

10 Telltale Signs of a Fraudulent Order: How to stop chargebacks before they stop you



There's one imperative question you need to ask about your business: How much are chargebacks really costing us? If you're not comfortable with the answer, it may be time to take another look at your fraud prevention strategy and what may need to change or improve. It's tempting to equate business success with order volume and err on the side of lowering fraud controls to push more orders through. However, this can wreak havoc by increasing chargebacks. Chargebacks, in turn, create higher fees and operational costs, can lead to additional merchandise losses or loss of services and potentially jeopardize a merchant's processing privileges.

For merchants accepting card payments, there are generally two types of chargeback fraud. True fraud occurs with stolen credit card information where a transaction that the cardholder did not authorize is processed. Friendly fraud or "I didn't buy that" fraud is a form of sophisticated shoplifting where a customer attempts to obtain a refund for something he or she actually purchased. In both cases, the owner of the credit card contacts the issuing bank, which then issues a chargeback dispute.

While friendly fraud is a growing problem that costs merchants billions of dollars every year, the leading cause of chargebacks is true fraud – so it's important for merchants to be able to identify potentially fraudulent orders before they go through. It's impossible to perfectly identify every instance of fraud, so it's also important to be able to react effectively and efficiently when fraud occurs, preempting further losses related to the provisioning of goods or services.

Forecasts for Card Not Present ("CNP") Fraud

The major fraud spike that happened three years ago cost merchants \$32 billion.¹ A recent study indicates CNP fraud is expected to only get worse, driven by the closing opportunities for point-of-sale fraud and the growth of e- and m-commerce.²

As fraudsters continue to find new ways to evade and respond to changing detection methods, CNP fraud losses are expected to eclipse \$7 billion by 2020.³



Friendly fraud or "I didn't buy that" fraud is a form of sophisticated shoplifting where a customer attempts to obtain a refund for something he or she actually purchased.

Impacts of Fraud on CNP Merchants

The chargeback dispute resolution process can be convoluted and complex. As many as 86% of cardholders will bypass the merchant and go directly to the Issuer to file a chargeback. In these cases, the merchant doesn't find out about the dispute until after the chargeback is filed, making resolution more complicated – and expensive – than it has to be.

Let's look at an example.

If a merchant sells a product for \$100 at a 22% margin, the net profit after Card Issuer Interchange and Acquirer MDR at 3.5% would be \$18.50:⁴

Total Sale = \$100.00

Margin (22%) = \$22.00

Credit Card Issuer Interchange & Acquirer MDR (3.5%) = \$3.50

Net Profit = Margin – Credit Card Issuer Interchange & Acquirer MDR

If this transaction results in a chargeback, the merchant will lose a total of \$106.50 on this order after issuing a refund and paying chargeback fees. At that rate, the merchant in this example would have to sell almost 5 additional orders at the same amount to recoup that one loss. That's a hefty reminder that there are additional associated costs to chargebacks, including processing the order, handling the chargeback, shipping costs and the cost of goods lost.

Net Profit = \$18.50

Consumer Refund = \$100.00

Chargeback Fee = \$25.00 (note: this is on the low end for fees as many e-commerce merchants pay \$100 or more)⁵

Net Loss to Merchant = Net Profit –
(Consumer Refund + Chargeback Fee)

Additionally, the example doesn't account for other costs including processing fees and overhead, or the possibility of a second chargeback that can occur based on pending billings for recurring merchants.

True fraud heavily impacts merchants too, and the past few years have proven how catastrophic the impact can be. Between the massive data breaches that have pushed stolen card credentials into the marketplace and the shift to EMV, which has pushed fraud to the online channel, cybercriminals have been busy. In 2016, merchants lost 11% more revenue to fraud than in 2015.⁶ And merchants are paying in more ways than just fraud losses – every \$100 in chargebacks REALLY costs merchants \$240 in wasted time, expensive fees, penalties or additional losses of goods and services.⁷



10 Signs of a Fraudulent Order

So what can merchants be on the lookout for to adequately screen for fraudulent orders? Here are 10 signals of a fraudulent transaction:

