

RR

# QUANTIFYING THE TOTAL COST OF ECOMMERCE FRAUD: MAKING BETTER, FASTER DECISIONS

December 2017

Derek E. Brink, CISSP

Vice President and Research Fellow, Information Security and IT GRC

**ABERDEEN**

Aberdeen's analysis of the total cost of eCommerce fraud shows that merchants are generally doing a good job at minimizing the impact of online orders that should not be taken (i.e., chargebacks). The much bigger opportunity is in making better and faster decisions to reduce the impact of online orders that are not taken because of suspected fraud (i.e., declines).

---

### Putting the Total Cost of eCommerce Fraud in Perspective

A simple keyword search on **eCommerce fraud** quickly reveals a rich and complex set of detailed, technical information — from the variety of ways that eCommerce fraud is currently being committed, to the even greater number of technologies that are designed to help address them.

From the most basic *business* perspective, however, managing the risk of eCommerce fraud is relatively straightforward, as online merchants are looking to balance three fundamental objectives:

- ▶ **Minimize fraudulent transactions.** Merchants naturally want to minimize the negative business impact of online orders that should not be taken in the first place. **Chargebacks** are transactions that are accepted but subsequently disputed — for a variety of reasons, with fraud being high among them — which leads to a reversal of revenue, along with fees from payment card processors and other associated costs.
- ▶ **Maximize legitimate transactions.** Likewise, merchants naturally want to accept all online orders that are legitimate. **Declines** are transactions that are not accepted because they are suspected to be fraudulent — many of which may in fact be okay. These *false declines* result in lost revenue for the current transaction, and potentially a loss of future revenue from the genuine buyers who were turned away.
- ▶ **Make better, cost-effective, and timely business decisions about fraud, in support of both of the above.** The total cost of making business decisions about fraud includes both the cost of *people* (e.g., full-time equivalent staff) and the cost of *tools and*

From the most basic business perspective, managing the risk of eCommerce fraud is relatively straightforward — online merchants are looking to balance three fundamental objectives:

- ▶ Minimize fraudulent transactions
- ▶ Maximize legitimate transactions
- ▶ Make better, cost-effective, and timely business decisions about fraud, in support of both of the above

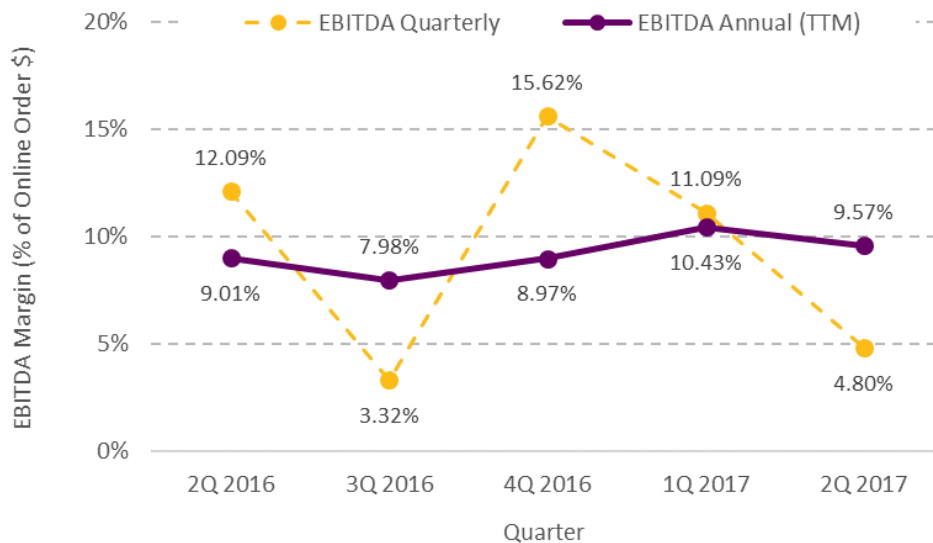
*data*. Moreover, in today's contemporary culture, even a few seconds of delay in the buyer's online experience can lead them to abandon their transactions and take their business elsewhere, making the *timeliness of making decisions* about eCommerce fraud as important as the total cost. *Prompt delivery* of goods and services in the overall order-to-fulfillment cycle is also important.

