Kount®

eBook

FRAUD IN A DIGITAL WORLD

Trends and Best Practices for Digital Goods Merchants

Fraudsters have increased attacks to exploit the unique vulnerabilities inherent in selling digital products. Discover the latest insights and top strategies for beating fraud, reducing mitigation costs, and increasing sales in the digital goods world.

Digital Services and Downloads 101

Electrons versus atoms. Virtually any product that can be sold in stores can now be sold online. Similarly, a huge number of products that can be sold as physical goods (books, magazines, games, movies, etc.) can now also be sold as digital products—either as services or downloads. The benefits of selling digital goods has fueled strong growth in this market segment:

- Immediacy. Instantaneous fulfillment leading to increased likelihood of impulse purchases is a key benefit.
- Cost Savings. Digital products often enjoy lower operational, production, and fulfillment costs compared to physical goods, resulting in lower prices for buyers (e.g., Kindle books cost less to produce and deliver than hardcover or paperback versions).
- Convenience. Apps offering digital goods often make purchase and fulfillment almost effortless (e.g., adding a song to your iPhone from iTunes requires just one click).
- Global Market. Digital products are not impacted by the shipping, logistics, time-zone, or import/export challenges associated with physical goods.
- Automated/Continuous Delivery. Digital goods can be fulfilled 24/7 via automated systems for “always open” availability.

Massive Sales Growth of Digital Products

Huge and growing. The digital goods market has been booming over the past few years and double digit growth is projected for the foreseeable future in every segment:

- **Music and Video.** In 2016, digital orders accounted for half of all music sales and streaming revenue grew by 60.4%[1]. Streaming video subscription revenue is projected to grow to $10.36 billion by 2020[2].
- **Cloud-Based Applications.** By the end of 2017, public cloud services will have grown 18% to $246.8 billion[3].
- **eLearning.** The eLearning market is projected to soar to approximately $325 billion by 2025[4].
- **eGift Cards.** Digital gift card sales are growing at a 40% annual rate[5] and will reach a projected $15 billion in 2017[6].
- **Mobile Apps.** There were more than 90 billion app store downloads worldwide in 2016[7] and global mobile app revenue for 2017 is projected to hit $77 billion, up 120% since 2014[8].

Video Streaming/Download Services
Music Streaming/Download Services
Internet Television
Online Games/Gaming
eBooks
eGift Cards
eLearning/Online Courses
Digital Subscriptions
Mobile Apps
Cloud-based Applications (SaaS)
Downloadable Software
Electronic Tickets (Concerts,
Sports, Events, Etc.)
Photos/Graphics
Fonts

Factors Impacting Fraud In Digital Products

Digital goods present different fraud mitigation challenges.
The unique aspects of selling and fulfilling digital goods create inherently greater fraud risks:

- Expectation of Immediate Fulfillment
- Less Data Available for Fraud Screening
- Higher Incidence of Mobile Transactions
- Balancing User Experience with Risk

Expectation of Immediate Fulfillment

No time to catch your breath. While sellers of physical goods may have minutes or even hours before deciding to ship/not ship, digital goods merchants must decide in real-time to fulfill/not fulfill. Fraudsters exploit this highly-condensed decisioning window to improve their chances of escaping detection.

False positives. Sellers of digital products don’t want to lose sales, and so tend to approve borderline transactions. After all, tightening fraud rules too much means higher false positives, forfeited revenue, and potential loss of customers. Conversely, not screening prudently enough leads to increased chargebacks, higher fines and fees, and even loss of merchant account privileges.

Susceptibility to automated fraud. Sophisticated criminal gangs employing bots, automated tools, and mobile wallets can rapidly place hundreds of orders. Before fraud activity is detected, a seller may lose thousands of dollars in stolen digital goods and be exposed to even further losses due to chargeback fines and penalties.

No manual review. Sellers of physical goods often have time to investigate borderline or suspicious transactions via manual reviews. Many sellers of digital goods don’t have this luxury, leading to greater ambiguity and higher risk.

Less Data Available for Fraud Screening

Less data, more risk. Data is a fraud prevention analyst's best friend. But with digital goods, orders often have fewer data points to inform a prudent fulfill/no fulfill decision.

Limited transactional data. eCommerce buyers placing orders for physical goods typically must provide a delivery address. This information can be incorporated into risk scoring that applies additional screening factors like geo-location, IP address, etc. But digital goods almost never require a physical delivery address. Fraudsters capitalize on this to make fraud attacks harder to detect.

Siloed information. Payment and fraud teams in digital product companies are frequently siloed. Because fraud against digital products can happen so swiftly, slow or inefficient communication can lead to extended windows of fraud vulnerability.

Higher Incidence of Mobile Transactions

Mobile goods, mobile challenges. Mobile commerce is exploding, increasing its share of overall eCommerce volume[9]. This sales growth is even more pronounced in the digital goods industry, with many digital products intended specifically for mobile devices (mobile apps, music downloads, electronic tickets, etc.):

- U.S. mobile commerce sales are projected to soar nearly 260% to $284 billion by 2020[10].

Unfortunately, increased mobile commerce can also mean increased fraud:

- Successful fraud transactions in the mobile channel jumped from 26% to 35%[10].
- Mobile orders for gift cards are more likely to be fraudulent than desktop orders[11].
- Mobile wallets and emerging mobile payment systems can dramatically accelerate the speed of fraud attacks.

Balancing User Experience with Risk

To buy or not to buy, that is the challenge. Fraud prevention systems that introduce friction into transactions for digital goods can severely impact sales:

- A page delay of just 1 second could potentially lose $2.5 million a year for an eCommerce site with $100,000 in daily sales[12].
- Radware study found that a 2-second delay in load time resulted in abandonment rates of up to 87%[13].

Conversely, faster page response increases sales:

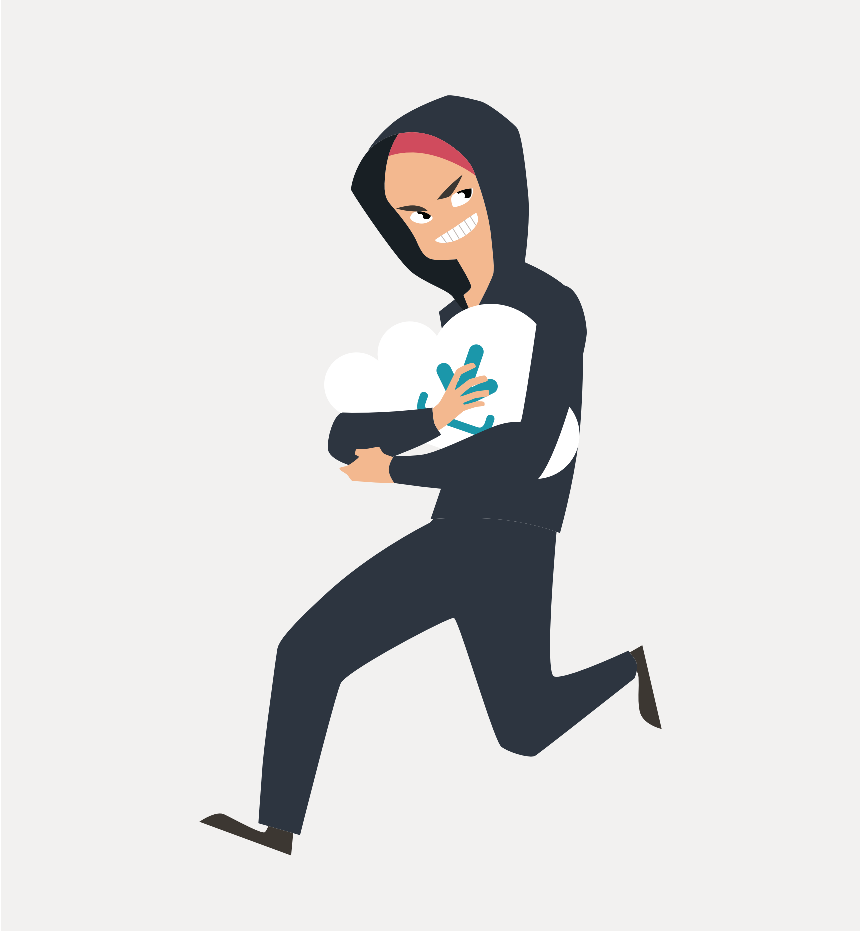
- Walmart saw a 2% increase in conversions for every second of improvement in load time[14].
- Fanatics (a sports apparel company) shaved 2 seconds off median page load time and almost doubled conversions[14].
- Every 100 millisecond improvement can result in a 1% increase in revenue[14].

