To Catch RTP Scammers in Action, Banks Must Abandon Traditional Security Thinking

Vanguard Report

July 2022

Commissioned by

callsign®

451 Research

S&P Global
Market Intelligence

About the Author

Sampath Sharma

Fintech analyst, S&P Global Market Intelligence

Sampath Sharma Nariyanuri, CFA, is a fintech analyst at S&P Global Market Intelligence, covering technology-enabled payments, lending, insurance, investing and digital banking sectors in the Asia-Pacific region.

Sampath has covered financial services at SNL Financial/ S&P Global Market Intelligence for more than seven years as a news editor. His previous experience includes working as a reporter at Outlook Profit and as an analyst at Amba Research. He is a CFA charterholder and holds a post-graduation diploma in online media from the Asian College of Journalism in Chennai, India.

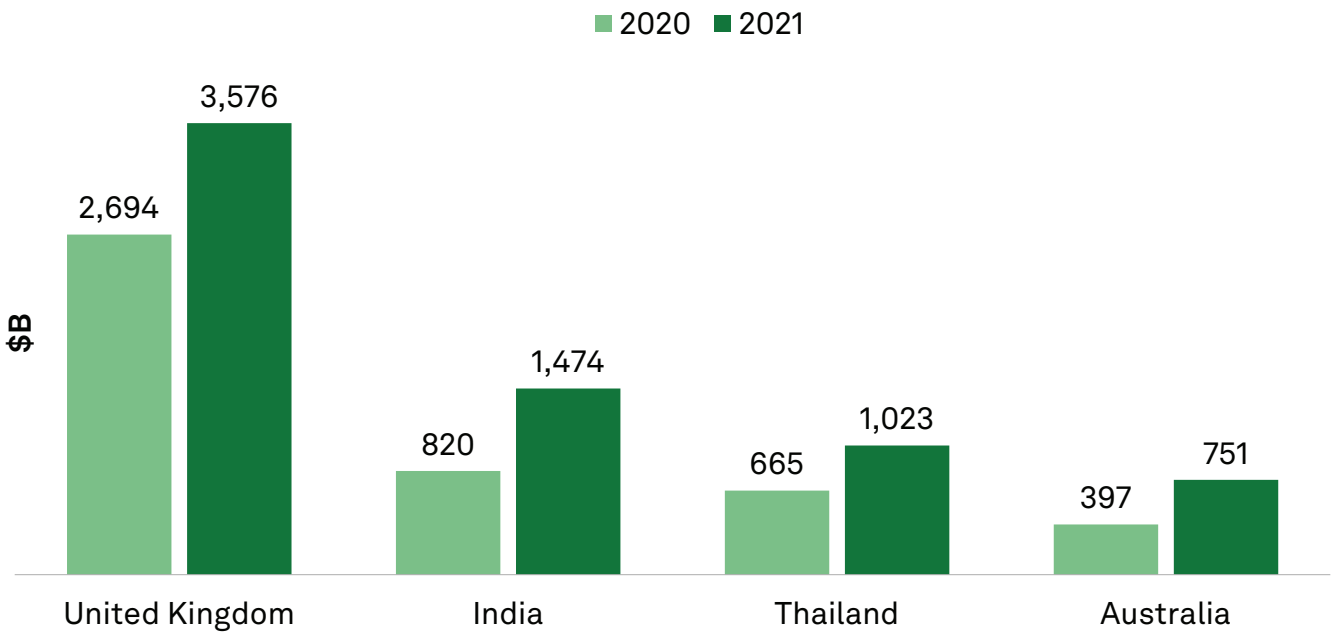
Introduction

Real-time payments (RTP) are growing at breakneck speed in many countries and accelerating the consumer shift to digital banking channels. While their adoption is relatively low in the U.S., financial institutions bringing speed to the table could be poised for significant deposit growth. For more than 45% of U.S. consumers, access to RTP capabilities ranks as an attractive driver for opening a new account with a bank, according to a 451 Research 2022 Voice of the Connected User Landscape (VoCUL) survey. This trend is evidenced elsewhere, with real-time payments growing rapidly (see Figure 1).

But banks courting customers by offering RTP products need to overcome the historical trade-off between speed and security. As the examples of large RTP markets such as the U.K. show, financial crimes can grow at an alarming rate with the rise of instant payments. According to banking and finance industry trade association UK Finance, customers lost £583.2 million in 2021 after being manipulated into transferring money into accounts controlled by fraudsters. The U.K.'s Faster Payments system was the payment method for 97% of those losses.

With the rise of payments processed via Zelle and The Clearing House's RTP network, and the expected launch of FedNow in 2023, financial institutions in the U.S. should prepare for an upswing in fraud. However, banks must look past conventional fraud controls, which largely do not work when the payment goes out the door instantly and cannot be easily reversed. They must adopt a multilayered approach to preventing fraud. Combining behavioral biometrics with device and threat intelligence will help distinguish between legitimate parties and fraudsters; and providing dynamic warnings will further keep consumers safe from scammers.

