt to this paradigm shift in transactions, allowing companies to send and receive payments 24/7/365.

**M&T** Bank

Countries such as Japan, Sweden and Finland have a faster payment system and no longer use paper checks. In contrast, every year in the United States, consumers and businesses make and receive more than 140 billion non-cash payments with a total value of more than \$175 trillion using checks, wire transfers and/or credit cards.<sup>1</sup>

Thanks to ongoing collaboration by numerous stakeholders – from the Fed to banks and credit unions to retailers, consumer groups and financial regulators – real-time payments are becoming a reality in the U.S. The Clearing House participated in this collaboration and set out to create its own infrastructure and system, now known as Real-Time Payments.

Real-Time Payments is the first new payment method launched in the U.S. in over 40 years. The last major payment rail system built domestically was the Automated Clearing House (ACH), established in 1974. At that time, the Fed and many financial institutions realized the financial system was manually processing so many paper checks that the system was unsustainable. From that point on, ACH began to absorb a portion of check transactions allowing consumers to take advantage of electronic efficiencies.

Today, the Clearing House has created its Real-Time Payments system to help ensure:

- A universal, safe, and faster electronic solution for business and personal payments
- The ability to settle payments rapidly and with finality
- Immediate notification, confirmation, and real-time messaging
- Universal access to users

<sup>1</sup> Federal Reserve, Faster Payments Task Force, "The U.S. Path to Faster Payments: Final Report Part One," Jan. 2017, <https://www.federalreserve.gov/newsevents/press/other/US-path-to-faster-payments-pt1-201701.pdf>

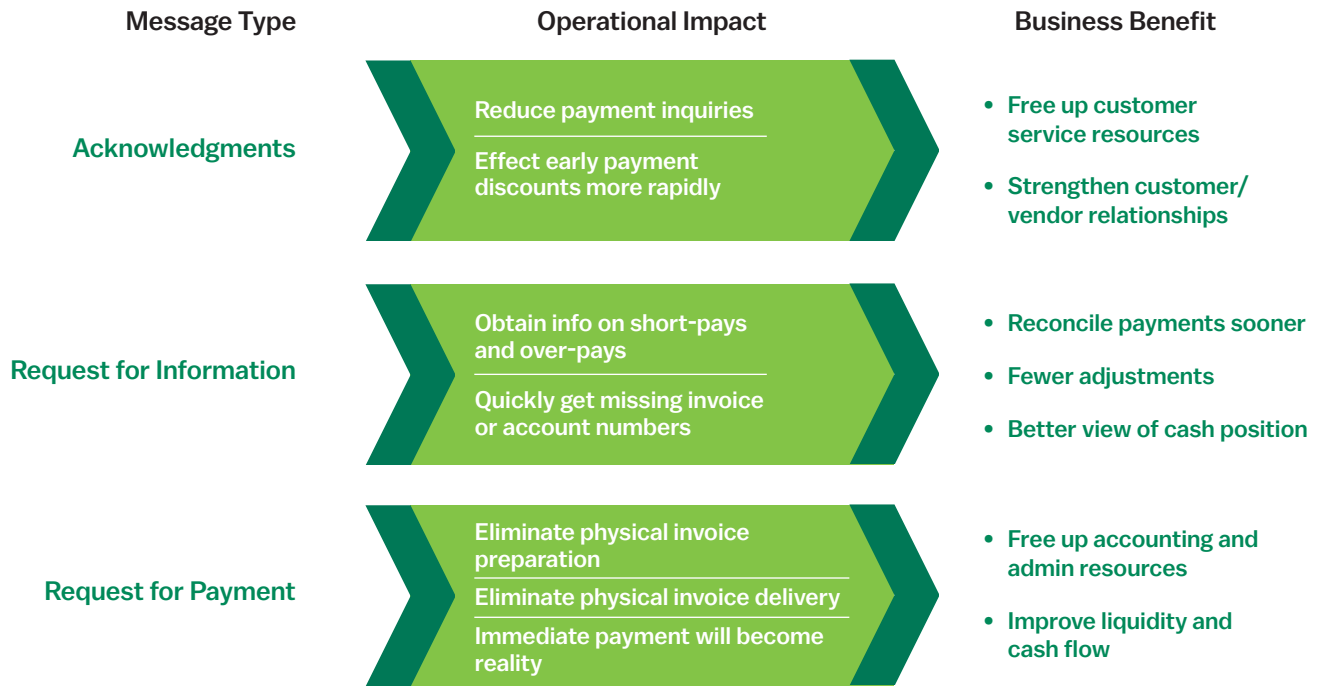
## MODERNIZATION OF BILL PRESENTMENT AND INVOICING TO IMPROVE CASH FLOW

The first real-time transactions on the Real-Time Payments system began processing in November 2017. Experts foresee many use cases for Real-Time Payments, including invoices, payroll, expense reimbursement and submissions to tax authorities – all of which serve to improve cash flow for businesses.

In addition to speed, the Real-Time Payments network will provide the ability for senders and receivers to communicate digitally in this fully integrated system in a way that does not exist with checks or ACH. For example, a sender will receive an almost instantaneous notification from their bank confirming that the payment was delivered or returned.

As the non-monetary messaging component of Real-Time Payments is implemented, businesses will have the opportunity to further modernize operations with the ability to send and receive real-time Acknowledgements, Request for Information (RFI) and Request for Payment (RFP) messages. This messaging provides transparency to all parties involved.

## BENEFITS OF NON-MONETARY MESSAGING



Acknowledgements may help to alleviate customer service workload by reducing the number of inquiries on whether a payment has been received. Similarly, requesting information could be used to obtain reasons for over-pays or short-pays, freeing up time used for outbound inquiries for information. For example, if a payment is received without documentation, the recipient can instantly message the sender to ask for an invoice or account number, enabling proper credit to the correct account. In a business/supplier relationship, the supplier can offer discounts to a business that pays by a certain date. The business can instantly make a payment on that date and see the discount immediately applied by the supplier. In turn, the supplier can confirm receipt of payment and let the business know the ordered goods will be shipped on a certain date.

Request for payment has the potential to eliminate the need for physical invoice preparation and delivery, and businesses can take steps now to ready their accounting systems. Businesses can begin preparing to support the sending of RFP messages by creating a centralized directory of vendors and suppliers to include account number, email address and phone number for payment purposes. Real-Time Payments are

currently account number-based but are expected to enable email- and phone number-based payments, similar to Zelle®.

### A NEW VIEW OF SECURITY AND FRAUD PREVENTION

Fraud and security also need to be a focus for banks and customers, to help ensure re-use and upgrades are made to key suspicious detection systems, such as those that are used to support ACH and Wire.

In today's use of wire transfers, there is a significant time lag in processing. Processing a wire transfer can take up to 90 minutes, which enables an end user or banker to flag a suspicious transaction for fraud review and, in some cases, pull back the transaction before the money reaches the recipient.

In the world of Real-Time Payments, the ability to correct a transaction disappears because the activity can be processed in as little as two seconds. This puts the impetus on ensuring the recipient is the person or business that really should be getting the funds prior to clicking the "send payment" button.

One potential security improvement: In this new payments universe, passwords likely will be a vestige of the past – replaced by tokens. Users with mobile devices that have fingerprint capability will have tokens stored on their devices to be used in combination with randomized tokens unique to each transaction.

To help ensure real-time fraud is controlled, the current U.S. dollar limit on a Real-Time Payment transaction is \$100,000. When real-time payments first went live in the United Kingdom in 2008, transaction limits were set at a similar level, but quickly increased as demand ramped up and the system became familiar to participants. Limits may continue to go up in the U.S. as security protocols become established here. Presently, all real-time payments in America are U.S. dollar-based.

## M&T BANK PLATFORM CHANGES COMING SOON

M&T Bank is taking steps to meet customer demand as Real-Time Payments become more mainstream. We are adding functions to our existing platform, which will enable our customers to see Real-Time Payments come into the network as part of their cash position. In addition, we are building a new, modernized core platform with a centralized payment hub in our flagship product, M&T Bank Treasury Center<sup>SM</sup> for Commercial and Business clients. Small businesses will also be able to enroll in Real-Time Payments with our M&T BizPay product.

## THREE STEPS TO PREPARE FOR REAL-TIME PAYMENTS

Decision makers should be preparing now for changes to the payments system that will be taking place over time, such as readying accounting and data systems to take full advantage of real-time payments.

- 1** The first step is to determine whether your accounting systems can support Real-Time Payments. Work with your system vendor to make sure they have the technology in place.
- 2** Next, determine your company policy on real-time payments. Consider questions such as: how will you reconcile payments received after hours, on weekends and holidays? How many approvers are needed to send a payment, and how does that process operate outside of normal work hours and/or locations? Don't hesitate to hold a company brainstorming session that includes all departments.
- 3** Finally, prepare every employee to resist potential fraud in the Real-Time Payments environment. Many fraudsters have moved to softer targets: hacking people via social engineering techniques such as impersonation fraud and business email compromise. One study found 78 percent of companies were targets of payments fraud last year.<sup>2</sup>

Three of the most common forms of impersonation involve unverified messages. The first is executive impersonation, in which criminals impersonate one or more senior company executives via email in an attempt to trick an employee into sending money. Always verify such incoming emails are truly from the alleged sender using previously known contact information.

The second is employee impersonation. This involves scammers hacking an employee email account to send what appears to be a legitimate email to payroll/accounting requesting the employee's account number and payment address change.

Lastly, there is vendor impersonation, which operates in a similar fashion to employee impersonation. This type of fraud is executed in a variety of ways, but all result in a payment request that appears to come from a vendor familiar to your organization.

All employees should be trained to be suspicious of any message asking for passwords or access to files.

**[Learn more in Three Ways to Help Prevent Executive and Vendor Impersonation.](#)**

<sup>2</sup> 2018 AFP Payments Fraud and Control Survey

**Questions?**  
We're here to help.



**CALL**  
1-800-724-2240 or your  
Relationship Manager



**CLICK**  
At [mtb.com/commercial](https://mtb.com/commercial)