Types of Fraud That Target Digital Products

Widespread fraud attacks against digital goods merchants. Sellers of digital goods get hit with the same fraud tactics and techniques used against all eCommerce operations.

One major difference, however, is that the stolen digital goods don't have to be stored in a warehouse or physically delivered to some unsuspecting buyer. Instead, millions of dollars in stolen property can be stored digitally and resold quickly on legitimate or illegal secondary marketplaces. This rapid monetization of stolen digital goods is a primary reason why they are so attractive to fraudsters. Because of this and other factors, the types of fraud listed below are the most prevalent and/or damaging for digital goods merchants:

- Friendly Fraud and Payment Fraud
- Mobile & Mobile App Fraud
- eGift Cards
- Account Takeover (ATO) and Account Sharing
- Card Testing



Friendly Fraud and Payment Fraud

No such thing as friendly fraud. The name comes from "friendly fire" because chargebacks harm the consumer's supposed "allies" (issuer, acquirer and/or merchant). Friendly fraud can be either innocent or malicious:

- **Consumer error.** Consumers may honestly not recognize charges on their bill. For example, a teen that makes a purchase in an app without a parent's knowledge. Or the charge appears under a holding company name instead of the product name the cardholder knows.
- **Buyer's remorse/expired refund period.** Consumers file chargebacks instead of requesting refunds or exchanges through proper channels.
- **Card-not-present (CNP) fraud.** Fraudsters use stolen credit card accounts to fraudulently obtain digital goods and account access. They then quickly turn these into cash by reselling the downloaded files or accounts on both legitimate and illegal online marketplaces. CNP fraud skyrocketed 40% in 2016[15] and is projected to cost online businesses $7.2 billion in fraud losses by 2020.[16]

Mobile & Mobile App Fraud

Mobile attacks against digital goods merchants. With so many digital goods intended specifically for use or consumption on mobile devices, the confluence of mobile commerce and higher mobile fraud rates presents significant challenges for sellers in digital goods:

- 60% of overall fraud originates on mobile[17].
- The fraud rate from mobile commerce is twice as high as conventional eCommerce, according to The Fraud Practice[18].
- $2.33 in costs for every $1 in fraudulent mobile transactions, according to the estimated “true cost” of mobile fraud published by LexisNexis[19].

Unfortunately, even in the face of this clear and costly trend of higher mobile fraud, many digital goods merchants are merely “bolting on” standalone or ad hoc mobile antifraud tools to risk management systems originally intended for desktop transactions. The result can be exposure to increased levels of mobile fraud.

True Cost
$2.33
Fraud
$1.00

eGift Cards

Fast, easy money. An estimated $950 million will be lost to eGift card fraud this year[20]. And because 8 out of 10 of the top internet retailers offer digital eGift cards[5], this fraud loss extends far beyond digital-goods-only sellers to impact almost all of the eCommerce world. The exposure is significant. For example, 3 out of 4 consumers say they'll purchase an average of two to three eGift cards and gift cards this coming holiday season:

- eGift cards had the highest fraud attack rates of all products sold between Black Friday and Christmas last year[5].
- Nearly 1 out of every 10 fraud attempts over the holiday season will target eGift cards[21].

Here's why: using multiple synthetic ID's and stolen credit card accounts that are cheaply available on the Dark Web, a single fraudster can fraudulently obtain hundreds of eGift cards in just hours without arousing suspicion (e.g., $100 eGift card amounts won't raise alarms during the holiday season).

The fraudster can then resell these eGift cards on secondary eGift card resale marketplaces for as much as 80 cents on the dollar, pocketing tens of thousands of dollars in cash in just a few hours.

Account Takeover (ATO) and Identity Theft

Lucrative target. Fraudsters hacking or stealing consumer credentials to take over digital goods accounts is becoming increasingly prevalent. It is especially lucrative if autoload is enabled on an account, enabling repeated purchases until the customer's account is completely drained.

