The Effect of COVID-19 on Real-Time Payments

By Judy Mok and Amy Schwartz

Fraudsters are nothing if not opportunists. As the world has struggled with a global pandemic and economic uncertainty, fraudsters have thrived. Federal agencies such as the FBI, DOJ, and FTC have all warned that fraudsters are aggressively targeting businesses and consumers with COVID-19–related scams.[1] And the numbers bear that out: a recent TransUnion survey found that nearly a quarter of Americans have been targeted by COVID-19 scams since the start of the pandemic.[2] Businesses and consumers will almost certainly face more fraud attempts in 2020 than ever before.

As The Clearing House's real-time payment (RTP) network gets a foothold in the United States, it too will become a target for fraudsters looking to make a quick buck. This article discusses the new RTP system, the benefits of RTP, the potential for fraud in connection with real-time payments, and the laws that may bear on loss allocation.

RTP Network

a. What Is RTP?

In the United States, RTP is a new network rail operated by The Clearing House, an association of some of the largest U.S. banks.[3] Any federally insured depository institution can be an RTP participant, regardless of size. At present, RTP's network reaches 53 percent of demand deposit accounts in the United States.[4]

A real-time payment is one where money moves almost instantaneously from one bank account to another. It can be executed at any time and on any day. RTP is a "push" payment system, meaning that payment is sent directly from the payer's bank to a recipient's account—the payee does not need to "pull" the funds from the payer's account using the payer's account information details. As a result, recipients typically receive payments within seconds of the sending bank initiating the transaction. Notably, a sending bank will not be able to revoke or recall a payment once it has been authorized and submitted to the RTP network (although there is a process to facilitate bank-to-bank communication around the return of funds).

b. Benefits of the RTP Network

RTP offers extraordinary convenience. As its namesake benefit suggests, it allows for immediate, certain payments. This can provide important flexibility with cash-flow, which can be particularly useful for cash-constrained small businesses and consumers.

In addition, RTP offers extensive data exchange and real-time messaging, which helps with accuracy, data transparency, and customer engagement. Real-time messaging allows for a two-way dialogue between the sender and the receiver. Among other things, the RTP network notifies the sender once funds have been delivered to allow the sender to better monitor its transactions. The RTP system also provides an audit trail with detailed payment information. By providing senders and recipients with clear and immediate payment information, RTP endeavors to mitigate fraud.

c. RTP Is Expected To Grow

In 2019, the Federal Reserve Board (the "Fed") announced that it too would join the world of real-time payments. The Fed plans to launch its FedNow℠ Service (FedNow) in 2023 or 2024. FedNow would operate alongside RTP. The Fed's foray into real-time payments ensures that real-time payments will expand quickly.

The expansion is for good reason. As social distancing and contactless business became requirements during the COVID-19 pandemic, the need for real-time payments became even clearer. At an August 6, 2020, symposium, Fed. Gov. Lael Brainard indicated that "The COVID-19 pandemic is taking a tremendous toll on communities across America."[5] Brainard emphasized that, instant payments through the FedNow service, "will enable millions of American households and small businesses to get instant access to funds, rather than waiting days for checks to clear."[6]

Judy Mok and Amy Schwartz are Of Counsel at Ballard Spahr LLP.

Fraud Concerns with RTP

Although RTP offers a host of fraud-mitigation tools, it is not without its risks. RTP is prone to the same types of fraud attacks and scams that are ubiquitous in other payments systems. Europe, which has had real-time payment systems for years, has shown that real-time systems are susceptible to fraud.

Any "push" payment transaction comes with fraud risks. This is because, once the payer "pushes" the transaction, the funds are out of the payer's control. For example, fraudsters frequently try to trick their victims into sending payments from the victim's bank account to a bank account owned or controlled by the fraudster. The fraudsters' tricks are sophisticated—they use social engineering tactics and impersonation scams to present seemingly legitimate requests for money. Once the victim authorizes the payment, the funds appear in the fraudster's account in real time. Fraudsters then quickly transfer or withdraw the money. Because RTP transactions are irrevocable, and because settlement happens in real time, victims cannot reverse a payment and the funds are usually long gone by the time the victim discovers the scam.

In the United Kingdom, push payment fraud increased 44 percent in 2018.[7] In 2019, it continued to climb, with a 40 percent increase in the first half of the year.[8] As RTP gains popularity in the United States, it too is likely to be a target for fraud. This is especially true given the recent increase in the transaction limit from \$25,000 to \$100,000.[9] Given that fraudsters can now trick victims into sending larger dollar transactions, there is a heightened incentive for fraud.

Like other payment systems, the RTP network is susceptible to account takeover scams (ATO). In ATO scams, fraudsters use phishing or other scams to mine for a victim's private financial data. The fraudster then uses the private financial data to assume control of the victim's accounts. Once the fraudster assumes control, the fraudster then pushes payments from the victim's account to an account controlled by the fraudster. Because of the speed at which RTP payments move, account holders who are not actively monitoring their accounts may not even know that their funds are being stolen until the funds are already gone.