Figure 1: Global Real-Time Payments Are Growing Rapidly



Source: S&P Global Market Intelligence, central banks and real-time payment system operators

The Take

Faster payment methods will open the door for criminal organizations looking to target customers. Due to limited institutional protections, growing fraud could seriously damage customer trust and become an inhibitor to the sustainable growth of the RTP ecosystem. Meeting the expectations of customers who are used to chargeback-like protections in card frameworks could be an arduous task for banks providing RTP services. The recent flurry of lawsuits against certain large banks over fraud involving Zelle transactions portends ominous consequences if banks do not shore up their defenses.

A fundamental challenge for banks is that their existing fraud and compliance infrastructures are designed for legacy payment methods. Deploying traditional security solutions will not work against fraudsters riding the rails of real-time payments. Conventional fraud-prevention approaches focus on the accuracy of payment instruments and the authenticity of the payer, but the most common method of RTP fraud involves legitimate users executing money transfers from their own devices under the manipulation of scammers.

Banks' fraud-prevention strategies therefore need a significant revamp, and must focus on detecting signs of scams in real time so they can nudge and alert customers appropriately. Banks need to move fraud screening earlier in the payment journey in order to understand the identity and intent associated with the transaction. Identifying users and intent *before* the transaction is initiated helps banks make better and faster decisions on legitimacy. In addition to consumer education activities on security best practices, banks must take steps to enhance their understanding of the biometric behavior of their customers while using the bank's digital platforms to stop account takeover attempts and also to identify suspicious behavior.

The implementation of effective real-time warnings across digital banking platforms can reduce the instances of consumers falling victim to fraud scams. But for such interventions to work, the fraud messaging system needs to be intelligent and timely, and must create contextual and effective messages. Ultimately, the intervention system should strike a balance that can ensure payments are secure without creating too much friction in the user's payment journey.

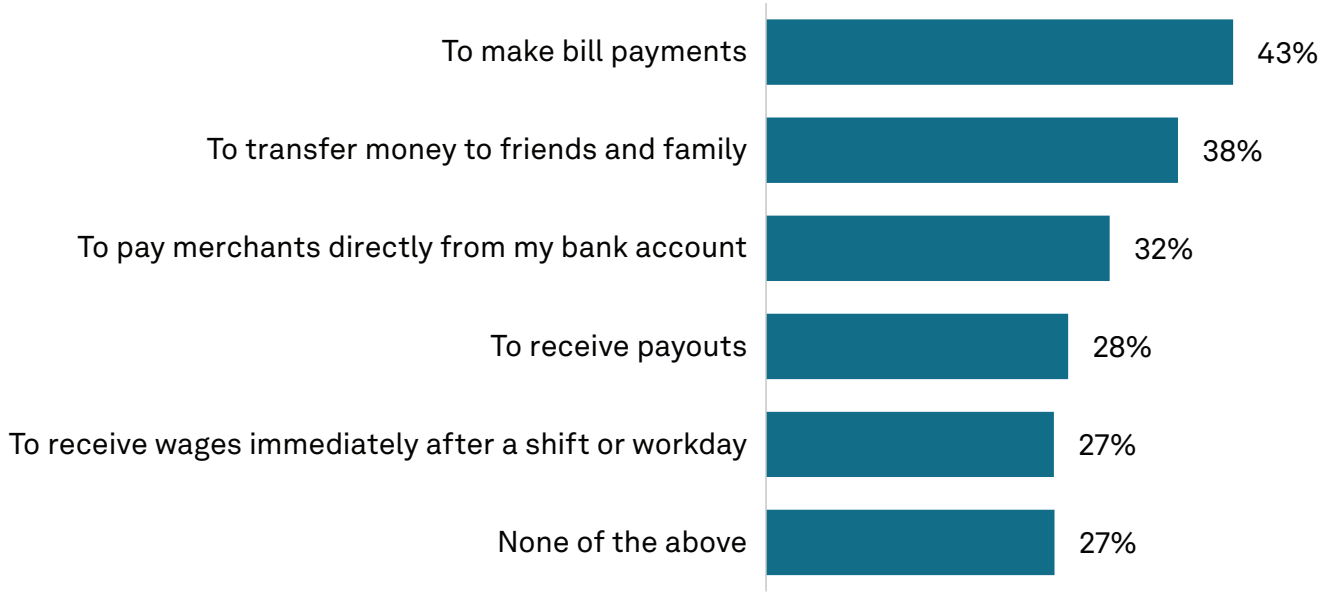
Effective fraud-prevention must be able to detect all types of fraud across all digital banking channels. As fraud continues to evolve, banks must constantly strive to stay ahead of fraudsters. Meanwhile, regulatory leadership is likely needed to protect the overall industry and enable sharing of digital overlay services such as account name checking, but excessive intervention is undesirable.

Unpacking RTP Fraud

Compared to card payments, RTPs support a different set of use cases and provide no built-in payment protections to customers. Fraud strategists must look at the drivers of RTP usage to understand the nature of fraud attacks specific to faster payments. The absence of chargeback-like protections in the peer-to-peer context should cause banks to double down on their investments in fraud-prevention capabilities.

