LexisNexis® Risk Solutions 2018 True Cost of Fraud℠ Study

August 2018

LexisNexis® RISK SOLUTIONS

The LexisNexis® Risk Solutions 2018 True Cost of Fraud℠ Study helps merchants (retail and online/mobile), financial services companies, and lenders 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, mobile, and international sectors.
- 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.

How do I grow my business, navigate and manage the cost of fraud while strengthening customer trust and loyalty?

The study included a comprehensive survey of 1,264 risk and fraud executives during March & April 2018, broken out as follows:

- **703** from retail organizations
- **200** from e/m-Commerce organizations that earn a majority of their revenue (80%+) through online and/or mobile channels
- **175** from financial services companies
- **186** from lending institutions

Surveys were conducted online.

LexisNexis® Risk Solutions was not identified as the sponsor of the study.

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
  - Lost or stolen merchandise, as well as redistribution costs associated with redelivering purchased items
- This research covers consumer-facing fraud methods
  - Does not include insider fraud or employee fraud
- The LexisNexis Fraud Multiplier℠ cost
  - Estimates the total amount of loss a merchant occurs based on the actual dollar value of a fraudulent transaction

Segments by Industry Definitions

Retail

Mid/Large Physical Goods only

Earns $10 million in annual revenues; sells physical goods only.

Mid/Large Digital and Physical Goods

Earns $10 million in annual revenues; sells digital goods only, or digital and physical goods.

E-Commerce

Mid/Large Physical Goods only

Earns $10 million in annual revenues; sells physical goods only.

Mid/Large Digital and Physical Goods

Earns $10 million in annual revenues; sells digital goods only, or digital and physical goods.

Financial Services

Mid/Large Some or No Digital Transactions

Earns $10 million in annual revenues; less than 50% through the online and/or mobile channels.

Mid/Large Primarily Digital Transactions

Earns $10 million in annual revenues; 50% or more through the online and/or mobile channels.

Lending

Large Some or No Digital Transactions

Less than 50% of revenue through the online and/or mobile channels.

Large Primarily Digital Transactions

More than 50% of revenue through the online and/or mobile channels.

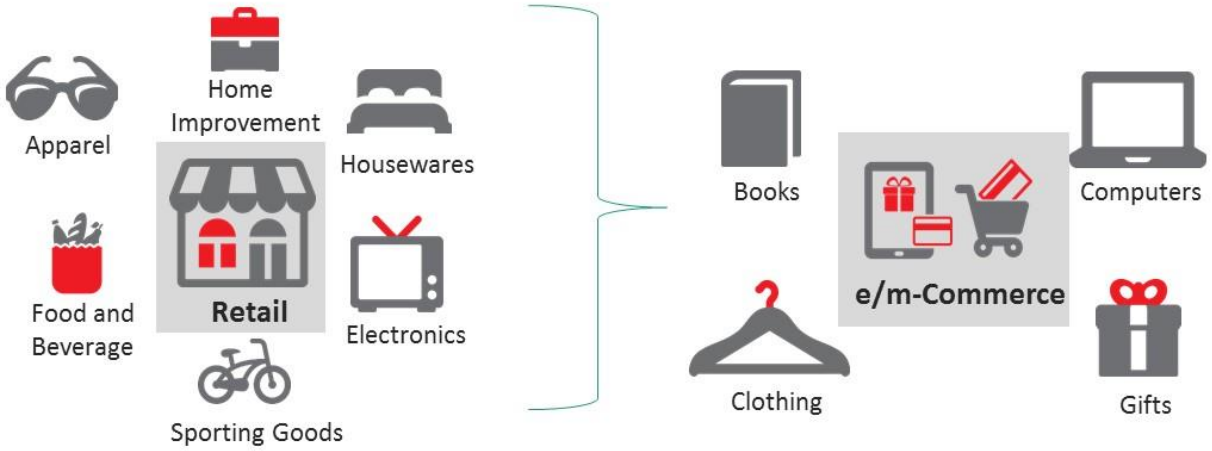
m-Commerce

Allows transactions through mobile web browser, mobile apps, or bill-to-mobile phone.

LexisNexis® RISK SOLUTIONS

Company Types by Industry

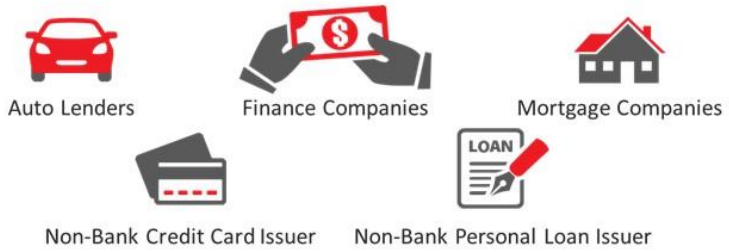
Retail & e-Commerce companies operate across various industries including:



Financial Services Companies Include:

- Retail/Commercial Banks
- Credit Unions
- Investments
- Trusts
- Wealth Management

Lending Institutions Include:



LexisNexis® RISK SOLUTIONS

Executive Summary: Key Findings

LexisNexis®
RISK SOLUTIONS

Key Findings

1

Sizeable fraud continues to occur across industries, though it has grown somewhat more for Financial Services and Lending.

- The average cost of fraud has grown 9.3% for Financial Services firms and 8.1% for Lending firms since 2017.
- Every $1 of fraud now costs these firms $2.92 and $3.05 respectively.
- Though it didn't grow as much as in the past, the cost for Retail firms is also getting closer to the $3 mark. e-Commerce costs grew the least, but still comes in at $2.56.
- Additionally, the level of fraud as a percentage of revenues has increased, particularly for Financial Services firms, which are really starting to feel the effects of "fast fraud".

2

And fraud consistently impacts digital, either whether it is the channel or type of good sold.

- Every $1 of fraud costs mid/large firms selling digital goods or conducting digital transactions between $3.00 to $3.37, which is up from 2017 across the board.
- For e-Commerce merchants selling digital goods in particular, a surge in fraudulent transactions, fraud associated with alternative transaction methods, and increased botnet activity push costs higher.
- Those in Financial Services and Lending continue to experience the risk that the anonymous remote channel add to financial transactions.

3

The mobile channel has grown for some industries and contributes even more to increased fraud risks.

- m-Commerce growth continues to be driven by larger firms selling digital goods or transacting digitally. Mid/Large Financial Services firms conducting digital transactions experienced the most growth since 2017, with m-Commerce usage increasing by 94% over last year.
- The LexisNexis Fraud Multiplier℠ is even higher for firms selling digital goods or transacting through the mobile channel, increasing across sectors since 2017 (costs range from $3.26 - $3.51 per $1 of fraud).
- Less secure web browsers and 3rd party and branded apps account for a significant portion of fraud losses, but firms offer them in the hopes of optimizing the customer experience and, in turn, facilitating customer acquisition/retention and revenue growth.

Key Findings (cont.)

4

Adding international transactions, within the online and/or mobile channels, further increases fraud risks and costs for some.

- This impacts Large Digital Lenders transacting internationally, as well as Mid/Large Financial Services Firms using m-Commerce and transacting internationally ($3.59 and $3.38 for every $1 of fraud respectively).
- Asia accounts for a bulk of the international fraud losses for both sectors (57% and 40%).
- This is likely related to significant fraud occurring through alternative and other non-traditional methods for Lenders and via bill-to-mobile phone for Financial Services, combined with challenges related to assessment of fraud risk by country/region and lack of specialized international tools.

5

Identity fraud and verification remain key issues for firms selling digital goods or transacting digitally.

- Mid/Large Financial Services and Large Lending firms, in particular, continue to fall victim to these types of fraud (49% and 54% of fraud losses respectively).
- Identify verification remains a top challenge for these sectors, and causes issues with manual reviews and delayed transaction confirmation.
- Mid/Large Retailers selling digital goods and using m-Commerce, and Mid/Large e-Commerce merchants selling digital goods are challenged by minimizing customer friction while verifying identities, especially with the use of newer payment methods.

6

Tracking of fraud has increased, but for those hit harder by fraud, it still isn't optimal.

- Segments with the highest fraud costs (M/L Retailers selling digital goods and using m-Comm, M/L e-Commerce merchants using m-Comm, M/L Financial Services transacting internationally and using m-Comm, and Lg Digital Creditors), to a large degree, track fraud costs by both channel and payment/transaction method.
- And, they are likely to be tracking where prevented and successful fraud occurs, BUT not consistently or holistically. Many are **not** tracking prevented and successful fraud by both channel and transaction type, which leaves multi-channel firms open to risk as fraudsters continuously test for weak entry points.
- Combined fraud solution and automated alert system usage remains high or has increased among these at-risk segments, but this doesn't seem to improve the accuracy or efficiency of the fraud identification process (volume of manual reviews and false positives hasn't decreased).

Key Findings (cont.)

7

A number of higher risk firms are using fraud prevention solutions, but not necessarily the right combination to successfully prevent fraud.

- The average number of reported solutions used has increased or is on par with 2017 for the aforementioned segments that are hit hardest by fraud.
- But while solutions continue be the major component of fraud mitigation spend for these segments, a sizeable portion is still budgeted for manual reviews.
- The use of advanced identity and transaction verification solutions remains fairly limited across segment (many of these is still at or under 50% of the market).
- This correlates highly with higher fraud costs.

8

Findings show that using the right combination of tools is crucial to combatting fraud risks and cost.

- Survey findings show that those who layer solutions by identity authentication and transaction/ identity verification experience fewer fraud costs.

LexisNexis® RISK SOLUTIONS

1

Sizeable fraud continues to occur across industries, though it has grown somewhat more for Financial Services and Lending.

LexisNexis®
RISK SOLUTIONS

The cost of fraud continues to be high across study industries, but has grown somewhat more since last year for Financial Services and Lending firms.

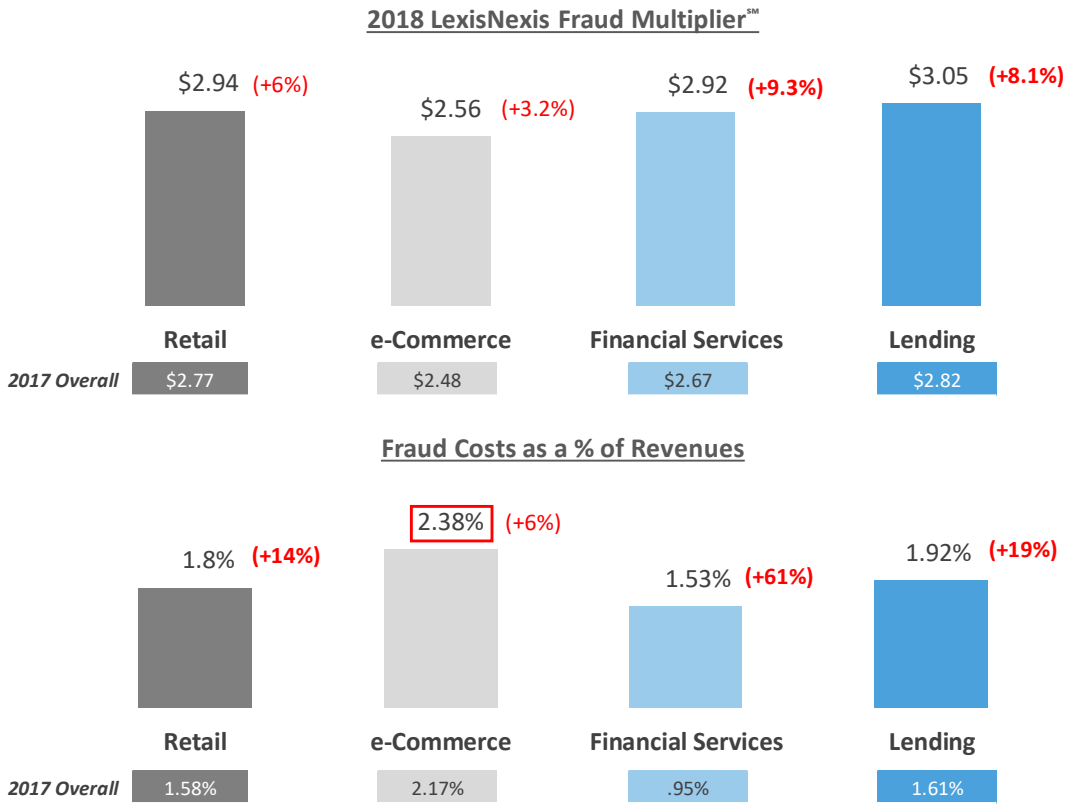
The average cost of fraud has grown 9.3% for Financial Services firms and 8.1% for Lending firms since 2017.

Every $1 of fraud now costs these firms $2.92 and $3.05 respectively.

Though it didn't grow as much as it has in the past, the cost for Retail firms is also getting closer to the $3 mark.

e-Commerce costs grew the least, but costs are still considerable at $2.56 for every $1 of fraud.

Additionally, the level of fraud as a percentage of revenues has increased, particularly for Financial Services firms, which are starting to feel the effects of "fast fraud" and its associated costs (as shown in next section).



Q10: What is the approximate value of your company's total fraud losses over the past 12 months, as a % of total revenues?

☐ Significantly different from all or most industry segments within response category at the 95% Confidence Interval

