Issued 11.30.22

RTP Rules Interpretation
Scope of the Request for Payment Warranty

Effective January 1, 2023

This interpretation is issued pursuant to RTP Operating Rule I.C. Capitalized terms not otherwise defined herein have the meaning ascribed to them in the RTP Operating Rules.

Background

Under RTP Operating Rule VII.B.2 (effective January 1, 2023) an RTP Participant that submits a Request for Payment (RFP) to the RTP System must:

> "warrant to TCH and the Message Receiving Participant that the Request for Payment (1) is made for a legitimate purpose and (2) is not part of a fraudulent scheme to induce a payment; harassing, or otherwise unlawful including violations of the prohibition on unfair, deceptive, or abusive acts or practices as set forth in Title X of the Dodd-Frank Act or violations of the prohibition on unfair or deceptive acts or practices in or affecting commerce as set forth in Title 5 of the Federal Trade Commission Act;"

This document provides an explanation of each component of the Request for Payment (RFP) warranty and a non-exclusive list of examples of scenarios that breach the warranty. It is important to note that the same factual scenario may give rise to breaches of more than one component of the warranty.[1]

In addition, certain conditions must be satisfied in order to bring a warranty claim pursuant to the process described in RTP Operating Rule VII.D., including that the Message Receiver initiated a Responding Payment in response to the Request for Payment alleged to have breached the RFP Warranty.[2]

In addition to the warranty described above, a Message Sending Participant must have a reasonable basis for determining that the Message Sender's RFPs will only be used for Permissible Uses and have made such a determination prior to submitting an RFP for the Message Sender. These Permissible Uses are defined in an RTP Rules interpretation as business to business, account to account, consumer bill pay, and certain kinds of initial or final payments.[3]

---

[1] For example, an RFP that is not sent for a legitimate purpose may also be harassing.
[2] Op. Rule VII.D.1.a.
[3] RTP Rules Interpretation: Permissible Uses for Request for Payment Messages (August 1, 2022), https://mc-e3a82812-8e7a-44d9-956f-8910-cdn-endpoint.azureedge.net/-/media/New/TCH/Documents/Payment-Systems/Rules_Interp_Permissible_Uses_RFP_08-01-2022.pdf?rev=36dade9d4d834fc7adda2cab29e54b26&hash=2F13F172A8E24CD652A6F5FEBB36A195.

Guidance and Examples: Application of the Request for Payment Warranty

1. Legitimate Purpose (Non-Consumer Message Sender)

Explanation. This component of the warranty is breached when a non-Consumer Message Sender sends an RFP to a Message Receiver that does not request payment for (i) a current sale or transaction; or (ii) an amount that is due, owed or otherwise agreed to be paid to the Message Sender. [4]

Scenario that Breaches Warranty	Additional Comments
The Message Sender that is a business sends an RFP to a Message Receiver that is also a business. Although the Message Receiver has purchased goods from the Message Sender in the past, the Message Receiver is not engaged in a current sale or transaction with the Message Sender and does not owe and has not otherwise agreed to pay the Message Sender.	
The Message Sender is an entity that provides digital wallets (prepaid accounts) for consumers. As a means of soliciting a payment to fund a new digital wallet, the Message Sender sends an RFP to a consumer that is not an existing customer and has not agreed to fund a new wallet. Because the consumer is not an existing customer and has not agreed to fund a new wallet, the warranty is breached regardless of the specific facts that led to the RFP. For example, the RFP may have resulted from a Message Sender's error or because of a digital wallet that was fraudulently established in the consumer's name.	This scenario would also violate the Permissible Use requirement. It is not a permissible account to account transaction because the Message Sender does not hold an asset account for the Message Receiver and did not send the RFP at the Message Receiver's direction. It is not a permissible consumer down payment because a digital wallet (prepaid account) is not a deposit account.
The Message Sender provides a recurring service to a consumer and sends an RFP to the consumer indicating it is for an amount owed to the Message Sender when in fact the consumer does not owe the payment to the RFP Sender. For example, the RFP may request payment for one time fees for optional services that the consumer did not purchase.	
The Message Sender sends an RFP for an amount that is more than the Message Receiver owes (e.g., the RFP	Where an RFP requests an amount that is greater than the Message Receiver owes, for purposes of the requirement to return

[4] RTP Op. Rule VII.B.3.

Receiver owes the Message Sender a $2,000 final payment but receives an RFP for $3,000).	funds under RTP Operating Rules VII.D.6.d.i and VII.D.7.d.i, only the amount of the Responding Payment that exceeded the amount owed must be returned to the Message Receiving Participant.