1. Unusually large orders – whether by number of items or dollar amount of the item(s) being purchased.⁸
2. Rush orders where fraudsters have the element of time to their advantage.⁹
3. Unusual use of international shipping addresses or international cards.¹⁰
4. A sequence of several small transactions occurring over a short time period made with the same or similar card numbers.¹¹
5. Several transactions made with the same card or account number but with separate shipping addresses or vice versa (several transactions made with many different card numbers but with the same shipping address).¹²
6. Several orders placed with different card numbers but from the same IP address (another signal for fraud is several failed transactions as fraudsters may be attempting many different card numbers until they find one that succeeds).¹³
7. A transaction is attempted from an IP address in a high-risk country (Russia, Malaysia, and Ghana) or an IP address whose location does not match either the billing or shipping address.¹⁴ A cloaked IP address is also an indicator of fraud.
8. Use of “spammy” or fake information to place an order, such as obviously fake phone numbers or email addresses (e.g. 555-444-3333 or asdkj321@freemail.com).¹⁵
9. Inconsistencies of customer information across a number of purchases. Any mismatch between billing names, entered phone number, or email addresses should be a red flag. Merchants may see the same email address used for multiple purchases but different phone numbers or names provided in each instance.¹⁶
10. Any transaction that attempts to overcharge the card for more than the transaction amount and then pay out a third party by a different payment type (cash, money order, check, etc.) is likely fraud.¹⁷



What to do in Cases of Fraud

While none of the points above are surefire ways to detect and stop fraud, they are some of the most popular techniques that fraudsters employ. Alone, they may seem innocuous, but the occurrence of several of these together can be a strong indicator of fraudulent activity.

CNP transactions pose additional hurdles to merchants trying to stop fraud since the physical security features of a card cannot be verified and it's not certain that the customer has physical possession of the card. This is why it's important to review suspicious transactions and review orders for anything unusual. Manual review can be burdensome, so velocity controls and other types of behavioral analytics technology can be employed to identify past elements of fraudulent behavior as a basis to predict potential fraudulent activity in the future. However, there are two main downsides. First, while past fraudulent behavior can be a good predictor of similar future fraudulent behavior, this type of technology does not do well identifying different or changing fraudulent behavior in the future.¹⁸ Second, the logic utilized applies to all cards and devices uniformly, increasing the likelihood of false positives and inhibiting legitimate sales from passing through.¹⁹ These false positives depress sales from legitimate customers, lowering profits.

CNP fraud can be trickier due to timing as well. By the time fraudulent patterns are identified, cybercriminals have collected their windfall and are on to the next scheme. This is the inherent risk in static legacy solutions that do not have the agility to keep up with fast-paced fraudsters, especially systems that require significant IT resources for integrations and implementations – which can range from 12-15 months

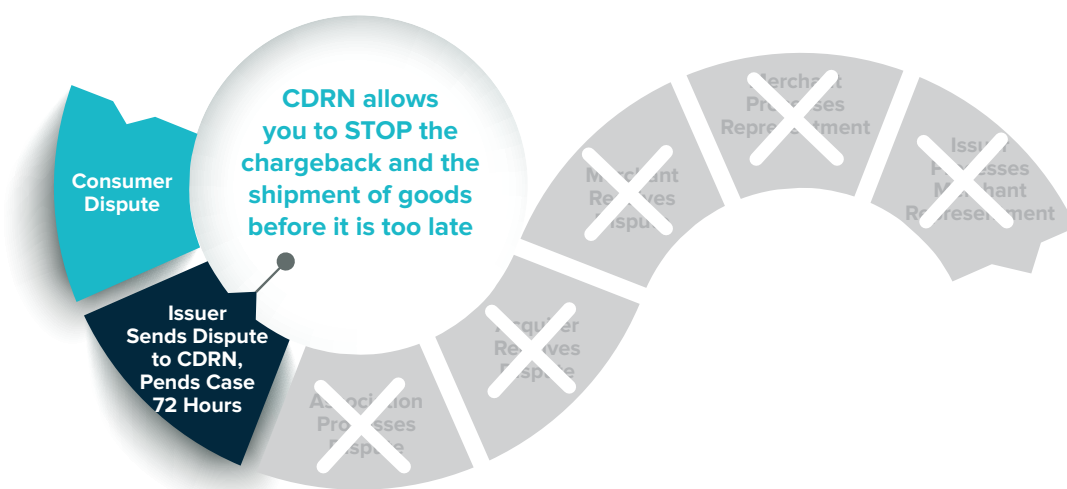
to process. For the investment required to get an average 18% in CNP fraud declines and 5% in CP fraud declines²⁰, these legacy approaches are often not worth the expense.

In order to maximize sales and minimize evolving risks, merchants need a solution that is agile and tackles the weaknesses of these static options without the pains of major IT integrations.

Verifi's Cardholder Dispute Resolution Network™ (CDRN) was founded on the belief that if merchants aren't actively preventing chargebacks, the costs, lost sales and risks add up quickly and ultimately damage the bottom line.

