LexisNexis® Risk Solutions
2017 True Cost of Fraud℠
# Table of Contents

Introduction ......................................................................................................................... 3

Executive Summary .............................................................................................................. 5

  Overview .......................................................................................................................... 5

  Key Findings .................................................................................................................... 5

Recommendations ............................................................................................................... 7

Fraud is a Threat in the Online Channel ........................................................................... 8

Identity Verification is a Problem ...................................................................................... 12

The Mobile Channel May Heighten These Challenges ...................................................... 16

What’s Being Done to Combat Fraud ................................................................................ 18

Using the Right Combination of Fraud Tools is Crucial .................................................... 22

LexisNexis® Risk Solutions Can Help .............................................................................. 24

Methodology ..................................................................................................................... 25
INTRODUCTION

The LexisNexis® Risk Solutions 2017 True Cost of Fraud℠ Study aims to help merchants (retail and online / mobile), financial services companies and lending firms grow their business safely even with the growing risk of fraud. The research provides a snapshot of current fraud trends in the United States and spotlights key pain points that:

- Merchants (retail and online / mobile) should be aware of as they add new payment mechanisms and expand channels into online and mobile channels.
- Financial services companies and lenders should be aware of as they add new transaction and account opening mechanisms, as well as when expanding into the online and mobile channels.

The study answers a question critical to businesses: How do I grow my business and manage the cost of fraud while strengthening customer trust and loyalty?

Included in this study is feedback from fraud executives in 4 industry segments: retail merchants; eCommerce merchants; financial services firms; and lending institutions.

Fraud Definitions

- Fraud is defined as the following:
  - Fraudulent and / or unauthorized transactions (for retail and online / mobile merchants);
  - Fraudulent transactions due to identity fraud, which is the misuse of stolen payments methods (such as credit cards) or personal information (for financial services companies and lenders);
  - Fraudulent requests for refund / return; bounced checks; and
  - Lost or stolen merchandise, as well as redistribution costs associated with redelivering purchased items.
- This research covers consumer-facing fraud methods.
- It does not include insider fraud or employee fraud.
- The LexisNexis Fraud Multiplier℠ is defined as follows:
  - The total amount of costs related to fees, interest, merchandise replacement and redistribution per dollar of fraud for which the merchant is held liable.
Merchant definitions

- Small merchants earn less than $10 million in average annual sales.
- Medium-size merchants earn $10 million to less than $50 million in average annual sales.
- Large merchants earn $50 million or more in annual sales.
- International merchants operate from the U.S. and do business globally.
- Domestic merchants do not sell merchandise outside the U.S.
- There are two types of merchants that sell online as follows:
  - Retailers with an online channel – primarily bricks / mortar retailers with an online or mobile channel in addition to the physical channel; tends not to have a majority of revenues or transactions through just the online or mobile channels.
  - eCommerce merchants – more “pure online” merchants which generate the majority (80%+) of their revenues through the online channel.
- Mobile eCommerce merchants (mCommerce merchants) accept payments through either a mobile browser or mobile application, or bill payments to a customer’s mobile carrier. Large mCommerce involves those earning $50 million or more in annual sales.
- Digital and physical goods merchants sell both of these types of goods and services.
- Digital financial services / lending firms (or “primarily digital”) are those which generate 50% or more revenue through online or mobile channels (also referred to as remote channels).
EXECUTIVE SUMMARY

Overview
Sizeable fraud is occurring within the US retail, eCommerce, financial services and lending sectors. For businesses in these industries, the key focus is all things digital. This means online sales, especially involving digital goods, for retailers; retail fraud has increased significantly over 2016 based on a spike in online shopping volume and fraudster focus on digital goods. Financial services and lending firms that generate most business through digital (online, mobile) channels are also a key target, especially through identity fraud with applications and account takeovers. As a result, the cost and volume of fraud is higher for these digitally-focused merchants and firms than others; and the larger the merchant / firm, the higher the costs.

This causes real frustration for both merchants / firms and their customers. Larger merchants selling digital goods and financial services / lending firms that conduct most business remotely are typically using multiple fraud mitigation solutions to combat fraud. At the same time, they still struggle with identity verification, which in turn can increase costs associated with excessive manual reviews and customer friction because of delayed transaction confirmation. And for those selling digital goods, the very nature of this faster transaction mode makes it difficult to balance fraud mitigation against friction that can lead to customers leaving before transactions are completed.

But, perhaps the right combination or layering of solutions aren’t being used. Study findings show that a multi-layered approach that includes identity verification, identity authentication and transaction risk assessment can reduce the volume of successful fraud attempts and associated fraud costs among businesses in these sectors. The following are key findings and recommendations to help retail / eCommerce merchants and financial services / lending firms understand and navigate this challenging environment.

Key Findings
- The cost of fraud is sizeable for retail, eCommerce, financial services and lending organizations. Every $1 of fraud costs organizations in these industries between $2.48 and $2.82 – that means that fraud costs them more than roughly 2 ½ times the actual loss itself. Fraud cost as a percent of revenues ranges between 1.58% and 2.39%.
- The eCommerce, financial services and credit (rather than mortgage) lending sectors are getting hit somewhat harder. Organizations in these sectors represent the higher range of fraud costs as a percent of annual revenues. Some of that can relate to relying on manual review efforts, which drives up direct expenses in labor
(either internally or outsourced). For eCommerce and financial services, they are also declining more transactions, which lowers potential revenue levels from which the impact of fraud costs are measured. And, for eCommerce, this coincides with a rise in online purchasing during the past year and the trend of fraudsters targeting the anonymous channel.

- **The digital space, either as a transaction channel or type of good being sold, is a high risk for even more negative fraud impact.** Regardless of industry segment, the percent of average monthly fraud attempts is higher for these types of organizations. For those using the online channel, this is the result of more fraudster focus on the anonymous purchasing environment, particularly leveraging the no-card-present opportunities compared to EMV chip barriers at physical points of sale. This has also given rise to Botnet fraud. For digital goods sellers, there has been a rise in e-gift card volume and fraud. This type of e-good can often be distributed / obtained / downloaded quickly, leaving less time for risk verification – particularly among those conducting manual reviews. As a result, these organizations have higher fraud costs, with those tracked for retailers selling digital goods rising significantly over 2016. In a number of cases, the above is heightened among mid and larger organizations.

- **Yet, digital channel / digital goods selling organizations are not fully leveraging the value of risk mitigation solutions.** Identity verification remains a challenge and common type of fraud; there is only moderate use of advanced identity verification solutions among these organizations. Being “digitally” focused does not mean the exclusion of traditional non-digital products or channels. It appears that some of these companies are applying a one-size fits all approach to fighting both types of products and channels – yet fighting different types of challenges.

- **These issues will only increase as more firms adopt the mobile channel.** Larger merchants / firms tend to be the pioneers of the mobile channel. Based on their experiences, identity verification, new payment / transaction methods and delayed confirmation are key challenges. They are also most likely to express concerns about the risk and security of conducting transactions via this channel – again, based on experience.

- Findings show that retailers, eCommerce merchants and financial services and lending firms which **layer solutions by identity and fraud transaction solutions experience fewer issues and cost of fraud.**
Recommendations

- Retailers, eCommerce merchants, financial services firms and lending institutions should implement different risk mitigation solutions to address unique risks from different channels and sales models. There is no one-size-fits-all solution. Solutions used to mitigate risk with physical goods or non-digital channel transactions won’t fully mitigate those generated from digital goods and transaction channels. Digital goods sellers require more real-time transactions and verification given the faster transaction pace. Digital channels are more anonymous and difficult with regard to identity verification. With the mobile channel, the very nature of mobility means that mobile-based payment transactions and devices carry different levels of risk and challenges regarding identity and device verification than with online / Internet browser transactions.

- It’s not just about the number of risk mitigation solutions, but rather the most effective multi-layered approach that attacks different types of fraud. It is critical for companies to address both identity and transaction-related fraud. These are two different perspectives. Identity verification / authentication is important for “letting your customers in” with the least amount of friction and risk. Transaction-related fraud is about keeping the “bad guys out”. A layered approach can reduce costs associated with manual reviews, successful fraud attempts and fewer false positives.

- Mid / Large companies that focus on selling digital goods or conduct a majority of transactions through digital channels need to remain particularly vigilant and open to a wider variety of risk mitigation solutions – sooner rather than later. Fraud and its associated costs are already more of an issue for these companies. This will become more heightened as they adopt the mobile channel in the near-term – and as the volume of these transactions grow (which retail shows us by example as being likely to increase quickly). A layered solution approach should particularly consider those which support faster / real-time identity and transaction verification decision making. The above is particularly important to eCommerce and financial services firms.