2. Legitimate Purpose (Consumer Message Sender)

Explanation. This component of the warranty is breached when a Consumer Message Sender sends an RFP to request payment from a Message Receiver who (i) is not known to the Message Sender and (ii) would not reasonably expect to receive the Request for Payment from the Message Sender.[5]

Scenario that Breaches Warranty	Additional Comments
The Message Sender is a fraudster that has established a new digital wallet (prepaid account) in a consumer's name. As a means of soliciting a payment to fund the new digital wallet, the fraudster sends an RFP to the consumer.	This scenario would also violate the Permissible Use requirement. It is not a permissible account to account transaction because the Message Sender and Message Receiver are not the same person and the payment sent in response to the RFP did not result in a transfer between asset accounts that are both owned by the same Person.

3. Part of a Fraudulent Scheme to Induce a Payment

Explanation. This component of the warranty is breached when a Message Sender engaged in wrongful or criminal deception to induce an accountholder to make a payment uses an RFP to solicit such payment. Factors that may be relevant to determining whether this component of the RFP warranty has been breached include, but are not limited to, the materiality of the alleged deception, whether the Message Sender is a legitimate business, whether the Message Sender impersonated another person or misrepresented the purpose of the requested payment, and whether the Message Receiver filed a police report relating to the RFP/Payment at issue.[6] A legitimate business means a Person that in fact sells the goods or services that an RFP purports to collect payment for.[7]

The RFP warranty was not designed to provide "purchase protection" type coverage for disputes between consumers and merchants about the quality or delivery of goods and services. Absent wrongful or criminal deception by the Message Sender to induce a payment, disputes regarding the quality or

[5] *Id.*

[6] A police report is not a pre-requisite to initiating a claim that an RFP is part of a fraudulent scheme to induce a payment, but may serve as evidence of such a scheme.

[7] Whether a Message Sender is a legitimate business is one factor relevant to determining whether this component of the RFP warranty is breached, but is not in itself conclusive as legitimate businesses may also engage in fraudulent activity.

delivery of goods and services do not give rise to a valid breach of warranty claim under this component of the warranty.

Message Receiving Participants should be aware that where an RFP warranty claim involves a dispute about the quality or delivery of such goods/services as determined by TCH, the Message Receiving Participant has the burden of evidencing the facts necessary to support the RFP Warranty claim if the claim proceeds to arbitration under RTP Op. Rule VII.D.7.

Examples of scenarios that would not give rise to a breach of this warranty component include complaints about a legitimate merchant where goods were not delivered due to the merchant's error, or goods were received but are different from what the Message Receiver expected.

Scenario that Breaches Warranty	Additional Comments
A Message Sender that claims to run a computer repair business but does not actually have such a business offers a computer repair service to a business. The Message Sender claims the business needs antivirus software that it has no intention to provide. The Message Sender sends an RFP for a payment for the repair service. The business makes the Payment and the Message Sender does not provide the repair service.	This scenario would also violate the Permissible Use requirement. It is not a permissible Business to Business transaction because the RFP does not have a business purpose.
A fraudster calls a grandparent alleging to be a friend of consumer's grandchild. The fraudster claims the grandchild has been arrested and will remain in jail for the weekend if consumer doesn't send bail money in response to an RFP. The fraudster sends the RFP and the Message Receiver (grandparent) responds with a Payment.	This scenario would also violate the Permissible Use requirement. It is not a permissible account to account transaction because the Message Sender and Message Receiver are not the same person and the payment sent in response to the RFP did not result in a transfer between asset accounts that are both owned by the same Person.
A fraudster sends a consumer a fake text message "fraud alert" purporting to be from their bank, followed by a phone call from the fraudster that shows the bank's name in caller ID. The fraudster tells the consumer that the bank has detected fraudulent activity in their account and the consumer must make a payment to their own account to "stop the fraud." The fraudster (Message Sender) sends an RFP and the consumer makes a Payment in response, which transfers funds to the fraudster.	This scenario would also violate the Permissible Use requirement. It is not a permissible account to account transaction because the Message Sender and Message Receiver are not the same person and the payment sent in response to the RFP did not result in a transfer between asset accounts that are both owned by the same Person.
A Message Sender claims to offer a recurring consumer service that the Message Sender does not actually offer. The Message Sender sends an RFP to collect payment for the purported service. The accountholder makes a	This scenario would also violate the Permissible Use requirement. It is not a permissible Consumer Bill Pay transaction because the Message Sender does not offer a recurring consumer service.

