Out of Sight, Out of Mind: The Problem with Digital Goods and Services

What are digital goods and services? Essentially, they're things you buy in the digital world that don't arrive in the mail – online subscriptions, games, e-books, music, streaming services and the like. More and more of the goods and services we buy are digital; volume has increased by almost 70% over the last two years because of the explosion in electronic devices and the speed and ease of the payment process. It's good news for consumers – they've come to expect instant approval and receipt of goods. Unfortunately, it's good news for fraudsters, too. Transactions often face fewer controls, the sums are small and easily overlooked, geography is irrelevant and criminals don't have to run the risk of stealing and storing physical goods.

Digital goods transactions are also more susceptible to friendly fraud, which occurs when the cardholder or their family/friend knows about the transaction but reports it as unauthorized to their issuing bank. Sometimes cardholders genuinely fail to recognise the charge on their statement, or may take the view that charging back digital purchases is okay because there is no real loss of property to the merchant. Fraud rates on digital goods have stayed consistently above the global card-not-present average.

There are other factors that need to be addressed. First, many issuer and merchant fraud monitoring tools have not yet successfully evolved to identify and mitigate fraud on digital goods. Second, some issuers take a risk-based approach that subjects lower value transactions to lower scrutiny. Third, chargeback is becoming more accessible to consumers who do not recognise (or, in some cases, do not want to pay for) a particular good; fraud chargeback rates on digital goods are significantly higher than non-digital e-commerce. It is often much easier for the cardholder to get their money back by declaring the transaction was unauthorized and charging it back through their bank than it is to contact the merchant and discuss a possible refund.

So, what's the answer? Merchants can increase the intelligence of their transaction monitoring, while also enhancing security on customer accounts. Many merchants selling digital goods will encourage customers to create an account and store their card details, making much more money from repeat or subscribed buyers than one-time purchasers. Should any of these customer accounts be compromised, the underlying card details may be available for use, so security and monitoring is crucial at the customer account level. Issuers should be aware of the differences between traditional e-commerce fraud and digital e-commerce fraud and adapt their real-time decisioning strategies accordingly. While often the e-commerce merchant suffers the liability and losses from fraudulent activity, issuers are limited by the number of fraud chargebacks allowed on any one card, and therefore suffer the loss of fraud transactions that exceed that limit. This accounts for approximately 20% of digital goods fraud, which is not insignificant. In addition, low value transactions often present the issuer with a dilemma: Is charging back financially viable, given the estimated cost for the issuer for one chargeback can be up to $50? This has further consequences for fraud identification and mitigation, as merchants may be unaware of fraudulent transactions that are not charged back, so cannot incorporate them into their fraud prevention strategies.

The digital goods and services marketplace is continually growing, and susceptibility to fraud and cyberattacks will increase if merchants and issuers fail to adapt their fraud risk strategies to address the changing environment. That means being proactive with intelligent decisioning that stays one step ahead of the fraudsters. Multi-layered intelligence and up-to-date risk monitoring tools are vital to identify signs of friendly fraud. Continuing education for frontline staff to adapt to non-traditional transaction types and fraud techniques will help issuers and merchants lessen their exposure and reduce their losses. Mastercard is committed to providing advice and educational content in this field, and we are encouraging collaboration between issuers and merchants. Mastercard is also prioritizing analysis and identification of friendly fraud in the digital space with the intent of sharing insights with issuers and merchants to reduce fraudulent activity on digital goods.