LexisNexis® RISK SOLUTIONS

2

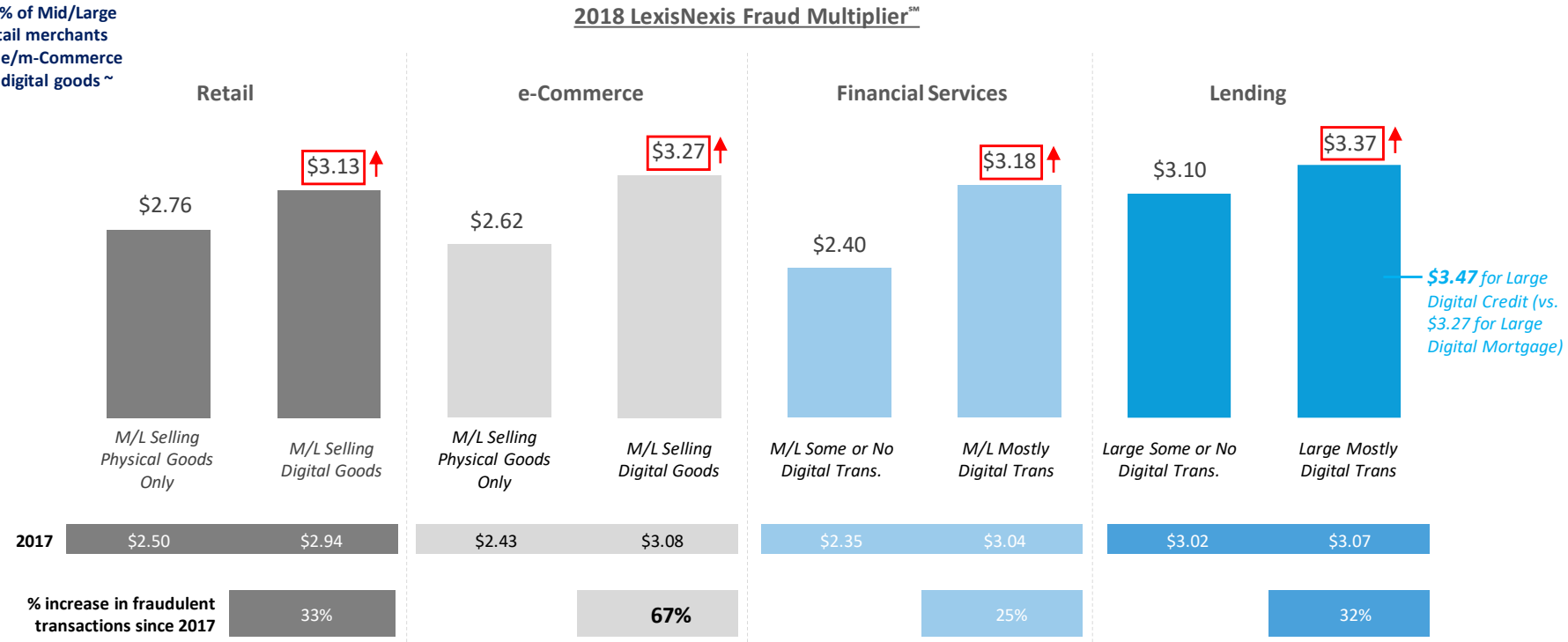
And fraud consistently impacts digital, either whether it is the channel or type of good sold.

LexisNexis®
RISK SOLUTIONS

The cost of fraud is even higher for organizations that are digital – Retail and e-Commerce merchants selling digital goods or Financial Services and Lending firms conducting digital transactions.

Though costs are similar across sectors, Large Digital Lending firms experienced the largest increase in fraud costs over the past year. Not only have they seen a rise in the number of fraudulent transactions, but the costs associated with them includes not only the face value for which the firm is held liable, but also fees/interest incurred during application/underwriting/processing stages, fines and legal fees, labor investigation, and external recovery expenses. This impacts Large Digital *Creditors* in particular, where approval procedures are less stringent than for Mortgage products.

~ 52% of Mid/Large Retail merchants with e/m-Commerce sell digital goods ~



LexisNexis® RISK SOLUTIONS

Q10: What is the approximate value of your company's total fraud losses over the past 12 months, as a % of total revenues?

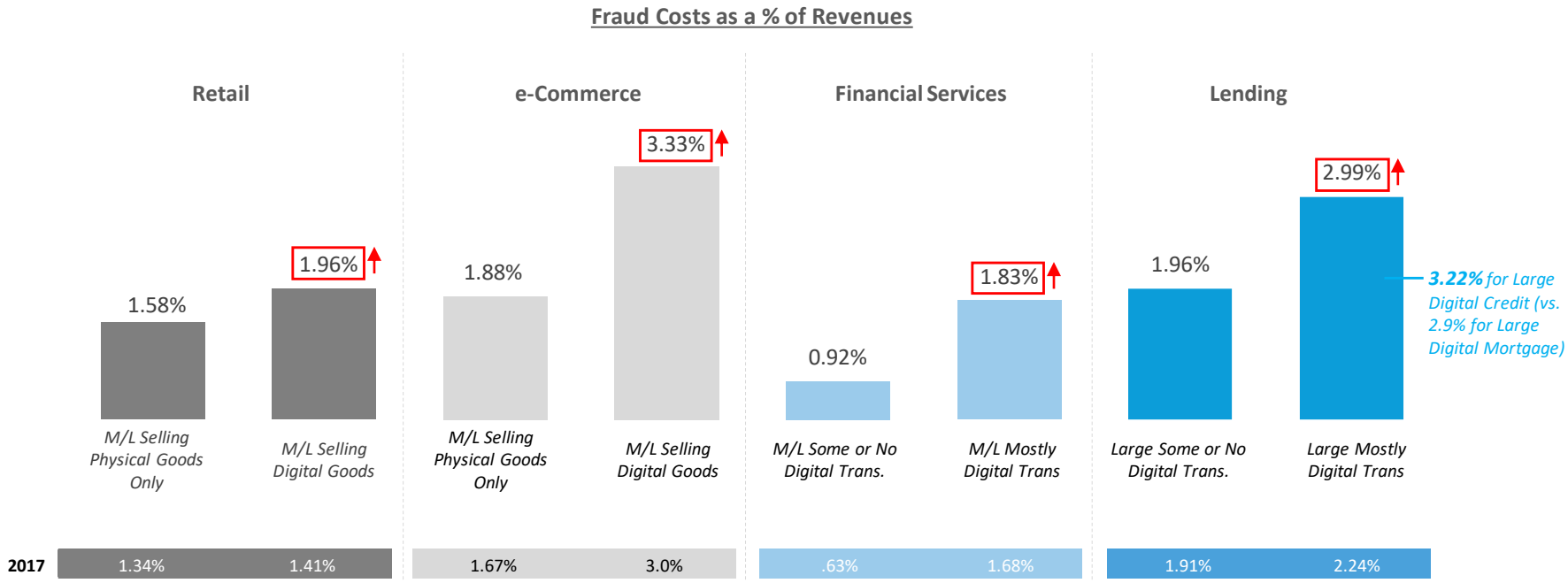
☐ Significantly different from other segment within industry category at the 95% Confidence Interval

↑ Significantly different from 2017 within segment at the 95% Confidence Interval

And this impacts the bottom line, with fraud costs as a percentage of revenue increasing across sectors for these segments.

Mid/Large e-Commerce merchants selling digital goods continue to lose a higher percentage of revenues to fraud costs than other sectors, but are followed closely by Large Digital Lenders.

That said, fraud still has a sizeable impact on Retail and Financial Services firms dealing with digital goods or transactions.



LexisNexis® RISK SOLUTIONS

Q10: What is the approximate value of your company's total fraud losses over the past 12 months, as a % of total revenues?
Q24: In a typical month, approximately how many fraudulent transactions are successfully completed?

☐ Significantly different from other segment within industry category at the 95% Confidence Interval

↑ Significantly different from 2017 within segment at the 95% Confidence Interval

For Mid/Large e-Commerce merchants selling digital goods in particular, there is a relationship between fraud and continued botnet activity and usage of non-traditional payment methods.

While credit card transactions are the single largest method for transactions and losses, a sizeable portion of digital goods transactions also occur through a variety of non-traditional methods (37%, comprised of third-party mobile wallets, checkout by Amazon, e-gift cards, virtual currency and mobile apps).

This is coupled with larger digital goods merchants assigning a portion of fraud costs to these other transaction methods, at a time of increased mobile app fraud related to heightened botnet activity.[1]

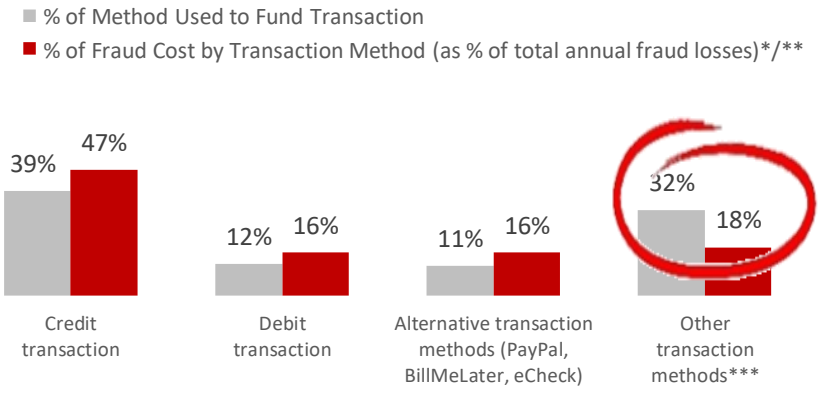
E-COMMERCE – Mid/Large ($10M+) Merchants Selling Digital Goods

~ 67% of Mid/Large e-Commerce merchants sell digital goods ~

Digital Products Sold – Most Mentioned

- Cloud-based applications
- Digital subscriptions
- Mobile apps
- Downloadable software
- Online gaming
- Music streaming/downloading

Transaction Methods/Fraud



73% agree that combatting automated botnet fraud activity is overwhelming

86% agree that selling digital goods increases risk of fraud

[1] https://www.appsflyer.com/resources/the-state-of-mobile-fraud-q1-2018/

LexisNexis® RISK SOLUTIONS

**CAUTION: Small sample size; use directionally, asked only of those who track fraud and then further split into size segments*

*** % can add to more than 100% since answers based on using a channel, in which case the base size changes per channel*

D1b: What type of digital goods are sold by your company?

Q3: Please indicate the percentage for each method used (over the past 12 months) to fund transactions or disburse funds.

Q18: Please indicate the percentage distribution of the payment methods used to commit fraud against your company.

***Company-branded mobile app, gift cards, virtual currency, mobile wallets, checkout by Amazon, social media payments

3

The mobile channel has grown for some industries and contributes to increased fraud risks.

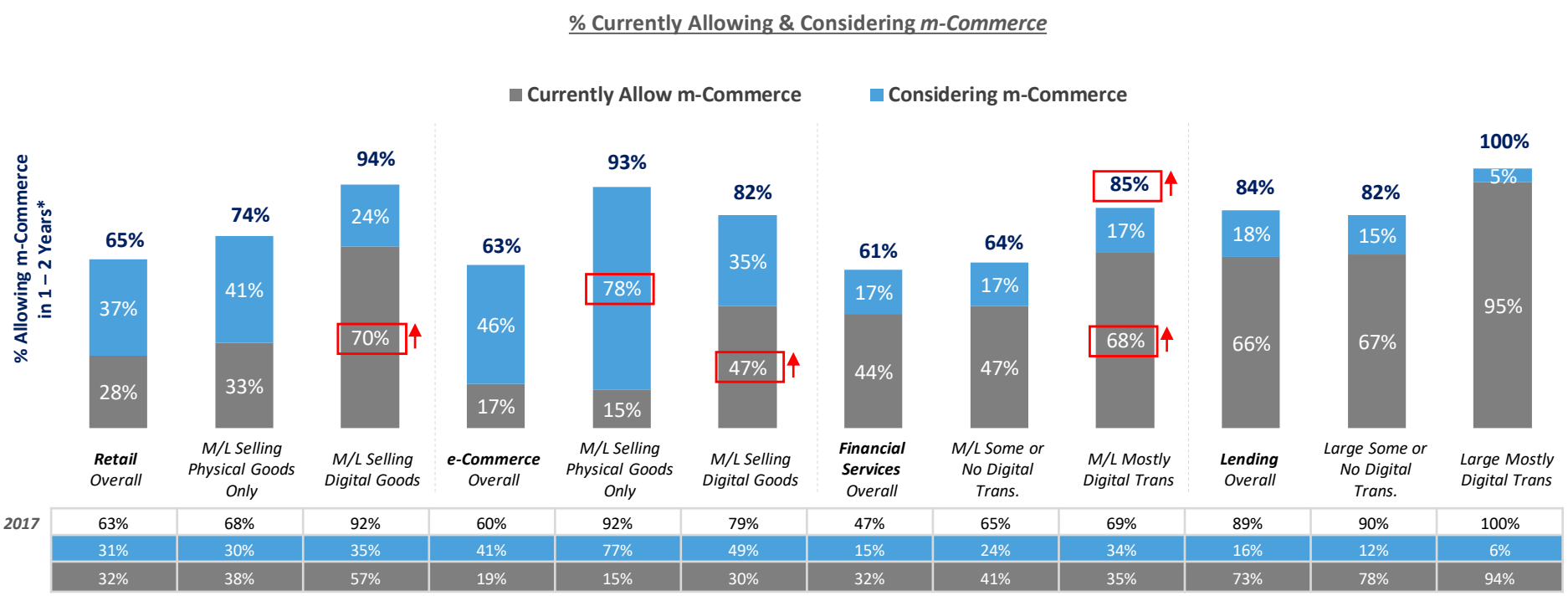
LexisNexis®
RISK SOLUTIONS

As predicted in previous waves of this study, m-Commerce growth continues to be driven by larger firms selling digital goods or transacting digitally.

Mid/Large Financial Services firms conducting digital transactions experienced tremendous growth, with m-Commerce usage increasing by 94% over last year.

Though still emerging among e-Commerce firms, m-Commerce usage among these mid/large merchants selling digital goods grew well over 50% compared to a year ago. Mid/Large Retail merchants selling digital goods continue their trend of year-over-year double-digit adoption of m-Commerce since at least 2016.

Large Lenders conducting digital transactions continue to be synonymous with mobile.



2017												
	63%	68%	92%	60%	92%	79%	47%	65%	69%	89%	90%	100%
	31%	30%	35%	41%	77%	49%	15%	24%	34%	16%	12%	6%
	32%	38%	57%	19%	15%	30%	32%	41%	35%	73%	78%	94%

*Not all who say "likely in next 12 months" may actually be able to do so in that timeline. Budgets and other unforeseen factors could delay adoption.

Q4: Please indicate the percentage of transactions completed (over the past 12 months) for each of the following payment channels currently accepted by your company.
Q6: Is your company considering accepting payments by mobile device over the next 12 months?

☐ Significantly different from other segment within industry category at the 95% Confidence Interval

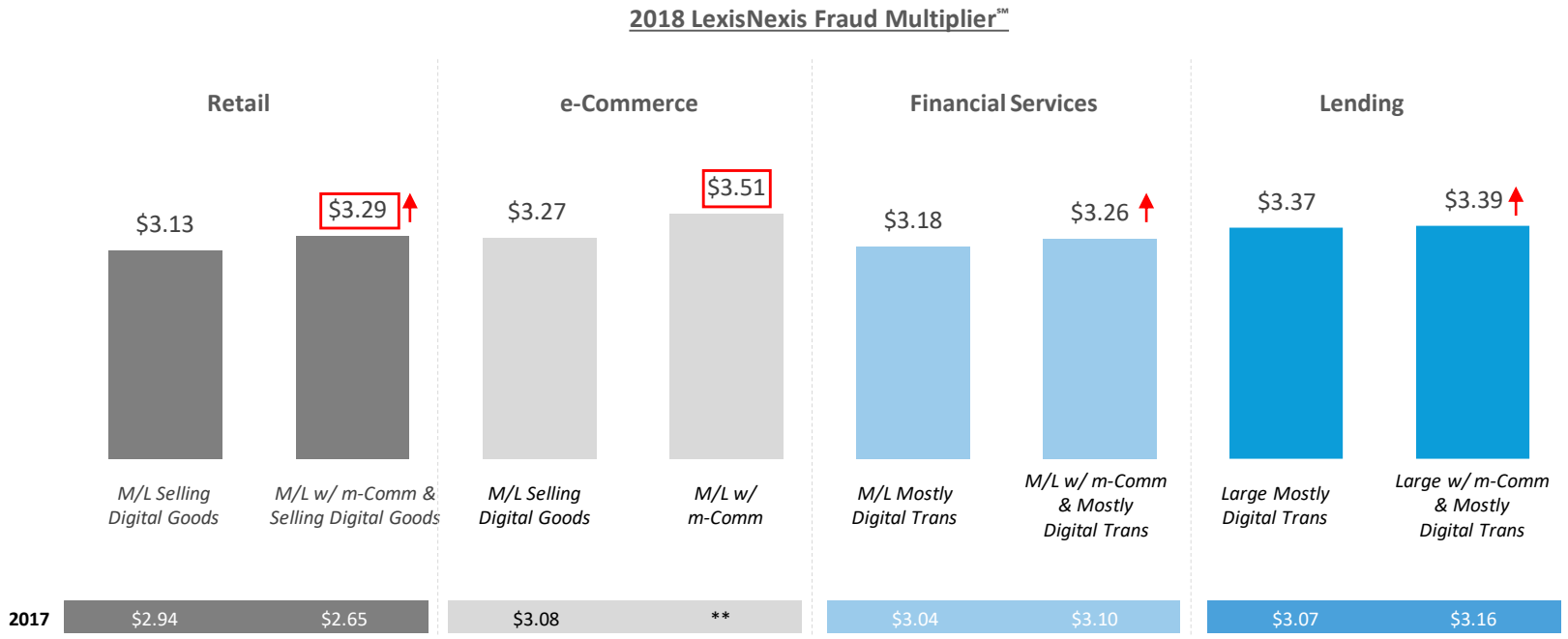
↑ Significantly different from 2017 within segment at the 95% Confidence Interval

LexisNexis® RISK SOLUTIONS

But m-Commerce growth=fraud. The LexisNexis Fraud Multiplier℠ is even higher for firms selling digital goods and/or transacting through the mobile channel.

The cost of fraud has increased significantly across sectors, even among Large Lenders conducting digital transactions, where a majority has been doing sizeable business in the mobile space for several years.

This continues to demonstrate how the combination of digital goods and/or multiple remote channels and increased fraud targeting of mobile apps is impacting fraud risks and costs.



** m-Commerce incidence too low for Mid/Large m-Commerce in 2017; base size too small to show comparison findings

Q10: What is the approximate value of your company's total fraud losses over the past 12 months, as a % of total revenues?

☐ Significantly different from other segment within industry category at the 95% Confidence Interval

↑ Significantly different from 2017 within segment at the 95% Confidence Interval

LexisNexis® RISK SOLUTIONS

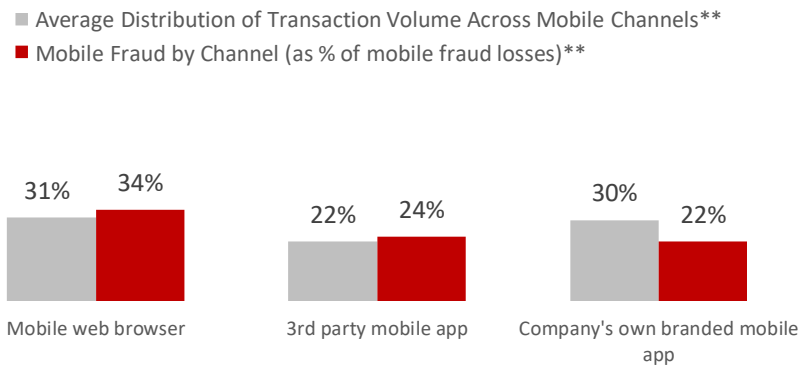
Mid/Large e-Commerce merchants are being hit hard by fraud, not only through the less secure mobile web browser, but through 3rd party mobile apps as well.

Higher fraud volumes among these merchants coincides with **reported increases in mobile app fraud**, particularly affecting shopping and gaming, and related to increased "click flooding" and botnet activity.[1]

This impacts Mid/Large Retailers selling digital goods as well, though their fraud losses tend to be more distributed across the various mobile channels.

RETAIL – Mid/Large ($10M+) w/mCommerce & Selling Digital Goods

Mobile Channel Transaction/Fraud Volume

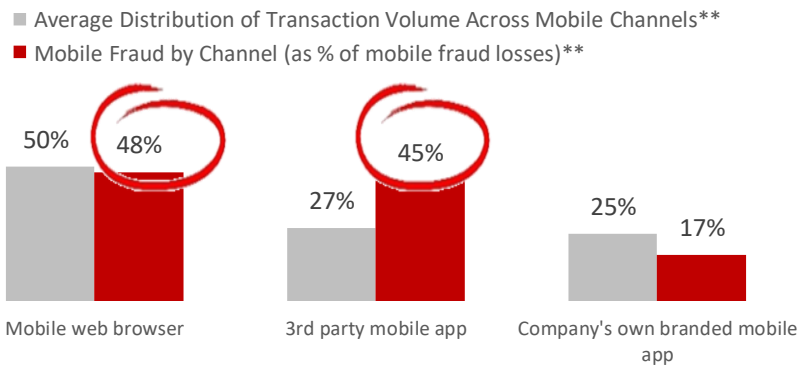


85% agree the evolution of mobile payment & channel adds significant fraud risk

65% agree that security of mobile transactions still unknown

E-COMMERCE – Mid/Large ($10M+) w/mCommerce*

Mobile Channel Transaction/Fraud Volume



64% agree the evolution of mobile payment & channel adds significant fraud risk

63% agree that security of mobile transactions still unknown

[1] http://www.businessofapps.com/mobile-app-fraud-has-increased-by-30-already-this-year; https://www.mediapost.com/publications/article/316976/mobile-app-ad-fraud-up-30.html

LexisNexis® RISK SOLUTIONS

Q4: what is the distribution of transactions through each of the mobile channels your company uses/accepts?
Q17: Please indicate the distribution of fraud across the various mobile channels you use/accept.

**CAUTION: Small sample size; use directionally, asked only of those who track fraud and then further split into size segments*
*** % can add to more than 100% since answers based on using a channel, in which case the base size changes per channel*

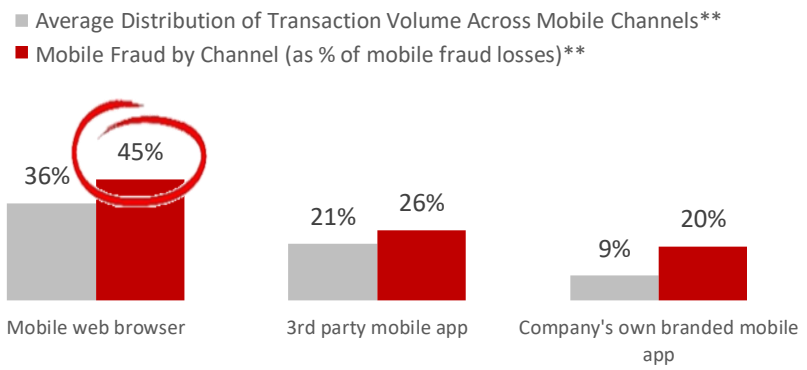
The mobile web browser is also a significant issue for Mid/Large Financial Services firms. They experience nearly half of their fraud losses through this channel.