- In addition to solutions investments, companies also need to be efficient with fraud management. Fraud occurs in multiple ways depending on the type of goods / services, channel and payment method. Different technology drives different payment methods, channels and even the nature of goods purchasing. Therefore, fraudsters have many attack points. Without tracking both successful and prevented fraud by both channel and payment method, companies’ efforts at fighting fraud are weakened.

The following are detailed findings from the LexisNexis® Risk Solutions 2017 True Cost of Fraud℠ Study.
The threat of fraud is growing among merchants/firms in the retail, eCommerce, financial services and lending sectors. Those selling digital goods and conducting business primarily through online/mobile channels\(^1\) are getting hit hardest.

In our LexisNexis Risk Solutions® 2016 True Cost of Fraud™ Study among U.S. retailers, we reported that fraud and its associated costs among merchants was growing, with those selling through the online or mobile channels getting hit hardest. Turning the clock forward 12 months, we find this trend continuing, driven not just by the transaction channel but also the type of goods/services sold.

The average volume of monthly fraud attempts among U.S. retailers has increased nearly 12%, which is a higher jump than the 2015-2016 change (8%). And, it has jumped even more significantly among retailers selling digital goods (see Figure 1).

---

**Average Retail Fraud Transactions Have Increased, Particularly Among Digital Goods Sellers**

Weighted data

Q: In a typical month, approximately how many fraudulent transactions are successfully completed by fraudsters?

March 2015 – April 2017; base = all merchants experiencing fraud

<table>
<thead>
<tr>
<th>Year</th>
<th>Overall Retail Fraud Attempts</th>
<th>Selling Digital Goods Fraud Attempts</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>156</td>
<td>333</td>
</tr>
<tr>
<td>2016</td>
<td>206</td>
<td>442</td>
</tr>
<tr>
<td>2017</td>
<td>238</td>
<td>495</td>
</tr>
</tbody>
</table>

**Average # Monthly Fraud Attempts & Successes – U.S. Retailers**

- Fraud Attempts per Month
- Fraud Attempts per Month That SUCCEED

<table>
<thead>
<tr>
<th>Year</th>
<th>Overall Retail Fraud Attempts</th>
<th>Selling Digital Goods Fraud Attempts</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>630</td>
<td>655</td>
</tr>
<tr>
<td>2017</td>
<td>370</td>
<td>1193</td>
</tr>
</tbody>
</table>

---

\(^1\) For the purposes of this report, digital channels relate to online or mobile channels; digital goods relate to any goods or services that are stored, delivered and used in its electronic format
The dramatic rise in digital goods fraud correlates with a spike in Botnet fraud and the rise in e-gift card volumes (reportedly up 29% annually\(^2\)), especially during the 2016 holiday season. While digital goods are comprised of more than just e-gift cards, this particular type of digital good has become an easy target for fraudsters; the lack of a physical card supports anonymity, the lack of physical magnetic strip technology makes it easier for replicated use and e-gift cards can be quickly resold for cash.\(^3\)

Online transactions have risen dramatically as well during the past year, with the U.S. Department of Commerce reporting a 16% year-over-year increase in eCommerce volume.\(^4\) Online lending has made leaps and bounds since securitization in 2013 made online platforms more accessible to capital and 2015 partnerships emerged between large banks and lenders.\(^5\) The average monthly volume of fraud attempts is higher for credit lenders (1,362) than mortgage lenders (851). With non-lending financial services, there has been significant growth since 2012 of the “omni-digital” consumer segment, which conducts banking only through remote channels such as mobile phones, PCs and tablets – impacted significantly by Millennials.\(^6\) With more volume comes more opportunity for the “bad guys”.

Merchants selling digital goods and larger firms transacting primarily through digital channels experience higher average monthly fraud volumes (see Figure 2).

---


\(^5\) http://www.businessinsider.com/online-lending-has-reached-a-tipping-point-2017-4

\(^6\) https://thefinancialbrand.com/65628/digital-banking-consumer-trends

---

**Table:**

| Digital Goods Sellers and Larger Online Financial Services & Lending Firms Have Higher Fraud Volumes |
| --- | --- | --- | --- | --- |
| **Weighted data** | **Average # Monthly Fraud Attempts & Successes** |
| **Q:** In a typical month, approximately how many fraudulent transactions are successfully completed by fraudsters? |
| **2017; base = all merchants experiencing fraud** | **Fraud Attempts per Month** | **Fraud Attempts per Month That SUCCEED** |
| Retail Merchants | eCommerce Merchants | Financial Services Firms | Lending Firms |
| 276 | 334 | 2031 | 1193 | 556 | 380 | 1959 | 655 | 281 | 382 | 501 |

---

**Figure 2:** Average number of transactions and fraud attempts per month for retail, eCommerce, financial services and lending (2017)
Not surprisingly, then, the cost of fraud is higher for merchants selling digital goods and larger financial services / lending firms that conduct transactions primarily through online / mobile channels.