- ATO increased 31% and malicious account creation—where fraudsters use stolen or synthetic identities to open fake accounts in innocent consumers' names—increased 20% in 2016[22].
- Tools make account takeover even easier for fraudsters, combining multiple sources of stolen data to find accounts that can be hacked.

Once comprised, accounts can be used by a fraudster or sold on the Dark web. The account types most at risk include:

- Online game and gaming accounts
- Streaming accounts
- Mobile app and software accounts
- Subscriptions

Account Sharing. More than 1 in 5 adults borrow streaming video passwords[23]. This can make it a difficult task to differentiate an account that has been shared from one that has been taken over.

Card Testing

Small-ticket transactions are a big target. Low-value transactions are common for sellers of digital products and so are less likely to arouse suspicion. Fraudsters know this and specifically target digital goods for card testing (also known as "carding") so they can retain the maximum amount of credit for a future "big score" while confirming that the stolen account is working.

With bots and automated tools available to fraudsters for card testing, a digital goods merchant can quickly be hit with thousands of card tests before becoming aware of the problem.

TC-40. TC-40's are the claims that get filed every time a cardholder reports their card has been used fraudulently. These claims are reported to card brands and issuers. However, many issuers won't process chargebacks for TC-40 claims below a certain amount (e.g., $20) because the chargeback fee will cost more than covering their loss on the transaction. With no chargebacks to alert them that TC-40 claims are piling up due to card testing, digital products merchants may suddenly get blind sided with a notice from their processor that they are being fined. Or that the processor will stop processing transactions. Or worse, customers start complaining that their credit cards are being declined for no apparent reason.

Costs of Fraud for Digital Products Merchants

The other 3 legs of a 4-legged stool. Losses are just one aspect of fraud. Digital goods merchants also need to factor in fraud mitigation expenses, revenue loss from false positives, and brand reputation to ensure they're achieving maximum ROI.

Fraud Mitigation Expense. Digital goods merchants spend an average of $10.1 million per year[24], which is nearly 43% higher than physical goods merchants[24]. This may be due to digital goods merchants employing nearly five times more fraud mitigation personnel than physical goods merchants[25].

Revenue Loss. A Javelin study found that at least 15% of all cardholders have had at least one transaction incorrectly declined[26]. Based on this data, it's obvious that merchants—including digital goods merchants—are turning down too many good orders. That's immediate revenue loss and the potential loss of significant customer lifetime revenue, too.

Brand Reputation. When consumers are able to purchase stolen digital goods at lower prices on secondary markets, it hurts brand reputation. And if merchants suspend sales of certain products due to fraud attacks, that can further harm consumer retention and potentially market share.

12 Best Practices to Fight Digital Products Fraud

1

Multiple, advanced screening technologies. A single tool can be easily defeated. The more technologies used and the more data analyzed, the more obstacles fraudsters have to overcome.

2

Multiple stages. Put checks in place throughout the buying path—before authorization (e.g., velocity checks), at authorization (e.g., risk scoring), and post-authorization (e.g., Chargeback Alerts).

3

Chargeback alerts. Electronic notification services warn you immediately whenever a TC-40 claim is filed.

4

Require account registration. The data entry required for account creation slows down fraudsters and creates additional friction, causing them to abandon your site.

12 Best Practices to Fight Digital Products Fraud

5

Two-factor authentication. Require PINs and/or confirmation by SMS text message.

6

Biometrics. Block and/or detect bots by using CAPTCHA and by monitoring navigation cues, time-on-page cues, non-customary behavior and other activity that reveals non-human conduct.

7

All payment types. Make sure your fraud prevention isn't limited by the payment types it can assess. Otherwise, you may find your growth stymied when it's time to enter new channels, markets, or countries.

8

Device and channel neutral. Whether an order originates on desktop, mobile, phone, or fax, make sure the same multi-layered approach and multiple screening technologies get applied—while still providing customization that allows you to optimize results based on the unique attributes of that channel.

12 Best Practices to Fight Digital Products Fraud

9

Standardized policies. Clearly document and publicize policies for customer refunds, chargebacks, and "stolen" digital goods and provide "talking points" to help customer service reps better handle complaints.