3rd party and branded mobile app fraud is an added risk on top of this.

For the Lending sector, the mobile channel is problematic in particular for Large Creditors. While fraud volumes are similar through the mobile web browser for Large Creditors and Mortgagees, losses through 3rd party and branded mobile apps are significantly higher for Large Creditors.

FINANCIAL SERVICES – Mid/Large ($10M+) Digital

Mobile Channel Transaction/Fraud Volume

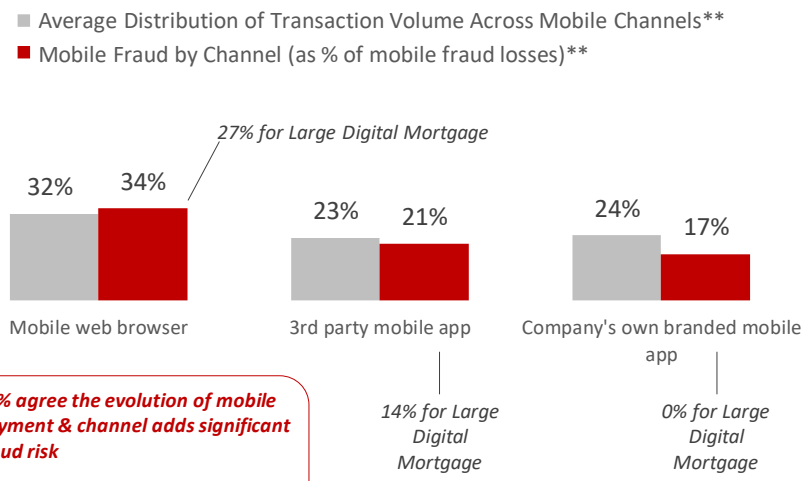


73% agree the evolution of mobile payment & channel adds significant fraud risk

61% agree that security of mobile transactions still unknown

LENDING – Large ($50M+) Digital Credit*

Mobile Channel Transaction/Fraud Volume



94% agree the evolution of mobile payment & channel adds significant fraud risk

76% agree that security of mobile transactions still unknown

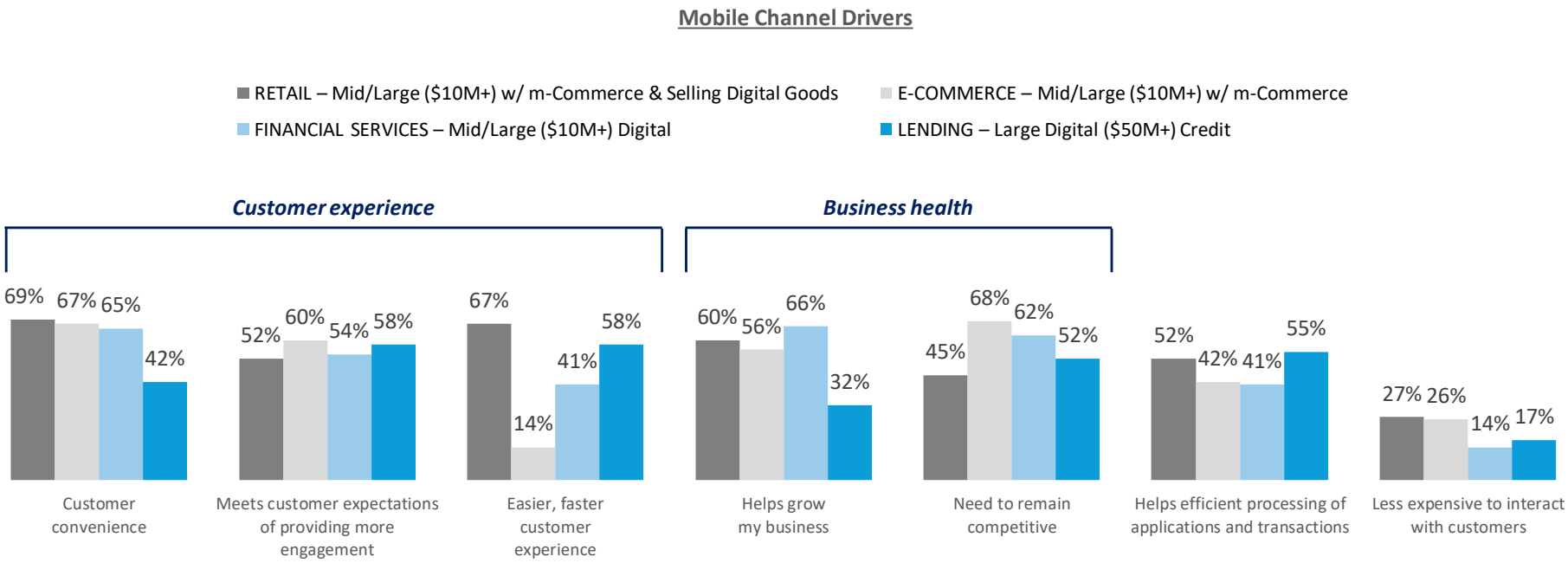
LexisNexis® RISK SOLUTIONS

**CAUTION: Small sample size; use directionally, asked only of those who track fraud and then further split into size segments*
*** % can add to more than 100% since answers based on using a channel, in which case the base size changes per channel*
Q4: what is the distribution of transactions through each of the mobile channels your company uses/accepts?
Q17: Please indicate the distribution of fraud across the various mobile channels you use/accept.

So why risk offering the mobile channel as a transaction option? It optimizes the customer experience, which can lead to customer acquisition/retention and revenue growth.

Where drivers differ, Mid/Large Retail merchants selling digital goods and Large Digital Creditors are somewhat more concerned than others with the efficiency of processing applications and transactions.

And reduced cost of transacting tends to be more of a driver for those in Retail/e-Commerce.



LexisNexis® RISK SOLUTIONS

Q5: What were the reasons your company decided to start accepting mobile account origination or transactions?

4

Adding international transactions, within the online and/or mobile channels, further increases fraud risks and costs for some.

LexisNexis®
RISK SOLUTIONS

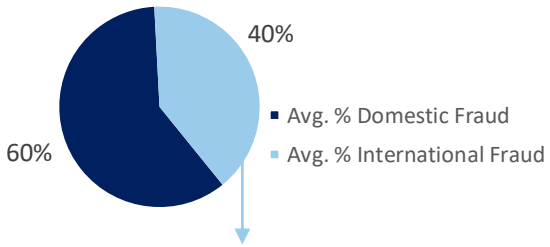
Fraud costs are even higher for Mid/Large Financial Services firms that use m-Commerce and transact internationally -- $3.38 for $1 of fraud.

These firms attribute 40% of their fraud losses to international transactions. Assessment of fraud risk by country/region increased significantly since 2017 as a top mobile fraud challenge and seems to be most challenging in Asia, Africa, and Russia, which account for a majority of theses international fraud losses.

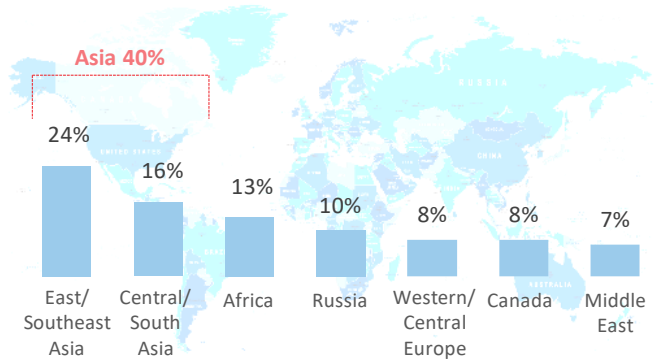
While the mobile web browser continues to experience the largest share of fraud, and fraud is sizeable among mobile apps, bill-to-mobile phone fraud becomes much more of a factor in international fraud (than compared to domestic).

