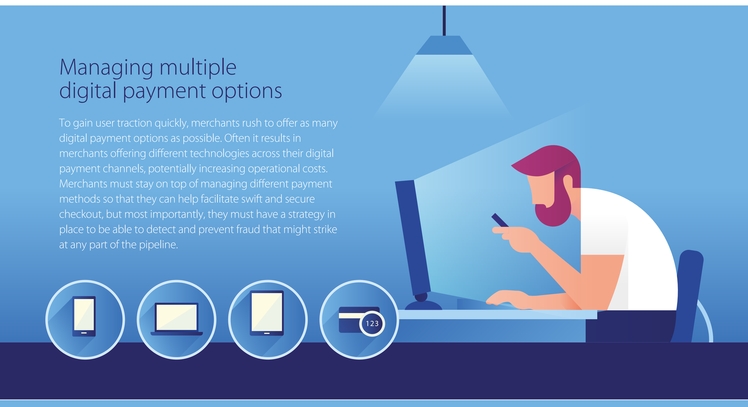
Challenges Faced by Digital Goods Merchants

Let's look at some challenges that digital goods merchants face when dealing with payments and fraud and some tips on how to control fraud decisions.

Managing multiple digital payment options

To gain user traction quickly, merchants rush to offer as many digital payment options as possible. Often it results in merchants offering different technologies across their digital payment channels, potentially increasing operational costs. Merchants must stay on top of managing different payment methods so that they can help facilitate swift and secure checkout, but most importantly, they must have a strategy in place to be able to detect and prevent fraud that might strike at any part of the pipeline.



Little window to review for fraud

Immediate payment acceptance and delivery are increasingly the default standard for digital products and services. The waiting time for order approval may cause some customers to drop out midway through the ordering process. A reliable and automated fraud detection system is crucial to gain accurate decisions regarding good and bad customers. A combination of rules and machine learning can act as a set of guardrails to provide digital goods merchants control over fraud decisions.

High volume, low value of orders

Since the incremental unit production cost for digital goods are minimal, digital merchants have a strong urge to sell more volume to maintain higher profit margins. In addition, checkout simplicity for mobile-based transactions, while provides reducing checkout friction for genuine customers, also works in opposite tension to security, and fraudsters can exploit it for their own agenda. It is important to have a balance between order acceptance and fraud controls.

Fewer data points for identity verification

Massive data breaches and phishing scams make it easier for fraudsters to obtain consumer information. Selling digital goods often means merchants have to contend with having fewer key data sources, making it even harder to verify a customer's identity. Data feeds related to payment channel, user behavior and activity—such as device type, operating system, transaction velocity, or behavior across sales channels—are key to combatting digital goods fraud because they can provide merchants insights to uncover transaction patterns and purchase behaviors that may differ across channels or payment types.

Odds of chargebacks and false positives

Merchants often incur greater operational and opportunity cost given the time and effort taken to address chargebacks for near instant order delivery. On the flip side, merchants also have to contend with false positives, that is, when they reject a genuine customer order by mistake. Genuine customers whose orders were rejected might move on to another merchant, so that rejection might be enough to lose a customer's lifetime value. A suitable fraud management strategy for digital goods requires a balance of speed and accuracy.

Digital currency, particularly in online games

In-game currency is a popular fraud target. In a practice known as gold farming, online game credits are acquired and accumulated by fraudsters or their accomplices through gameplay and later sold for real cash. Although gold farming has dropped in popularity over the years and online gaming companies are implementing transaction systems that discourage such activities, gaming accounts with in-game currencies should monitor for account takeover of customer payment information.

Source: IDC, "New IDC Research Program to Explore Consumer Spending on Digital Devices, Services and Content", Jan 2017. https://www.idc.com/getdoc.jsp?containerId=prUS42205216