Every $1 of fraud costs these digital merchants / firms between $3.04 and $3.56 ($3.48 for digital across the 4 industries), with the higher figure representing retailers selling digital goods. For each of the four industry segments, those with a digital focus have a higher LexisNexis Fraud Multiplier℠ than others overall (see Figure 3). And, the rise in fraud volume among digital goods retailers since 2016 has driven the overall LexisNexis Fraud Multiplier℠ up for the retail segment (see Figure 4).

The nature of fraud costs and chargebacks differ between physical and digital goods. With physical goods, merchants need to purchase and replace lost merchandise. For digital goods sellers, the majority of costs are related to fees charged by 3rd party distribution vendors and credit card companies, including fines if chargebacks reach a certain threshold. This means that digital goods sellers have a higher proportion of indirect losses, which drives up the LexisNexis Fraud Multiplier℠ per $1 of direct fraud losses (i.e., chargebacks).

The LexisNexis Fraud Multiplier℠ is Higher for Merchants and Financial Services / Lending Firms Involved with Digital Goods and Transactions

Weighted data

Q: Thinking about the total fraud losses suffered by your company, please indicate the distribution of fraud costs across chargebacks, fees / interest, and lost / stolen merchandise during the past 12 months.

March – April 2017; base = those experiencing fraud in past 12 months

Figure 3: Cost per dollar of fraud losses (2017)
**Digital Goods are Driving Increased Retail Fraud Costs**

Weighted data

Q: Thinking about the total fraud losses suffered by your company, please indicate the distribution of fraud costs across chargebacks, fees / interest, and lost / stolen merchandise during the past 12 months.

February 2016 – April 2017; base = those experiencing fraud in past 12 months

For financial services / lending firms, higher successful fraud values may carry larger fees and lost interest that needs to be paid to funders (which can include separate divisions / businesses within the organization, involving internal transfer costs). Additionally, since nearly all large digital lenders are allowing mobile transactions, this segment can be characterized as “remote multi-channel” on average; therefore, there are more ways for fraudsters to attack them, as well as steal customer information – particularly through the less secure mobile channel. And since the mobile channel is particularly useful for giving access to the un-/underbanked who have less of an established profile and credit footprint, it makes identity verification even more challenging.

Not only is the cost of fraud higher for digitally-focused retail / eCommerce merchants and larger financial services / lending firms, but fraud also takes a bigger bite out of their bottom line revenues. Within lending, credit lenders get hit harder on the bottom line more than mortgage lenders (2.41% versus 1.26%).

**eCommerce Merchants Selling Digital Goods and Larger Digital Financial Services Firms Take a Harder Bottom Line Hit from Fraud**

Weighted data

Q: What is the approximate value of your company’s fraud losses over the past 12 months as a % of total revenues?

March – April 2017; base = those experiencing fraud in past 12 months

For fraud multipliers, see Table 4.
Identity fraud is a key challenge for retail / eCommerce merchants, financial services institutions and lending firms.

Verifying identities is a top challenge for these businesses when operating through the online channel and is among the top issues in the mobile channel as well. It is particularly challenging for financial services firms, which can experience the effects of such fraud through not only their own customer transactions but also, at least among credit card companies, that which occurs through retailers. And with compromised consumer data from various credit / debit card breaches and the rise of synthetic identities, the financial services sector provides a very lucrative target for fraudsters through take-overs of accounts with sizeable assets.

Figure 6: Top online and mobile channel fraud challenges (2017)
But identity verification impacts segments differently and isn’t just acute within financial services. When we dig deeper, we find that this becomes more pressing among larger eCommerce merchants and financial services / lending firms which conduct most transactions through the online or mobile channels (see Figure 7). This makes sense; these businesses have significantly more transactions occurring in the anonymous remote channels than non-digital firms and bricks / mortar retailers. Therefore, it’s a numbers game; there are significantly more transactions needing more levels of verification than are required for onsite transactions.