FINANCIAL SERVICES – Mid/Large ($10M+) w/ m-Commerce & International

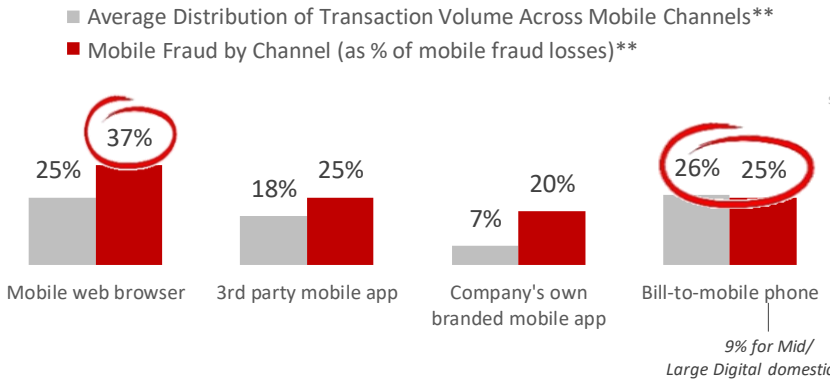
Fraud Losses



% Distribution of International Fraud Losses by Country/Region

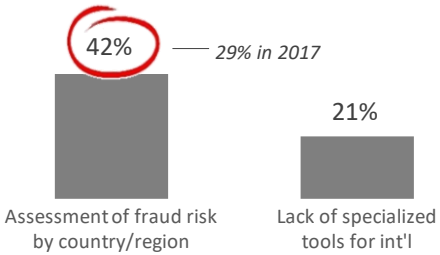


Mobile Channel Transaction/Fraud Volume

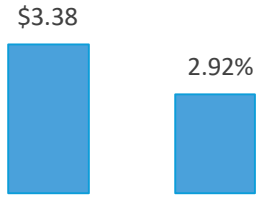


***Company-branded mobile app, gift cards, virtual currency, mobile wallets, checkout by Amazon, social media payments

Top Ranked Mobile Fraud Challenges



2018 LexisNexis Fraud Multiplier℠/ Fraud Costs as % of Revenues



LexisNexis® RISK SOLUTIONS

*** % can add to more than 100% since answers based on using a channel, in which case the base size changes per channel*

Q13: Please indicate the percent of fraud costs generated through domestic transactions compared to international transactions in the last 12 months.
Q14c: Please allocate 100 points across the following to indicate the distribution that each region represents of your total international fraud costs.
Q3: Please indicate the percentage for each method used (over the past 12 months) to fund transactions or disburse funds.
Q18: Please indicate the percentage distribution of the payment methods used to commit fraud against your company.

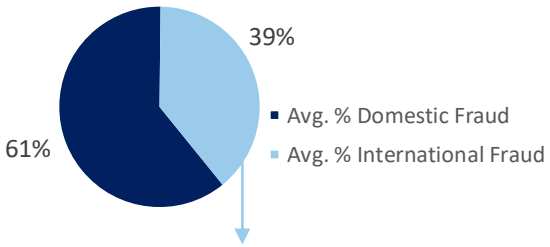
Fraud costs jump to $3.59 for every $1 of fraud for Large Digital Lenders that transact internationally.

Like Mid/Large Financial Services, these firms attribute 40% of their fraud losses to international transactions. But Large Lenders are challenged by both assessment of fraud risk by country/region and lack of specialized international tools. While this also seems to be most challenging in Asia for them, Lenders are also subject to sizeable fraud losses originating in Western/Central Europe and Canada.

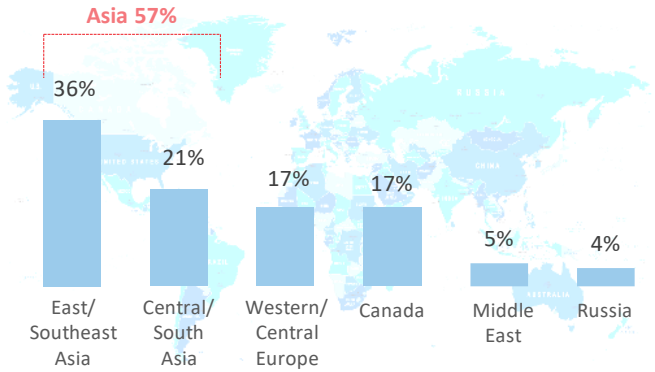
While traditional debit transactions account for the largest percentage of international fraud losses, alternative and other non-traditional methods combined account for nearly as much.

LENDING – Large ($50M+) Digital w/ International

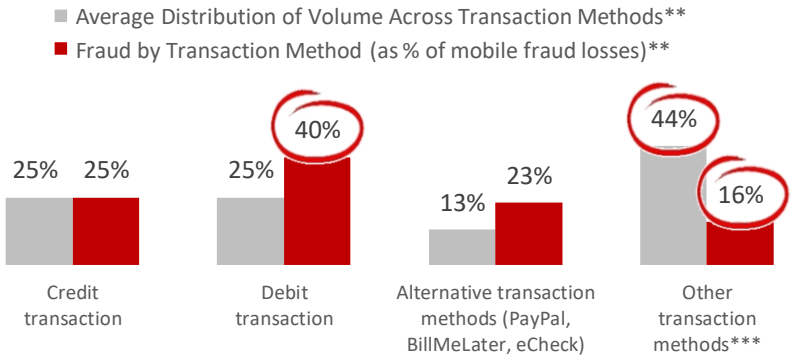
Fraud Losses



% Distribution of International Fraud Losses by Country/Region

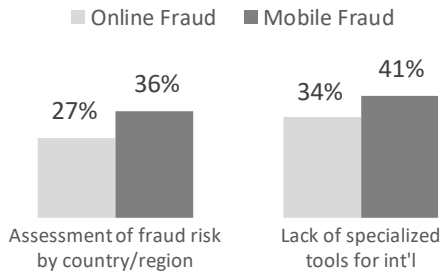


Transaction Methods/Fraud

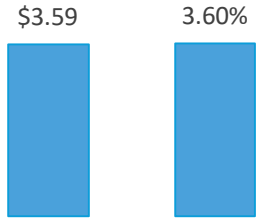


***Company-branded mobile app, gift cards, virtual currency, mobile wallets, checkout by Amazon, social media payments

Top Ranked Fraud Challenges



2018 LexisNexis Fraud Multiplier℠/ Fraud Costs as % of Revenues



LexisNexis® RISK SOLUTIONS

*** % can add to more than 100% since answers based on using a channel, in which case the base size changes per channel*

Q13: Please indicate the percent of fraud costs generated through domestic transactions compared to international transactions in the last 12 months.
Q14c: Please allocate 100 points across the following to indicate the distribution that each region represents of your total international fraud costs.
Q3: Please indicate the percentage for each method used (over the past 12 months) to fund transactions or disburse funds.
Q18: Please indicate the percentage distribution of the payment methods used to commit fraud against your company.

5

Identity fraud and verification remain key issues for firms selling digital goods or transacting digitally.