It's not hard to see how these three fundamental objectives can be in conflict. Acceptance policies that are too liberal lead to chargebacks. Acceptance policies that are too strict lead to false declines. Investing too little or too much in people, tools, and data — or taking too little or too much time to make acceptance decisions — could lead to either. Like Goldilocks, the key to happiness is to find the balance that is “just right.”

### Aberdeen's eCommerce Fraud Study

Some might argue that the business impact of eCommerce fraud is already fully baked into the operating models for online merchants, i.e., as “a cost of doing business” reflected in higher cost structures for sellers, and higher prices for buyers. But with both revenue and fraud seeing explosive growth, reducing the likelihood and total impact of eCommerce fraud would make a welcome contribution to any merchant's bottom line.

Figure 1: Annual Profitability for the Internet, Mail Order, and Online Segment of Retail Has Been Ranging Between 7.98% and 10.43%



Source: Adapted from CSImarket.com; Aberdeen Group, September 2017

**Earnings before interest, taxes, depreciation, and amortization (EBITDA) is an indicator of the overall profitability of a business.**

To put this point in perspective, consider the aggregate **earnings before interest, taxes, depreciation, and amortization (EBITDA)** for the

*internet, mail order, and online* segment of the retail industry. Over the past five quarters, the annualized EBITDA (based on the *trailing twelve-month* period, or *TTM*) ranged **between 7.98% and 10.43%** of top-line revenue, as shown in Figure 1. This is the yardstick for overall profitability against which the total cost of eCommerce fraud should be compared.

Aberdeen's study to measure and quantify the likelihood and business impact of eCommerce fraud is based on direct phone interviews with respondents that met all of the following qualifications:

- ▶ Represent an online merchant in one of the **eight market segments** described in Table 1
- ▶ Have online orders of **at least US\$50M per year** (and based on actual responses, up to US\$1.5B per year)
- ▶ Accept online orders which are **paid primarily by credit card** (i.e., not by PayPal, AliPay, etc.)
- ▶ Have an average order size of **less than or equal to US \$500**
- ▶ Know the answers to questions about **declines, chargebacks**, and the **cost and time** of decision-making, described in Table 2

---

**EBITDA for online merchants has been ranging between 7.98% and 10.43% of annual orders — this is the yardstick for overall profitability against which the total cost of eCommerce fraud should be compared.**

---

Table 1: Market Segment Definitions for Aberdeen's Study

**Aberdeen's eCommerce fraud study specifically targeted online merchants in the following eight market segments:**

1. **Alcohol, Tobacco, and Cannabis** covers merchants selling both these substances and their related accessories and paraphernalia. For cannabis specifically, sites selling accessories and paraphernalia are much greater in number than those selling actual dry herb or its derivatives directly to consumers.
2. **Apparel (Clothing, Accessories, Shoes, Sunglasses)** is a broad category and covers all clothing, shoes, and accessories such as belts, hats, and sunglasses. Given the universal market for such goods, the range of products and brands included in this category varies greatly, from discount stores to global luxury brands.
3. **Consumer Electronics** covers items as varied as televisions, laptop computers, digital cameras, flash drives, drones, electric scooters, hoverboards, and wireless earbuds. If it's powered by batteries (with the exception of vehicles), it will likely fall into this category.
4. **Cosmetics and Perfumes** covers fragrances, makeup, wigs, and skin care for both men and women.
5. **Department Stores** are classified as eCommerce merchants selling a wide variety of household products intended to save the consumer a trip to their local department store and/or grocery store. Given the broad selection of items at such sites, the specific products sold by this category of online merchants may overlap with Apparel, Cosmetics and Perfumes, or Consumer Electronics.
6. **Furniture, Appliances, and Home Improvement** covers all major purchases for the home or other properties, and those purchases intended to improve or repair such properties.
7. **Health, Leisure, and Hobbies (Outdoor, Fitness, Sporting Goods, Weapons)** covers many disparate sub-categories of merchants who sell items ranging from fishing equipment and swords, to training weights and board games.
8. **Jewelry and Precious Metals** includes designer and personalized jewelry of varying values, precious metals, and coins for collectors.

Source: Aberdeen Group, September 2017

Aberdeen's measurement of the total cost of eCommerce fraud is based on questions about four key factors that qualified respondents could credibly answer about the **Cost of Fraud** (*declines; chargebacks*) and the **Cost of Decisions** (*people; tools and data*), as described in Table 2.

---

**Aberdeen's measurement of the total cost of eCommerce fraud is based on questions about four key factors that qualified respondents could credibly answer about the **Cost of Fraud** (*declines, chargebacks*), and the **Cost of Decisions** (*people; tools and data*).**

---



Table 2: Factors for Estimating the Total Cost of eCommerce Fraud

Factors		Description
Cost of Fraud	Declines	Merchants accept most of their online orders, but some online orders are declined. Respondents provided Aberdeen with the <i>percentage of annual online orders that they decline</i> due to concerns about fraud.
	Chargebacks	Chargebacks are claimed against orders that were accepted but subsequently disputed, requiring merchants to return all payments received along with additional fees. Respondents provided Aberdeen with <i>the amount their organization is losing in chargebacks</i> , which was then expressed as a percentage of annual online orders.
Cost of Decisions	People	Organizations invest in people to help make decisions about which orders to accept, and which orders to decline because they are suspected to be fraudulent. Respondents provided Aberdeen with <i>the number of full-time equivalent staff</i> their organization uses to decide which online orders to accept or decline, which was then expressed in financial terms as a percentage of annual online orders.
	Tools and Data	Organizations often also invest in tools (technologies) and data to help make decisions about which orders to accept, and which orders to decline because they are suspected to be fraudulent. Respondents provided Aberdeen with the amount their organization is spending on tools and data to decide which online orders to accept or decline, which was then expressed as a percentage of annual online orders.

Source: Aberdeen Group, September 2017

### Quantifying the Total Cost of eCommerce Fraud: Aberdeen’s Monte Carlo Model and Analysis

To quantify the likelihood and business impact of eCommerce fraud, Aberdeen developed a simple **Monte Carlo** model based on the **range** (*lower bound, upper bound*) and **shape** (*probability distribution*) of each of these four key factors — as informed by its phone interviews with knowledgeable practitioners in each of the eight market segments.

In a **Monte Carlo** analysis, each variable in a calculation is expressed as a **range** (*lower bound, upper bound*) and a **shape** (*probability distribution*) — as opposed to as a single, static value.

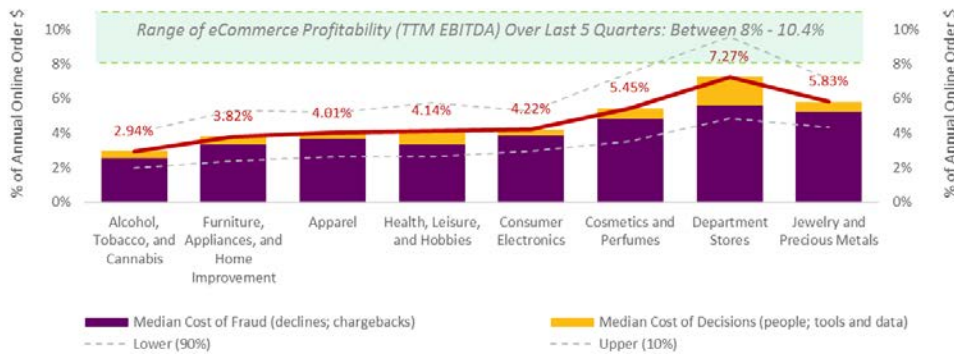
The relevant calculations are then carried out based on a randomly selected value from the probability distribution for each variable, over many (say, 10,000) independent iterations.

In doing so, the result is also expressed as a range and distribution — as opposed to a single, static value such as “the average cost of a data breach is \$201 per record” or “the average scrap learning rate is 45%.”