This award-winning, and multi-patented solution helps merchants reduce overly restrictive front-end fraud controls and seamlessly stop chargebacks in real time with minimal IT involvement. CDRN's patented "closed loop" process is directly integrated with card Issuers to redirect disputes from the Issuer to the merchant for proper and prompt resolution with the consumer and without escalating to a chargeback. With the ability to identify both fraud and non fraud ("friendly fraud") chargebacks, CDRN enables the merchant to stop the fulfillment of goods or services, preventing losses due to shipping costs and unrecoverable merchandise.

CDRN PROCESS





CDRN offers unmatched chargeback prevention with the ability to help merchants streamline the chargeback dispute resolution process:

- **Extensive and Growing Partner Network of Top Card Issuers** — Stops up to 50%* of your chargebacks
- **Protect Your Bottom Line** — Avoid costly fees, fines and penalties...and potential loss of your processing privileges
- **Complete Coverage** — Prevents BOTH fraud and non-fraud chargebacks
- **Avoid "False Positives"** — Some solutions create dispute signals that don't turn into actual chargebacks, adding unnecessary costs for protection in addition to money lost to over-refunding on false chargebacks and second chargebacks.
- **Real Time Notifications Stop Losses** — Prevent chargebacks from additional billings and stop losses from fulfillment of goods and services.
- **Improve Staff Allocation** — CDRN takes the burden off your staff so you save time to focus on your business
- **100% Accuracy** — With Verifi's zero-defect guarantee if a CDRN case is successfully resolved but later filed as a chargeback, you don't pay

Conclusion

When merchants get real about the true cost of chargebacks, it's easy to make the business case for a comprehensive, end-to-end chargeback management strategy. It is essential to strike a balance between front-end fraud controls that guard against fraudulent transactions and back-end solutions that promote healthy sales without putting a merchant's operation at risk to suffer losses related to true or friendly fraud. The tell tale signs above are a good foundation to use in preventing fraud; however, manual review can be expensive. Utilizing a chargeback prevention solution can cut down on resources diverted to manual review and lower chargebacks without negatively impacting sales. Finding the right balance is essential to maintaining a secure merchant account, avoiding fees and other penalties and ensuring that good sales continue to pass through.

* <http://www.verifi.com/terms-of-use/#general-performance-claims>



Why Choose Verifi?

Partner with Verifi to reduce your payments risks, streamline business processes and lower operational costs. Whether it's stopping fraud, maximizing your billings on our flexible and robust global gateway or our award-winning chargeback prevention and dispute management services, our team of experts and custom solutions will protect your payments and boost your profits across the entire transaction lifecycle.

Contact Verifi

323.655.5789

info@verifi.com

www.verifi.com

©2017 Verifi, Inc.

ALL RIGHTS RESERVED.

Citations

- 1 http://www.pymnts.com/news/2015/2014-fraud-spike-cost-u-s-retailers-32-billion/#.VUd_zEtkf8E
- 2 <https://www.infosecurity-magazine.com/news/crooks-raked-in-16b-via-identity/>
- 3 <http://www.marketwired.com/press-release/card-not-present-fraud-losses-to-exceed-7-billion-by-2020-2122258.htm>
- 4 <http://www.fraudpractice.com/FL-PayChargeback.html>
- 5 <http://www.fraudpractice.com/FL-PayChargeback.html>
- 6 <https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2016.pdf>
- 7 <https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2016.pdf>
- 8 <https://support.stripe.com/questions/avoiding-fraud-and-disputes>
- 9 <https://support.stripe.com/questions/avoiding-fraud-and-disputes>
- 10 <https://support.stripe.com/questions/avoiding-fraud-and-disputes>
- 11 <https://support.stripe.com/questions/avoiding-fraud-and-disputes>
- 12 <https://support.stripe.com/questions/avoiding-fraud-and-disputes>
- 13 <https://support.stripe.com/questions/avoiding-fraud-and-disputes>
- 14 <https://www.serviceobjects.com/blog/online-fraud-prevention/>
- 15 <https://support.stripe.com/questions/avoiding-fraud-and-disputes>
- 16 <https://www.serviceobjects.com/blog/online-fraud-prevention/>
- 17 <https://support.stripe.com/questions/avoiding-fraud-and-disputes>
- 18 <http://www.pymnts.com/news/2015/outsmarting-the-cnp-fraudsters/#.VR1jfovTEds>
- 19 <http://www.pymnts.com/news/2015/outsmarting-the-cnp-fraudsters/#.VR1jfovTEds>
- 20 <http://www.pymnts.com/news/2015/outsmarting-the-cnp-fraudsters/#.VR1jfovTEds>