10

Real-time data orchestration. When transaction data by itself is insufficient to precisely quantify risk, accessing third-party data sources in real-time can provide crucial context, helping you correctly evaluate borderline transactions.

11

Advanced AI & Machine Learning technology. Artificial Intelligence (AI) and Machine Learning help you go beyond mere detection and prevention. They enable you to take it to the next level: predicting emerging fraud threats in low-information scenarios, such as first-time fraud.

12

Experienced human intelligence. Systems developed and tuned by fraud industry experts have an inherent advantage against adaptable human adversaries. Make sure your fraud system is developed by providers with deep and broad eCommerce antifraud expertise.

Start Beating Fraud and Boosting Sales

Discover how the Kount Complete can reduce chargebacks on digital products transactions, plus lower fraud mitigation costs and boost sales in as little as 60 days.

REQUEST A DEMO

> Chargebacks dropped as soon as we turned on Kount [and] have continued to fall. Our chargeback rate is now 50% lower than it was before Kount.

Brett Goldberg
TickPick

> Our chargeback rate plummeted from 2.6% to less than 0.1%. Kount has really made my life infinitely easier. I'm back to doing my job instead battling fraud.

Christine Barnum
CD Baby

AWARD-WINNING RESULTS

SOURCES:
1 http://www.ifpi.org/downloads/GMR2017.pdf
2 https://www.statista.com/statistics/560395/streaming-video-subscription-revenue/
3 https://www.gartner.com/newsroom/id/3616417
4 http://gulfnews.com/business/sectors/technology/e-learning-set-for-rapid-growth-both-regionally-and-globally-1.2090691
5 https://www.cardcash.com/gift-card-statistics/
6 https://www.giftcardgranny.com/statistics/
7 https://techcrunch.com/2017/01/17/app-downloads-up-15-percent-in-2016-revenue-up-40-percent-thanks-to-china/
8 http://www.business2community.com/mobile-apps/2017-mobile-app-market-statistics-trends-analysis-01750346#FbJoL3feKpYcLX2M.97
9 http://about-fraud.com/infographic-digital-merchants-fraud/
10 http://www.prweb.com/releases/2016/08/prweb13630057.htm
11 https://cardnotpresent.com/cnp-merchants-cannot-attack-fraud-on-mobile-orders-the-same-as-desktop-orders-report/
12 https://blog.kissmetrics.com/loading-time/
13 https://blog.radware.com/applicationdelivery/applicationaccelerationoptimization/2014/01/55-web-performance-stats-youll-want-to-know/
14 https://www.forbes.com/sites/jiawertz/2017/03/17/how-to-compete-for-consumers-online-while-attention-spans-diminish/#4363d6446667
15 http://www.uspaymentsforum.org/wp-content/uploads/2017/03/CNP-Fraud-Around-the-World-WP-FINAL-Mar-2017.pdf
16 https://cardnotpresent.com/report-businesses-to-lose-7-2-billion-to-cnp-fraud-by-2020-may-12-2016/
17 https://www.websitemagazine.com/blog/60-of-overall-fraud-originates-on-mobile-infographic
18 www.thefraudpractice.com
19 https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2016.pdf
20 http://blog.kount.com/blog-against-fraud/6-visible-and-hidden-costs-of-egift-card-fraud
21 http://cardnotpresent.com/fraud-and-e-gift-cards-what-you-can-do-in-november-and-december-to-avoid-a-chargeback-hangover-in-january/
22 https://chargebacks911.com/chargeback-stats-2017
23 https://consumerist.com/2017/07/12/everyone-is-sharing-passwords-and-streaming-services-know-it/
24 https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html
25 https://www.prnewswire.com/news-releases/fraud-related-operational-expenses-top-10-million-for-digital-merchants-300151304.html, plus calculation: digital goods merchants spent 20% of operational budgets on fraud mitigation vs. 14% spent by physical goods merchants
26 https://www.javelinstrategy.com/coverage-area/impact-fraud-and-chargeback-management-operations
27 https://www.merchantriskcouncil.org/resource-center/surveys/2015/2015-mrc-global-fraud-survey
28 https://www.javelinstrategy.com/press-release/false-positive-card-declines-push-consumers- abandon-issuers-and-merchants