Although RTP has built-in fraud mitigation technology, the technology is not foolproof. When payments are paid and settled in real-time, there is less time to catch fraud. Victims have less time to monitor their accounts to prevent fraud on the front-end. Banks have less time to screen for fraud. Moreover, once stolen funds are in the RTP system, it is exponentially harder to recover them. Savvy fraudsters can transfer stolen funds through multiple accounts in mere seconds, making it near impossible to trace and recover stolen funds.[10]

Governing Laws

RTP transactions are primarily governed by: (i) the RTP System Operating Rules and incorporated governing documents (collectively, the "Operating Rules"); (ii) Article 4-A of the New York Uniform Commercial Code (Article 4-A); and (iii) the Electronic Funds Transfer Act (EFTA) and Regulation E (Reg E). For commercial and non-EFTA consumer payments made through the RTP network,[11] the rights of the participants and parties are governed by the Operating Rules and Article 4-A. Conversely, for RTP payments subject to the EFTA, the EFTA and Reg E apply and, to the extent consistent with the EFTA and Reg E, the Operating Rules and the laws of the State of New York also apply, excluding Article 4-A.[12]

Given the different laws that can govern RTP transactions, the risk of loss can vary based on the nature of the payment (EFTA vs. non-EFTA) and the specifics of the transaction. As between participating banks, in push transactions like RTP, the sending financial institution tends to bear the risk of loss because it is the party that is responsible for authenticating its customer and submitting the customer's payment on the RTP system.[13] By comparison, the receiving institution plays a much more passive role: it simply accepts payment.[14] Thus, the receiving institution tends not to bear liability.

On the other hand, the loss allocation principles as between a consumer customer and the sending bank present a much more complex picture. For RTP payments covered by the EFTA and Reg E, the obligations under EFTA and Reg E would control, and cannot be varied by agreement.[15] Consequently, if a consumer notifies their bank of an unauthorized EFTA transaction within the designated notice periods, the sending bank may suffer the loss. Alternatively, non-EFTA payments are governed by the Operating Rules and Article 4-A, both of which allow loss allocation modification by agreement.[16] Consequently, agreements between a sending institution and its commercial customer may affect the allocation of loss and afford the parties additional clarity on their rights and responsibilities.

Conclusion

Convenient, fast, and contactless payment methods like RTP are gaining a foothold in the United States and, as the pandemic drags on, are nearly certain to increase in popularity in the near term. As RTP becomes more mainstream, fraud attacks on it are likely to increase as well. Savvy financial institutions and commercial customers can protect themselves by having agreements in place to allocate loss and mitigate risk.

Notes

1. FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic, March 20, 2020, *https://www.ic3.gov/media/2020/200320.aspx*; Department of Justice Announces Disruption of Online COVID-19 Related Scams, April 22, 2020, *https://www.justice.gov/opa/pr/department-justice-announces-disruption-hundreds-online-covid-19-related-scams;* COVID-19 Scam Reports, By the Numbers, April 15, 2020, *https://www.consumer.ftc.gov/blog/2020/04/covid-19-scam-reports-numbers*.
2. TransUnion Research Quantifies How Social Distancing is Changing Shopping Patterns, March 24, 2020, *https://newsroom.transunion.com/transunion-research-quantifies-how-social-distancing-is-changing-shopping-patterns/*.
3. *See* The Clearinghouse, *https://www.theclearinghouse.org/about/history*.
4. *See* Forbes, "Real-Time Payments Network Reaches Banks Beyond TCH Members," June 15, 2020, *https://www.forbes.com/sites/tomgroenfeldt/2020/06/15/real-time-payments-network-reaches-banks-beyond-tch-members/#58dde7755f03*.
5. FedNow Service Webinar, "The Future of Retail Payments in the United States," Fed. Governor Lael Brainard, August 6, 2020, *https://www.federalreserve.gov/newsevents/speech/brainard20200806a.htm*.
6. *Id*.
7. UK Finance*, Fraud the Facts 2019, https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf*.
8. *The Guardian,* "Number of Bank Transfer Scams in UK Rises by 40% In A Year," September 26, 2019, *https://www.theguardian.com/money/2019/sep/26/number-of-bank-transfer-scams-in-uk-rise-by-40-in-a-year*.
9. *See* RTP System Operating Rules, § II, C(2).
10. *See* RTP System Operating Rules, §§ II, I.2, VII(C) at *https://www.theclearinghouse.org/payment-systems/rtp/-/media/91B3832A32A54B349998F6F4B85EAFF9.ashx*.
11. *See* RTP Operating System Rules, § I, F.1 at *https://www.theclearinghouse.org/payment-systems/rtp/-/media/91B3832A32A54B349998F6F4B85EAFF9.ashx*.
12. *See* RTP Operating System Rules, § F.2 at *https://www.theclearinghouse.org/payment-systems/rtp/-/media/91B3832A32A54B349998F6F4B85EAFF9.ashx*.
13. *See* RTP Operating System Rules, § III at *https://www.theclearinghouse.org/payment-systems/rtp/-/media/91B3832A32A54B349998F6F4B85EAFF9.ashx*.
14. *See* RTP Operating System Rules, § V at *https://www.theclearinghouse.org/payment-systems/rtp/-/media/91B3832A32A54B349998F6F4B85EAFF9.ashx*.
15. *See* 12 C.F.R. § 1005.6 (comments to 1005.6(b)-2 and 1005.6(b)-3).
16. *See* N.Y. U.C.C. Law § 4A-501(1) ("Except as otherwise provided in this Article, the rights and obligations of a party to a funds transfer may be varied by agreement of the affected party.").