Most importantly, the result can readily be represented in terms of both *how likely* and *how much business impact* — i.e., in terms of **risk**, as risk is properly defined.

**Monte Carlo** models are well-aligned with the proper definition of **risk**, and are well-suited to deal with the inherent **uncertainties** in quantitative estimates for the likelihood and business impact of the four factors of eCommerce fraud. Proven and widely used for several decades across a diverse range of industries and applications, Aberdeen has been successfully using Monte Carlo analysis to gain insights into security-, compliance-, and operational-related risks for the last four years.

**Figure 2: The Total Annual Cost of eCommerce Fraud is Surprisingly High Relative to Overall Industry Profitability**



Source: Monte Carlo analysis; Aberdeen Group, September 2017

The results of Aberdeen’s Monte Carlo analysis are summarized in Figure 2. For each of the eight market segments:

- ▶ The *median* total cost of eCommerce fraud, as a percentage of annual order dollars, is represented by the **solid red line**.
- ▶ The *range* for the total cost of eCommerce fraud is depicted by the lower bound (*90% likely to exceed*) and upper bound (*10% likely to exceed*), as represented by the **dashed grey lines** below and above the median. As defined here, this range is often referred to as the *80% confidence interval* for the estimate — which reflects the inherent *uncertainties* in any quantitative risk assessment.
- ▶ To provide additional insights into the differences between market segments, the median total cost of eCommerce fraud is also represented by the **two stacked bars**: the **purple** represents the median *Cost of Fraud* (declines; chargebacks), and the **orange** depicts the median *Cost of Decisions* (people; tools and data).
- ▶ Finally, the range of overall profitability (EBITDA) in the online retail industry over the last five quarters is also shown in **green**, as

a useful yardstick for comparison with the total cost of eCommerce fraud.

#### *Four High-Level Insights About eCommerce Fraud*

The results are different for each of the eight market segments, but in general Aberdeen's analysis highlights four high-level insights about current merchant performance at balancing their three fundamental business objectives related to eCommerce fraud:

- ▶ **Merchants are generally doing a good job at minimizing the negative impact of fraudulent transactions — but at a high Cost of Decisions.** As a percentage of annual online order dollars, *chargebacks* in Aberdeen's study ranged between just 4 and 46 basis points. But the Cost of Decisions ranged between 31 and 167 basis points — which means that merchants are currently spending **between 2.3 and 13.9 times more** on *making decisions* about fraud than they are actually losing on chargebacks.
- ▶ **Merchants are unlikely to be maximizing the positive impact of legitimate transactions, because of concerns about fraud.** As a percentage of annual online order dollars, *declines* in Aberdeen's study ranged between 2.5% and 5.14% — which means that merchants are currently turning away **between 11 and 100 times more** order dollars because of concerns about potential fraud than they are actually losing on chargebacks.
- ▶ **The total cost of eCommerce fraud is significant, particularly in proportion to overall industry profitability.** On average, the combined *Cost of Fraud* (*declines*, *chargebacks*) plus *Cost of Decisions* is **between 45% and 60%** of overall industry profitability (*EBITDA*). Said another way, for every dollar in overall industry profitability, the total cost of eCommerce fraud is between 45 and 60 cents. Surely a business impact of this magnitude is too much to be waved away as merely “a cost of doing business.”
- ▶ **Merchants taking longer to make decisions generally correlates with reducing the total cost of eCommerce fraud — but with diminishing returns.** As shown in Figure 3, taking a longer time between order and fulfillment to make decisions *does* correlate with a lower total cost of eCommerce fraud. But this is not a linear relationship — for example, taking twice as long to decide corresponds with *less* than half as much total cost. As previously noted, taking too long for either acceptance or delivery of online

---

Models are intended to be *useful*, not perfect. To the extent that additional factors (e.g., loss of current or future revenue from taking too long for acceptance or delivery) are not included, Aberdeen's analysis represents an *understated* estimate of fraud-related risks.