Payment in response to the RFP and the Message Sender does not provide the service.	
A consumer is purchasing a home. A Message Sender impersonates a representative from the consumer's title company, contacts the consumer, and instructs her to make the down payment for the home in response to an RFP that will be sent. The RFP results in a Payment to the Message Sender's account and not to the title company's account.	This scenario would also violate the Permissible Use requirement because the Message Sender is a fraudster and is not using an RFP for an initial payment for a financial obligation that will involve multiple payments.[8]

4. Harassing

Explanation. The warranty is breached when a Message Sender (i) uses language in a Request for Payment Message that could reasonably be perceived by the Message Receiver as threatening or intimidating ("Type 1 Harassment"); or (ii) originates repeated Requests for Payment to the Message Receiver within a timeframe that could be reasonably perceived by that Customer as harassing ("Type 2 Harassment").

For purposes of Type 1 Harassment, whether language could reasonably be perceived as threatening or intimidating will depend on the facts and circumstances.

Similarly, for purposes of Type 2 Harassment, whether repeated RFPs are considered harassing will generally depend on the facts and circumstances. The following do not constitute Type 2 Harassment:

- Sending a single reminder RFP to a customer who previously received an RFP for a required payment but has not made that required payment.

- Sending an RFP for a different payment following a permissible reminder RFP for a required payment as described above.

It is important to note that a breach of the "harassing" component of the RFP warranty and recovery under the RFP warranty claims process in RTP Operating Rule VII.D. does not excuse the Message Receiver from paying an underlying debt that they owe or a payment they have agreed to make to a Message Sender. Rather, where there is a breach of the harassing component of the RFP warranty and a successful breach of warranty claim, the Message Sender has effectively forfeited the ability to receive payment from a harassing RFP. Prior to bringing a claim that the harassing component of the warranty was breached, Message Receiving Participants are encouraged to inform their Message Receiver customers that if the Message Receiving Participant recovers and reimburses the customer, this does not excuse any valid payment obligation that may exist between the customer and the Message Sender. The customer may need to make another payment to satisfy their obligation to the Message Sender (e.g., by using an alternative payment channel or making an RTP Payment in response to a subsequent non-breaching RFP sent by the Message Sender).

[8] Had the Message Sender actually been the consumer's title company, this scenario would not violate the Permissible Use requirement.

Scenario that Breaches Warranty	Additional Comments
A Message Sender includes language in an RFP that threatens physical harm to a business owner if the RFP is not paid.	This is an example of Type 1 Harassment.
A Message Sender includes language in an RFP to a Message Receiver wrongly stating that the Message Receiver may go to jail if she does not make a payment for a payment owed to the RFP Sender.	This is an example of Type 1 Harassment.
A Message Sender (landlord) includes language in an RFP for a final rent payment stating that the landlord will damage the Message Receiver's personal property if the payment is not made.	This is an example of Type 1 Harassment.
A Message Sender sends multiple RFPs to the same Message Receiver within a short period of time. For example, a consumer has a subscription service that is paid for once a month. Two weeks before the payment is due, the Message Sender begins sending an RFP everyday for the month's payment.	This is an example of Type 2 Harassment.
A fraudster sends multiple unwanted RFPs to the same Message Receiver within a short period of time.	This is an example of Type 2 Harassment.

5. Otherwise Unlawful

Explanation. The use of an RFP in a manner that violates an applicable law or regulation.

Scenario that Breaches Warranty	Additional Comments
A Message Sender sends RFPs in a manner that violate the FDCPA's prohibition on abusive, unfair or deceptive practices to collect consumer debts.	
A Message Sender uses an RFP to collect payment for fees for an installment loan that is illegal under state consumer lending laws.	

6. Other Topics.

The RFP warranty does not address whether a Responding Payment is authorized. Thus, the warranty does not create a mechanism for a Message Receiving Participant to recover from a Message Sending Participant for an unauthorized RTP Payment, except to the extent the RFP Warranty was breached. For example, if an RFP does not breach the warranty and the Message Receiver's account is accessed without authorization and an unauthorized payment is sent in response to an RFP, the Message Receiving Participant cannot recover under the warranty.

However, if an RFP is not for a legitimate purpose or otherwise breaches the RFP warranty and the Message Receiver's account is accessed without authorization and an unauthorized payment is sent in response to the RFP, the Message Receiving Participant may recover under the warranty for the breach.