### Identity Verification is More Challenging for Larger Online Merchants and Digital Lending / Financial Services Firms

<table>
<thead>
<tr>
<th>Weighted data</th>
<th>% Ranking Identity Verification Among Top 3 Challenges in Online Channel</th>
<th>% Ranking Identity Verification Among Top 3 Challenges in Mobile Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q: Please rank the top 3 challenges related to fraud when serving customers in the Online Channel / Mobile Channel.</td>
<td>Mid / Large Retail selling digital goods Overall 50%</td>
<td>Mid / Lg Financial Svc w/ mostly digital transactions Overall 62%</td>
</tr>
<tr>
<td>Q: Please rank the top 3 challenges when selling digital goods in the US.</td>
<td>Overall 47%</td>
<td>Overall 41%</td>
</tr>
<tr>
<td>March – April 2017; base = those experiencing fraud in past 12 months and using the online or mobile channel for transactions</td>
<td>Mid / Lg eCommerce</td>
<td>Lg Lending w/ mostly digital transactions Overall 38%</td>
</tr>
</tbody>
</table>

Figure 7: Percent ranking identity verification among top 3 online / mobile channel challenges

It’s not surprising, then, that the average distribution of fraud losses among larger merchants selling digital goods and larger digital financial services and lending firms involves identity fraud. For financial services and lending firms, identity fraud also enables account takeovers.

### Identity Fraud Represents a Sizeable Portion of Digital Goods / Channel Losses

<table>
<thead>
<tr>
<th>Weighted data</th>
<th>% Distribution of Losses by Type of Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q: Please indicate the % distribution of fraud across the following types.</td>
<td>Mid / Lg Retailer Selling Digital Goods</td>
</tr>
<tr>
<td>March – April 2017; base = those experiencing fraud in past 12 months</td>
<td>Friendly Fraud 29% 27% 20% 25%</td>
</tr>
</tbody>
</table>

Figure 8: Distribution of losses by type of fraud for digital goods / channel merchants & firms (2017)
Identity fraud as a percent of losses is particularly high for mid / large eCommerce.

- One reason for this is the nature of being an anonymous remote channel, which has been targeted more aggressively by fraudsters since adoption of EMV chip technology at physical points of sale.

- Secondly, mid / large eCommerce are likely to sell digital goods, which involves fairly quick transactions. This enables “fast fraud”; without real-time transaction analysis, online merchants have more difficulty distinguishing between legitimate and fraudulent customers within the short window required to make the sale. In fact, findings show that mid / large eCommerce merchants which don’t use a real-time transaction tracking solution reported a larger distribution of fraud losses due to identity fraud than those using this type of solution.

Lack of Identity Verification Leads to Customer Friction

Aside from the direct cost of fraud losses, there’s also indirect and opportunity costs stemming from challenges with identity verification. Delayed transaction confirmation can increase customer friction; for the online channel, in which consumers increasingly expect faster results, this heightens the risk that they will leave before finalizing a transaction. Further, declining a legitimate transaction based on incorrect identity verification can result in not just lost revenues, but the loss of potentially positive lifetime value when alienating a prospective customer. Lastly, the lack of identifying legitimate from fraudulent customers can result in higher costs associated with manual reviews.
Findings from this study show that merchants and financial services / lending firms which have challenges with identity verification also struggle with not just delayed transaction confirmation, but also with excessive manual reviews, address verification and risk assessment by region. As shown in Figure 10, this is particularly the case for digital goods sellers and larger merchants / lenders conducting transactions in the mobile channel as well as online. These add to customer friction points.

**Identity Verification Issues Generate Other Friction Points with Digital Goods and Channel Transactions**

<table>
<thead>
<tr>
<th>Delayed Confirmation</th>
<th>Excessive Manual Reviews</th>
<th>Assessing Risk by Region</th>
<th>Address Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>eCommerce selling digital goods online (40%)</td>
<td>Mid / Large retailers selling digital goods in mobile channel (47%)</td>
<td>Large lenders transacting in mobile channel (43%)</td>
<td>Mid / Large eCommerce transacting online (63%)</td>
</tr>
<tr>
<td>Large lenders transacting in mobile channel (32%)</td>
<td>Financial services firms transacting online (40%)</td>
<td>Financial services transacting online (40%)</td>
<td>Lenders transacting online (40%)</td>
</tr>
</tbody>
</table>

Weighted data

Q: Please rank the top 3 challenges related to fraud when serving customers in the Online Channel / Mobile Channel.

March – April 2017; base = those experiencing fraud in past 12 months and using the online or mobile channel for transactions

Figure 10: Online / Mobile channel challenges among those selecting identity verification as a top challenge (2017)
Identity verification and customer friction issues will likely increase as more merchants and financial services / lending firms adopt the mobile channel.

Lending firms and large retailers with an online channel are most likely to be using the mobile channel today (see Figure 11), though for only a small percentage of transactions (see Figure 12).

mCommerce adoption has been slower among eCommerce merchants, though a sizeable portion of mid / large reported anticipated adoption within the next 1 – 2 years. If that plays out, it would follow the trend set by bricks / mortar retailers with an online channel, in which year-over-year growth since 2016 has come from the mid / large segment (see Figure 13).

Figure 11: Percent currently allowing and considering mCommerce (2017)
Merchants and financial services / lending firms recognize the risk of allowing mobile channel transactions. There is real concern that mobile payments and transactions add to the risk of fraud, particularly among financial services and lending firms. This is driven in part by perceptions that security of mobile device transactions is still an unknown.

Mobile Device Security Drives Concerns About Transactions in this Channel

Q: Using a 5-point scale (5 = completely agree), please rate the extent that you agree or disagree with the following statements.

March - April 2017; base = all merchants & firms

### Evolution of mobile channel adds significant risk of fraud
- Retail: 64%
- eCommerce: 56%
- Financial Services: 88%
- Lending: 77%

### Security of mobile device transactions is still unknown
- Retail: 60%
- eCommerce: 50%
- Financial Services: 65%
- Lending: 69%

Figure 14: Percent agreeing with statements about mobile channel transactions (2017)
Ineffective fraud management can lead to more work, wrong decisions and further customer friction.

A number of merchants / firms identified earlier as having higher fraud costs and volumes may not be tracking fraud to the fullest extent. Among mid / large eCommerce (which tends to sell digital goods) and mid / large financial services that conduct most transactions remotely, there is a sizeable portion who do not track fraud by either transaction or channel type. Credit lenders are less likely than mortgage lenders to track prevented fraud by channel.

Among merchants and firms that do track fraud, they are less likely to be tracking it from both perspectives. Fraudsters are experts at leveraging weak points; if they meet resistance through one channel, they will flee to another which is less protected. This has been shown by fraudster migration to online as EMV chip technology makes it more difficult for them to succeed in-store. It should be expected, then, that improved security with certain payment types will make fraudsters seek other, less secure payment methods. Since the digital channels and sale of digital goods is a primary target of fraudsters, the lack of tracking successful fraud by both transaction and channel type can weaken merchants’ / firms’ ability to manage the ongoing movement of fraud attacks.

Figure 15: Percent tracking prevented and success fraud by transaction and channel type (2017)
This isn’t to suggest that these mid / larger digitally-focused merchants / firms aren’t fighting fraud. On the contrary; they are more likely to be using an automated flagging system and multiple risk mitigation solutions than others.

The exception is with mid / large financial services firms that conduct most transactions online; they are less likely to combine an automated flagging system with a fraud mitigation solution, though still use multiple fraud solutions.

Within lending, mortgage lenders tend to use more solutions on average (6.2) than credit lenders (4.1), including advanced identity and transaction verification solutions.
While using more fraud mitigation solutions, larger digitally-focused merchants and firms may not be doing so in a way that can optimize fraud mitigation. With identity verification being a leading challenge that further impacts other fraud-related issues, the use of advanced identity authentication solutions among mid/large digital goods merchants and digital financial services/lending firms is somewhat limited (see Figure 17).

As noted earlier, the use of real-time transaction tracking is also limited, which weakens digital-goods sellers’ ability to catch “fast fraud”. Mid/Large digital goods retailers and large digital lenders tend to allow mobile transactions, yet the use of geolocation and device ID/fingerprinting solutions that support mCommerce fraud management are not heavily used. And lastly, each of these segments continues to experience higher volumes and cost of fraud.

Figure 17: Percent using specific fraud mitigation solutions (2017)
Plus, larger digitally-focused merchants and firms are dealing with the cost and inefficiency of excessive manual reviews.