Peer-to-peer transactions and bill payments are driving usage of instant payments in most large RTP markets, while cards remain the primary payment method at the point of sale, both online and offline. In the U.S., too, consumers are most inclined toward using RTPs for paying utility bills and for sending money to friends and family, according to the 451 Research VoCUL survey.

Figure 2: Real-Time Payments Use Cases



Q. In which of the following ways would you be interested in using real-time payments? (Check all that apply)
Base: All respondents (n=1,670)
Source: 451 Research's Voice of the Connected User Landscape: Connected Customer, Disruptive Technologies 2022

Fraudsters understand that RTP users feel comfortable making instant payments to someone they believe to be legitimate. Using social engineering tactics, they convince their victims to transfer money to bank accounts operated by the attackers. As corporations are increasingly using RTP networks, fraudsters are targeting their employees by impersonating colleagues or vendors.

Authorized push payment (APP) fraud, where victims are tricked into authorizing transfers into scammers' accounts, has so far emerged as the most common fraud in RTP markets. Other pertinent issues include bank account takeovers, where fraudsters take over the accounts of victims by using their stolen identities.

A potential jump in RTP fraud could have a devastating impact on banks' relationships with their customers. This is especially critical given that not all consumers express great faith in banks' fraud-prevention abilities.

Given the vast amounts of money coursing through RTP pipes, it is untenable for most banks to provide guaranteed protections for consumers and businesses, especially due to the absence of interchange-like economics on RTP transactions. Even if banks are not liable for reimbursing RTP fraud losses, customers will still expect banks to resolve their problems.

Consumer anxiety around the safety of direct transfers from their bank accounts was captured by 451 Research's VoCUL survey. Just 45% of surveyed consumers view payments via the Automated Clearing House (ACH) as extremely secure, with that percentage dropping to just 27% among Generation Z consumers.

The lack of customer trust in banks' fraud-prevention capabilities only adds to the challenge. Fewer than three in five (58%) respondents in 451 Research's VoCUL survey signaled high confidence in their bank's ability to protect them from fraud. Again, Gen Z consumers were relatively more skeptical, with fewer than half (47%) ranking banks' fraud-prevention abilities highly.

Being indifferent to customer complaints could lead to significant reputational damage for banks. On the other hand, those banks that build robust fraud-prevention capabilities could quickly earn customer trust and build a competitive edge.

RTP Fraud Solutions

Turning to traditional fraud infrastructure will not help prevent RTP fraud, since conventional solutions typically operate in a batch environment and cannot handle the increased speed and complexity that comes with instant payments. Solutions deployed in traditional banking channels focus on the accuracy of payment instructions being submitted, but such rules-based payments vigilance is not enough to detect manipulated consumer behavior in an authorized push payment.

Implementing a fraud-prevention process with a real-time approach first requires understanding the recurring behavioral traits of payments users, and then leveraging that knowledge to detect social engineering scams in action. Behavioral biometrics and analytics systems, for instance, review how users interact with their digital platforms and may help detect instances when the consumer is acting under coercion. With behavioral biometrics, banks can detect robotic behavior and prevent bots from taking over accounts. Employing threat-detection software helps identify signs of remote-access trojans, which are another common scam tactic.

Banks must avoid the common pitfall of issuing too many fraud alerts, which could lead to deterioration in the effectiveness of the warning system and create friction in the customer payment journey. Sophisticated scammers anticipate static messages, coach users past the security warnings and manipulate them into revealing personal information or making a transfer to a questionable account. This is where dynamic intervention solutions are superior, since they engage the consumer more directly in detecting and preventing fraud. These solutions reduce false positives and provide personalized messages to customers, leaving little room for warnings from banks to go unheeded.

In building a safe and secure RTP ecosystem, regulators and network operators have a role to play. Countries at an early stage of RTP evolution would do well to learn from best practices adopted by scheme operators in major RTP markets.

For instance, the U.K.'s Faster Payments system operator allows banks to embed an account name checking service into the payment initiation process to reduce misdirected payments and certain types of APP scams. Consumers and businesses can check if the name on the recipient bank account matches the person or business to which they intend to send money. Payment scheme operators can look at the big picture in the industry and provide an outline of fraud controls that all participating financial institutions must implement to protect the safety of the system.

Conclusion

Banks have a significant opportunity to drive increased engagement among their customers by offering instant payment capabilities, but they must set the stage by working to ensure that such payments are secure. Enhancing consumer trust is critical to the growth of the RTP market, given that U.S. consumers currently do not have high confidence in the safety of direct bank transfers.

The RTP opportunity could quickly turn into a nightmare if banks view RTP fraud through a traditional security lens. Since the bulk of RTP fraud is driven by APP scams, banks must invest in advanced security systems, including behavioral biometrics analytics and dynamic messaging systems. Intelligent fraud controls operate in the background without impeding the user's ability to conduct legitimate transactions. Banks embracing a real-time fraud-prevention philosophy can protect the financial lives of their customers and can differentiate themselves from rivals with both speed and security.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence