Thwarting Faster Payment Fraud

payments fraud protection RTP

Summary: Faster payments are growing in popularity, but so is the opportunity for thieves. What your institution can do to stay safe.

Early last year, a story surfaced of a trio of thieves that entered a video camera store outside of Detroit. The problem was the store had cameras inside and out running pretty much 24x7. When the employees weren't looking, these thieves stole a charger, which was all caught on camera. Needless to say, they were also caught. Clearly, some thieves are pretty stupid, while others aren't. Faster payments could potentially provide more opportunity for thieves, so community financial institutions (CFIs) need to be on the lookout.

Faster payments are growing in popularity among US consumers and financial institutions. To put things in perspective, nearly 600 US financial institutions have contracted thus far to offer Zelle, and more than 100mm consumers have access to Zelle in their mobile banking app, according to an October report from Aite Group. As faster or even real-time payments offerings proliferate and customer demand increases, it's incumbent upon CFIs to put practices in place to also minimize fraud losses.

Before offering faster payments of any type, CFIs first need to ensure they have sufficient controls in place. This includes quicker fraud detection and interdiction capabilities.

For those unaware, interdiction capability allows for a transaction to be set aside for a given period of time of minutes or even hours. This allows a human to review the transaction and then decide whether to allow it to proceed or not. Alternatively, transaction decisions can be set to send or decline. This removes the need for interdiction capabilities, but could result in negative customer impacts.

CFIs should also focus on strengthening account takeover controls and beefing up fraud control practices. There are also real-time fraud analytic providers that you may want to consider engaging, if you ramp up faster payments.

In addition to these and other rigorous fraud prevention tools, any institution's faster payments systems should consider additional easy-to-execute weapons that can be used to fight fraud. For instance, you might institute low transaction limits for new customers and increase the limits over time. Another idea is to establish lower thresholds when customers send money to a new payee.

Authentication of new payees is also crucial, of course. Absent a strong approach, fraudsters can more readily gain access to a customer's account and cause unauthorized transfers. If possible, CFIs should try to find the length of time the payee's email address or phone number has existed to help evaluate payee risk. Consumer education is also critical since payments systems are not like a credit card, so they don't offer zero-liability protection. Many customers may not be aware of this distinction.

Importantly, fraud concerns shouldn't be a show-stopper when it comes to offering faster payments. Payment systems aren't fraud-proof, but by putting into place essential risk controls and taking the proper precautions, CFIs can contain the fraud threat to an appropriate level for their risk tolerance.

If you have questions about this, let us know.

WEBINAR: GENERATING UPFRONT FEE INCOME THROUGH HEDGING

Join us on Feb 13 at 11:30 a.m. PT as we explore how to generate upfront fee income through hedging. See examples, and hear from 5Star Banks Market President on how this tool is benefiting his institution. REGISTER

Copyright 2021 PCBB. Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.