Mid / Large retailers selling digital goods and financial services / lending firms that conduct most transactions online send a sizeable portion of auto flagged transactions for manual review; credit lenders send significantly more transactions for manual review (44%) than mortgage lenders (28%). For digital merchants / firms, this coincides with limited use of real-time transaction and advanced identity authentication solutions and having a sizeable portion of their fraud mitigation spend dedicated to manual reviews (one-quarter or more).

**Manual Reviews Absorb One-Quarter or More of Fraud Mitigation Spend**

- Weighted data
- Q: What is the percentage distribution of mitigation costs across the following in the past 12 months?

March - April 2017; base = merchants / firms that spent >$0 on fraud mitigation

- Cost of Fraud Mitigation Solutions
  - 48%
  - 46%
  - 49%
  - 40%

- Cost of Manual Reviews
  - 32%
  - 26%
  - 24%
  - 26%

- Cost of Physical Security
  - 20%
  - 22%
  - 27%
  - 30%

**Figure 18: Distribution of fraud mitigation budget spend (2017)**

**Of Flagged Transactions, Just Under Half are Sent for Manual Review by Digitally-Focused Merchants and Firms**

- Weighted data
- Q: Of all transactions your company flagged as potentially fraudulent in the past 12 months, what percent was sent for manual review?

March - April 2017; base = merchants / firms with an automated flagging system

- Of Transactions Flagged by Automated System, % Sent for Manual Review:
  - 43%
  - 46%
  - 44%
  - 38%

**Figure 19: Percent of flagged transactions sent for manual review (2017)**
It’s not just about the number of risk mitigation solutions, but rather the right ones based on layering identity and transaction-based protection that can reduce successful fraud attempts.

Mid / Large digital goods retailers and larger digital financial services / lending firms actively fight fraud yet still struggle with its negative effects. While more efficient tracking of it will help, there is also the need to layer the right combination of solutions.

Survey findings show that companies in these sectors which invest in a multi-layered approach that includes advanced identity and fraud transaction verification / authentication experience a smaller percentage of successful fraud attempts than others which do not layer in this manner (see Figure 20).

### Percent of Successful Fraud Declines with a Multi-Layered Solutions Approach

**Weighted data**

Q: Does your company use any of the following fraud mitigation solutions? In a typical month, approximately how many fraudulent transactions are successfully completed (not prevented) at your company?

**March - April 2017; base = all merchants**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Core</td>
<td>Basic</td>
<td>Layering of Advanced ID Solutions</td>
<td>Layering of Transaction Risk Assessment Solutions</td>
</tr>
<tr>
<td>&amp; Limited Layering</td>
<td>Limited Layering</td>
<td>Layering of Advanced ID Solutions</td>
<td>Layering of Transaction Risk Assessment Solutions</td>
</tr>
<tr>
<td>&amp; Multi-Layered</td>
<td>Multi-Layered</td>
<td>Layering of Advanced ID Solutions</td>
<td>Layering of Transaction Risk Assessment Solutions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Layers of Protection</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Core</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Layering of Advanced ID Solutions</td>
<td>Some</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Layering of Transaction Risk Assessment Solutions</td>
<td>Some</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 20: Percent of successful fraud attempts by solutions layering (2017)**
A multi-layered solution approach can also reduce the cost of fraud.

Survey findings show that companies in these sectors which invest in a multi-layered approach of advanced identity and fraud transaction verification / authentication solutions realize lower costs of fraud (see Figure 21).

### The LexisNexis Fraud Multiplier℠ and Fraud Costs as a Percent of Revenues Decrease with a Multi-Layered Solutions Approach

<table>
<thead>
<tr>
<th>Layers of Protection</th>
<th>Basic</th>
<th>Limited Layering</th>
<th>Multi-Layered</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic Core</strong> - CVV, PIN / Signature,</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Check Verification, Browser Malware,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address Verification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Layering of Advanced ID Solutions</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device / ID Fingerprinting, Geolocation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication by Quizzes</td>
<td></td>
<td>Some</td>
<td></td>
</tr>
<tr>
<td>Authentication by Challenge Questions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer Profile Database</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Layering of Transaction Risk Assessment Solutions</strong></td>
<td></td>
<td>Some</td>
<td>✓</td>
</tr>
<tr>
<td>Automated Transaction Scoring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real-Time Transaction Tracking</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transaction Verification, Rules-Based Filters</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication of Transaction by 3D Tools</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Avg. Fraud Cost as a Percent of Revenues by Number &amp; Layering of Fraud Mitigation Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use up to 4 Solutions (Basic)</td>
</tr>
<tr>
<td>Use 3 - 7 Solutions (Limited Layering)</td>
</tr>
<tr>
<td>Use 5 - 10 Solutions (Multi-Layered)</td>
</tr>
<tr>
<td>Retail</td>
</tr>
<tr>
<td>eCommerce</td>
</tr>
<tr>
<td>Financial Services</td>
</tr>
<tr>
<td>Lending</td>
</tr>
</tbody>
</table>

**March - April 2017; base = all merchants**

Q: In thinking about the total fraud losses suffered by your company, please indicate the distribution across chargebacks, fees and replacement costs. What is the approximate dollar value or percent of total revenue of your company’s total fraud losses during the past 12 months?

The LexisNexis Fraud Multiplier℠ and Fraud Costs as a Percent of Revenues Decrease with a Multi-Layered Solutions Approach

**Figure 21:** Fraud costs by solutions layering (2017)
LexisNexis® Risk Solutions can help.

LexisNexis® Risk Solutions provides powerful identity verification, identity authentication and transaction scoring tools to combat fraud. These solutions can help:

- Increase sales
- Reduce manual reviews
- Minimize fraud and chargebacks

LexisNexis® Risk Solutions leverages the largest, broadest, deepest, and most reliable repository of identity information available. With more than 45 billion records from over 13,000 sources and more than 3 million record updates per day, nothing else comes close. Combining unmatched information assets with unique data linking, and advanced analytics, LexisNexis® Risk Solutions helps uncover the information you need for a complete picture of individuals and companies you do business with.

Customer-Focused Solutions Relevant to Remote Channel Needs Include:

**Identity Verification**
- Validate name, address and phone information
- Reconcile name variations, duplicates, multiple addresses, and myriad other inconsistencies and linkages
- Perform global identity checks with seamless integration and reporting capabilities

**Transaction Risk Scoring**
- Identify risks associated with bill-to and ship-to identities with a single numeric risk score
- Quickly detect fraud patterns and isolate high-risk transactions
- Resolve false-positive and Address Verification Systems failure

**Manual Research Support**
- Access billions of data records on consumers and businesses
- Discover linkages between people, businesses and assets
- Leverage specialized tools for due diligence, account management and compliance

**Identity Authentication**
- Authenticate identities on the spot using knowledge-based quizzes
- Dynamically adjust security level to suit risk scenarios
- Receive real-time pass / fail results
Methodology

In 2017, LexisNexis® Risk Solutions retained KS&R Inc., a global market research firm, to conduct the ninth annual comprehensive research study on U.S. retail merchant fraud. The inaugural editions of the True Cost of Fraud℠ Studies for the eCommerce, financial services and lending sectors were conducted in parallel by KS&R, Inc. as well.

The methodology of these studies was as follows:

- A comprehensive survey of 1,196 risk and fraud executives across retail, eCommerce, financial services and lending organizations deployed during March – April 2017. The number of completed surveys by sector were as follows:
  - 653 from retail organizations;
  - 190 from eCommerce organizations that earn a majority of their revenue (80%+) through online and / or mobile channels;
  - 185 from financial services companies; and
  - 168 from lending institutions.
- All surveys were conducted online via a US business panel. LexisNexis was not identified as the sponsor of the study.
- Respondents represented all channels (physical point of transaction, online, mobile), company sizes, and payment methods in order to be consistent with previous study waves.
- The overall margin of sampling error at the Total Level (all organizations) is +/- 1.45% at the 95 percent confidence level. The sampling error is larger for subsets of respondents.
- Data reflects the US population for these 4 sectors based on weighting to U.S. Economic Census. Weighting to representativeness was based on two dimensions, consistent with previous waves, including
  - Size of merchant/firm by number of employees; and
  - Industry segment.
For more information

Call: 800.869.0751
Visit: http://www.lexisnexis.com/risk

About LexisNexis® Risk Solutions
LexisNexis® Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, Risk Solutions provides products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy.

LexisNexis® Risk Solutions is part of RELX Group, plc, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

About KS&R, Inc.
KS&R is a multi-award winning supplier of global market research. The firm works closely with clients in a range of industries to improve market position and increase returns on marketing investments. The views expressed by KS&R are not necessarily those of LexisNexis® Risk Solutions. The opinions expressed in this paper are those of survey respondents and do not necessarily reflect the positions of LexisNexis® Risk Solutions.

LexisNexis® Risk Solutions 2017 True Cost of Fraud℠ Study