---

---

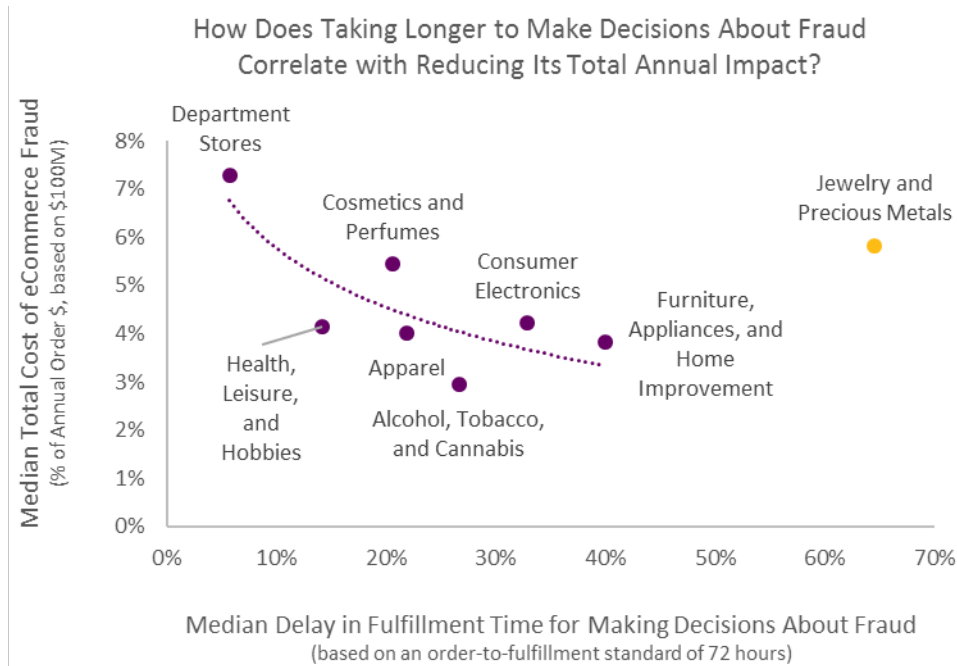
**A basis point is defined as one one-hundredth of one percent (0.01%).**

---



orders can also have a negative impact on legitimate transactions, both now and in the future. This is an additional factor that Aberdeen did *not* consider in its current model and analysis — making it an *understated* estimate of fraud-related risks.

**Figure 3: Taking Longer to Make Decisions About Fraud Correlates with Reducing its Total Annual Impact — with Diminishing Returns**




Source: Monte Carlo analysis; Aberdeen Group, September 2017

The *Jewelry and Precious Metals* segment is an outlier to the general correlation between the delay in fulfillment time for making decisions, and the total cost of eCommerce fraud (see Figure 3). In Aberdeen’s study, merchants in this segment took the *longest* time to decide — yet still had nearly the *highest* total cost of fraud. Qualitatively, it seems that buyers of these goods are more willing to tolerate a longer time from order-to-fulfillment, but these goods are also attractive targets for the fraudsters.

### For Many Online Merchants, Making Decisions About eCommerce Fraud Can’t Wait

Aberdeen’s study — which as noted, focused specifically on online merchants in eight market segments dealing in **physical goods** — shows that although the current level of performance for making decisions about eCommerce fraud generally “fits” within an order-to-shipment target of 72 hours, speed of decision-making is a problem which will only grow worse



under market pressure for faster delivery. In fact, the empirical data shows that it quickly becomes untenable: for an order-to-shipment target of 24 hours, online merchants will miss their target and ship late literally half of the time.

For many online merchants, however, decisions about eCommerce fraud simply cannot wait — they must be made in real time. As an example, consider the following case-in-point from the restaurant industry.


### *Customer Case-in-Point: ChowNow*

By providing restaurants of all sizes with the power of a comprehensive online ordering platform — which enables hungry customers to place their orders directly from the restaurant’s website, Facebook page, or branded mobile apps — service provider *ChowNow* helps them to expand their business, while staying focused on what they do best: food and customer service.

