Allied Solutions

Allied INSIGHTS

Fraud & Security RISK ALERTS

Timely insights to protect against fraud and mitigate risks

# Digital (Mobile) Wallet Fraud Risk

## SUMMARY

Accountholders are being victimized by digital (mobile) wallet fraud in both card-present - using their mobile device – and card-not-present - Apple Pay, Samsung Pay or Google Pay – online environments.

Digital wallet fraud refers to unauthorized activities that exploit digital wallets for illicit transactions, such as using stolen credit or debit card information or creating fake wallets to deceive users into disclosing payment details.

## HOW THE FRAUD IS PERPETRATED

**Steps of digital wallet fraud:**

1. Bad actors phishes an accountholder, pretending to be your financial institution, with the goal of convincing the accountholder to give them their credit/debit card information to enroll in a digital wallet.
2. The bad actor will then use this information to obtain a token provisioned to a device in their possession.
3. Once provisioned, the bad actor will use it with various merchants, usually purchasing gift cards.

## BEST PRACTICES TO COMBAT DIGITAL WALLET FRAUD

It's crucial to validate cardholder requirements before provisioning a token to a device. For existing cardholders with previously provisioned tokens, additional controls should be in place for any new token requests. Ideally, you should verify the device ID to ensure it belongs to the cardholder.

- Educate your membership to NEVER give out any of their card information to a caller, text message, email or in a chat. Since they already have it, the credit union will NEVER ask for the members' card information.
- If you are experiencing digital wallet fraud, consider running a compromised point of purchase analysis to determine a potential point of compromise for the impacted card to determine where the cardholders' cards may have been compromised prior to the fraud.

- Implement controls that look at transaction level activity.
- Understand digital wallet fraud starts with the enrollment. Confirm your enrollment criteria along with the rules that are in place. If the enrollment and rules are weak, the bad actors will infiltrate and execute digital payments.
- It's Allied's understanding that at least 50% of the fraud takes place on day one or within the 1st week of enrollment into a digital wallet; therefore, fraud prevention credentials need to be in the digital wallet on day one and kept in place.
- Validate and confirm the provisions for enrollment into a digital wallet. Are you using the green path or should you investigate the yellow or red path?
- Confirm how the token receives provision. This is critical.
- When the token receives provision, are you including a dynamic CVV2/CVC2/CID? (3-digit code on the back of the card).
- Validate and confirm the enrollment criteria used along with the rules in place for your digital wallet program.
- Validate and confirm what type of digital wallet and digital transaction fraud you are seeing. Is it card-present or card-not-present?
- Confirm what fraud prevention tools are in place for your digital wallet and digital transaction for both a card-present and card-not-present risk.
- It is key to confirm rules are in place PRIOR to the 1st digital transaction.
- Validate and confirm you have cryptogram in place prior to rolling out the digital wallet service.
- Educate your cardholders to understand the pop-up and to READ it before the landing page.
- Watch for digital wallet card-present contactless authorization code POS 07.
- Watch for digital wallet card-not-present contactless authorizations code POS 10.
- Be aware of a rogue app software tricking the terminal in a card-present digital transaction to a "force post". These transactions are NOT authorized. You can charge these unauthorized items back to the acquirer.
- Reconfirm that 100% of your digital transactions are part of your fraud monitoring system on day one.
- Validate if the fraud monitoring notes transactions out of the cardholder spend pattern.
- Be aware that transaction amounts indicate potential gift card purchases (e.g. even dollar amount plus a service charge where there are no pennies in the transaction amount).
- Validate the fraud monitoring alerts on spending that is out of pattern (e.g. high dollar) and continues for more than one day.
- Confirm you provide ongoing member education on digital wallet and digital transactions.

## RISK MITIGATION RESOURCES

- Article: Digital Wallet Fraud – What it is and how it's prevented
- Visit Allied's Fraud & Risk Education Library



LinkedIn