From its launch in 2012, ChowNow at the end of 2017 processes tens of thousands of online transactions per day on behalf of some 8,000 subscribers in the US and Canada. ChowNow’s Operations Director, John Page, puts the business impact of fraudulent transactions over the last five years in perspective. “When fraud was a \$20K to \$30K per month problem, it wasn’t as big of an issue to our CEO and Board,” he explains. “Our strategic focus was on growing relationships, and we didn’t want to create a lot of friction in the ordering process that would end up alienating and losing customers.”

As their business continued to expand, however, and fraud became a \$40K to \$50K per month problem, it started to attract attention from their investors. Restaurants subscribing to ChowNow’s online ordering platform don’t actually feel the impact of online fraud — if a transaction is fraudulent, ChowNow is the one that eats it. “Dispute processes are retroactive, and all very anti-business,” said Page. “Order verification by email or text messaging is not as friendly to users. About all we could do is block the profile of known offenders.” Other undesirable options included not supporting restaurants in certain territories, or cutting up to 10% of current subscribers for whom fraud was especially high.

By early 2017, the problem had grown to \$100K per month, and at the suggestion of ChowNow’s CTO Page started beta testing a real-time fraud prevention service from *Sift Science*. After a quick integration and testing period of just three months, the system went live. Although admittedly skeptical at first about relying on a machine learning platform,



based on his many years of hands-on experience, Page found that the results were undeniable — good patrons weren't being stopped or slowed down, and fraudulent transactions were automatically blocked.

In addition, ChowNow found that a “network” feature in the Sift Science Digital Trust Platform could tag user profiles (e.g., devices, IP addresses) and behaviors that may not have been flagged previously — for example: fraudulent orders at multiple restaurants; the use of multiple payment cards at the same location; and placement of abnormally large orders (and then re-selling the food). “People are constantly testing the system,” Page said, which is why he still keeps eyeballs on the transactions as they happen. A small number (about 100 transactions per day) still have manual review, but for the most part, the decision-making process is real-time and fully automated.

Even with ChowNow's continued expansion in business, the percentage of fraudulent transactions has declined by a factor of 5 times, and the total cost of fraud has dropped by a factor of about 2.5 times (including the cost of the real-time fraud prevention service) since implementing the new approach. Asked about words of wisdom to be shared with others, Page noted that the attitude of senior business leaders is often that “fraud isn't big enough; it isn't costing us enough to change the way we operate.” But the money saved can be leveraged and reinvested in the business — while also making it easier for the company to achieve its strategic business objectives.

### **Additional Market-Specific Analysis is Available**

Aberdeen's Monte Carlo model has been implemented using standard functionality of Microsoft Excel, and includes simple drop-down menus for **market segment** and **annual order dollars**. A snapshot of Aberdeen's analysis for each of the eight market segments listed in Table 1 is also available from [www.aberdeen.com](http://www.aberdeen.com) as a series of segment-specific *Knowledge Briefs* and *SmartBites*.

## Summary and Key Takeaways

- ▶ From the most basic business perspective, managing the risk of eCommerce fraud is relatively straightforward — online merchants are looking to balance **three fundamental objectives**:
  - **Minimize fraudulent transactions**
  - **Maximize legitimate transactions**
  - **Make better, cost-effective, and timely business decisions** about fraud, in support of both of the above
- ▶ These three fundamental business objectives can easily be in conflict. Acceptance policies that are too liberal lead to chargebacks. Acceptance policies that are too strict lead to false declines. Investing too little or too much in people, tools, and data — or taking too little or too much time to make acceptance decisions — could lead to either. Like Goldilocks, the key to happiness is to find the balance that is “just right.”
- ▶ Over the past five quarters, the annualized earnings before interest, taxes, depreciation, and amortization (EBITDA) for online merchants ranged **between 7.98% and 10.43%** of top-line revenue. This is the yardstick for overall profitability against which the total cost of eCommerce fraud should be compared.
- ▶ Aberdeen’s study to measure and quantify the likelihood and business impact of eCommerce fraud is based on direct phone interviews with respondents that met all of the following qualifications:
  - Represent an online merchant in one of **eight defined market segments**
  - Have online orders of **US\$50M to US\$1.5B per year**
  - Accept online orders **paid primarily by credit card**
  - Have an average order size of **US\$500 or less**
  - Know the answers to questions about **declines, chargebacks**, and the **cost** and **time** of decision-making
- ▶ To quantify the likelihood and business impact of eCommerce fraud, Aberdeen developed a simple **Monte Carlo** model based on the **range** (*lower bound, upper bound*) and **shape** (*probability*

Online merchants should **re-evaluate their current practices** — along with the latest tools and data from leading **solution providers** — with the goal of **achieving a better balance** between minimizing fraudulent transactions; maximizing legitimate transactions; and making better, cost-effective, and timely business decisions about eCommerce fraud.

*distribution*) of each of these four key factors — as informed by its phone interviews with knowledgeable practitioners in each of the eight market segments.

- ▶ Aberdeen's analysis highlights **four high-level insights** about current merchant performance at balancing their three fundamental business objectives related to eCommerce fraud:
  - **Merchants are generally doing a good job at minimizing the negative impact of fraudulent transactions — but at a high Cost of Decisions.** As a percentage of annual online order dollars, *chargebacks* in Aberdeen's study ranged between just 4 and 46 basis points. But the Cost of Decisions ranged between 31 and 167 basis points — which means that merchants are currently spending **between 2.3 and 13.9 times more** on *making decisions* about fraud than they are actually losing on chargebacks.
  - **Merchants are unlikely to be maximizing the positive impact of legitimate transactions, because of concerns about fraud.** As a percentage of annual online order dollars, *declines* in Aberdeen's study ranged between 2.5% and 5.14% — which means that merchants are currently turning away **between 11 and 100 times more** order dollars because of concerns about potential fraud than they are actually losing on chargebacks.
  - **The total cost of eCommerce fraud is significant, particularly in proportion to overall industry profitability.** On average, the combined *Cost of Fraud* (declines; chargebacks) plus *Cost of Decisions* is **between 45% and 60%** of overall industry profitability (*EBITDA*). Said another way, for every dollar in overall industry profitability, the total cost of eCommerce fraud is between 45 and 60 cents.
  - **Merchants taking longer to make decisions generally correlates with reducing the total cost of eCommerce fraud — but with diminishing returns.** Taking a longer time between order and fulfillment to make decisions correlates *non-linearly* with lower total cost of eCommerce fraud — for example, taking twice as long to decide corresponds with *less* than half as much total cost. Taking



too long for either acceptance or delivery of online orders can have a negative impact on legitimate transactions, both now and in the future.

- ▶ Speed of decision-making about eCommerce fraud is a problem which will only grow worse under market pressure for faster delivery. For an order-to-shipment target of 24 hours, Aberdeen's analysis shows that based on current performance online merchants of physical goods will miss their target and ship late literally half of the time. For many other online merchants, decisions about eCommerce fraud must be made in real-time.
- ▶ A snapshot of Aberdeen's analysis for each of the eight market segments is also available from [www.aberdeen.com](http://www.aberdeen.com) as a series of segment-specific *Knowledge Briefs* and *SmartBites*.

## Related Research

---

*Your Hidden Quality-of-Information Problems: What You Don't Know Can Hurt You*; September 2017

*Quantifying the Value of Cyber Insurance for Data Breaches*; August 2017

*Quantifying the Value of Counter Fraud Analytics in Insurance*; December 2016

*Fighting Fraud in Online Banking*; August 2015



## About Aberdeen Group

Since 1988, Aberdeen Group has published research that helps businesses worldwide to improve their performance. Our analysts derive fact-based, vendor-neutral insights from a proprietary analytical framework, which identifies Best-in-Class organizations from primary research conducted with industry practitioners. The resulting research content is used by hundreds of thousands of business professionals to drive smarter decision-making and improve business strategies. Aberdeen Group is headquartered in Waltham, Massachusetts, USA.

This document is the result of primary research performed by Aberdeen Group and represents the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen Group.