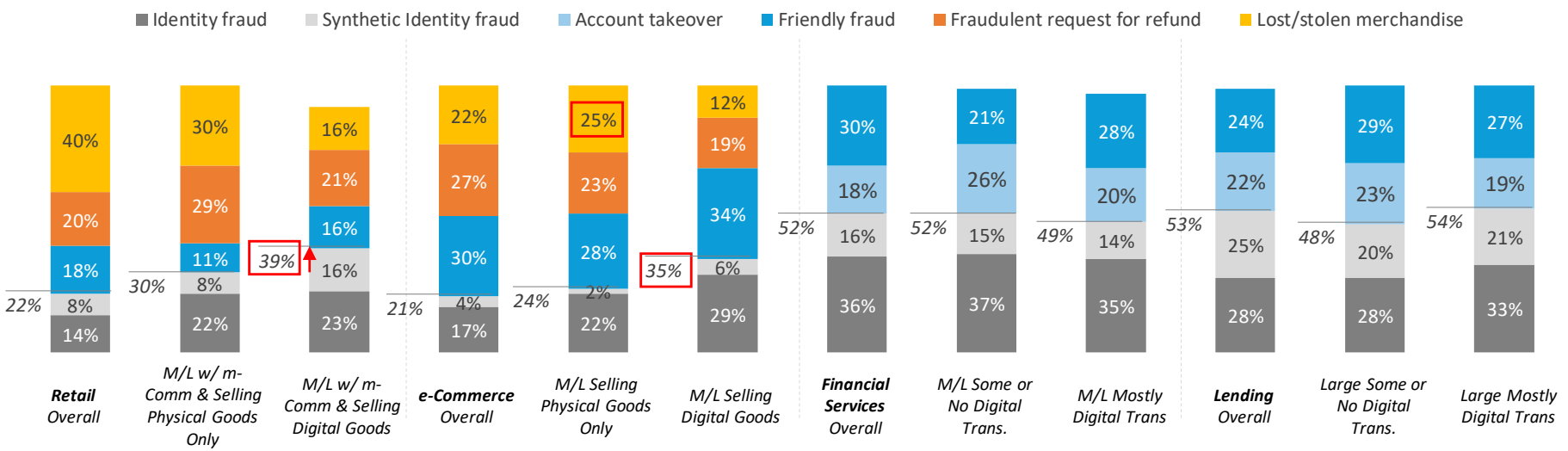
LexisNexis®
RISK SOLUTIONS

Identity and synthetic identity fraud continue to account for a significant degree of fraud losses for firms selling digital goods or transacting digitally.

Mid/Large Financial Services (49%) and Large Lending firms (54%), in particular, continue to fall victim to these types of fraud.

The amount of fraud attributable to stolen identity/synthetic identity has increased significantly since last year for Mid/Large Retailers selling digital goods through the mobile channel (39%), putting them on par with Mid/Large e-Commerce merchants (35%).

% Distribution of Losses by Type of Fraud



	Retail Overall	M/L w/ m-Comm & Selling Physical Goods Only	M/L w/ m-Comm & Selling Digital Goods	e-Commerce Overall	M/L Selling Physical Goods Only	M/L Selling Digital Goods	Financial Services Overall	M/L Some or No Digital Trans.	M/L Mostly Digital Trans	Lending Overall	Large Some or No Digital Trans.	Large Mostly Digital Trans
2017	19%	26%	20%	22%	31%	42%	45%	44%	47%	53%	47%	53%

Q12: Please indicate the percentage distribution of the following fraud methods as attributed to your total annual fraud loss over the past 12 months.

☐ Significantly different from other segment within industry category at the 95% Confidence Interval

↑ Significantly different from 2017 within segment at the 95% Confidence Interval

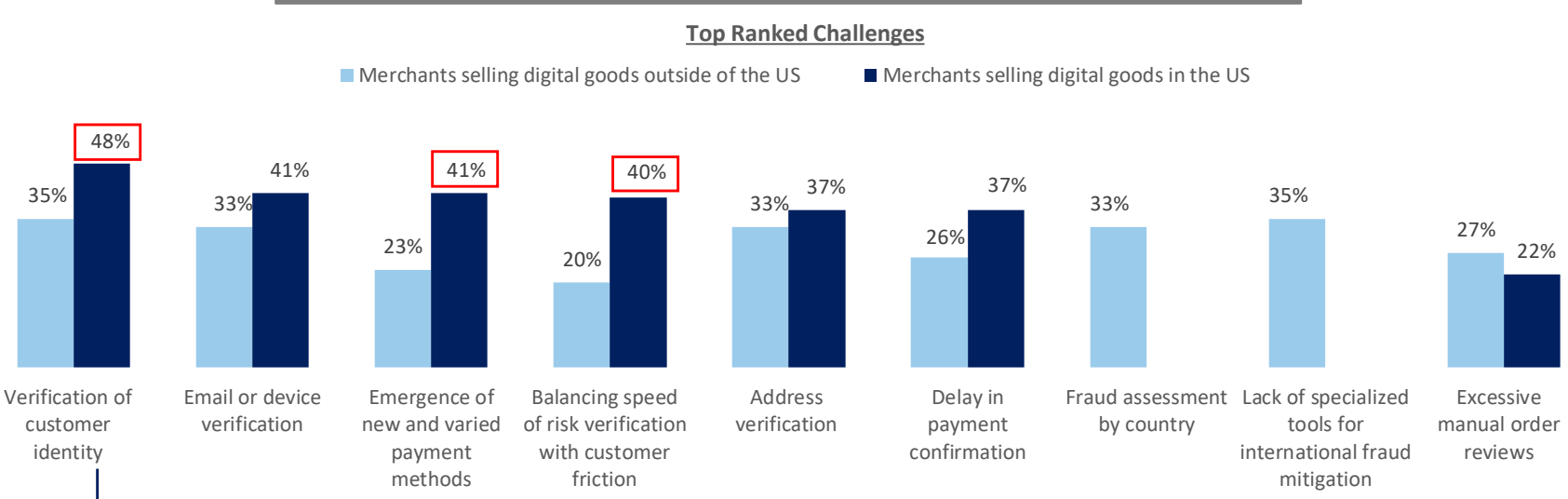
LexisNexis® RISK SOLUTIONS

Not surprisingly, Mid/Large Retailers selling digital goods and using m-Commerce are challenged by minimizing customer friction while verifying identities in the US, particularly with the use of newer payment methods.

This includes verifying digital identities (41% rank email or device verification) among their top 3 challenges when selling digital goods in the US. The rise of synthetic identities and volume of Botnet orders have made identity verification even more difficult. And with digital fraud being "fast fraud", time is of the essence when verifying a transaction. This can relate to delay in payment confirmation as a top challenge.

Top 3 challenges for selling digital goods outside of the US are more fragmented, indicating more variety of issues faced with these digital transactions.

RETAIL – Mid/Large ($10M+) w/m-Commerce & Selling Digital Goods



Key Reasons for Identity Verification Challenges

54%	54%	46%	47%
Limited/no access to 3rd party data sources	Rise of synthetic identities	Volume of botnet orders being placed at once	Limited ability to confirm location of order

76% among those ranking digital identity verification* as a top challenge

Q19aa: Please rank the top 3 challenges related to fraud faced by your company when selling digital goods to customers in the US
Q19bb: Please rank the top 3 challenges related to fraud faced by your company when selling digital goods to customers outside of the US
Q19a/b_2: Please rank the top 3 factors that make customer identity verification a challenge when selling digital goods inside/ outside the US.

LexisNexis® RISK SOLUTIONS

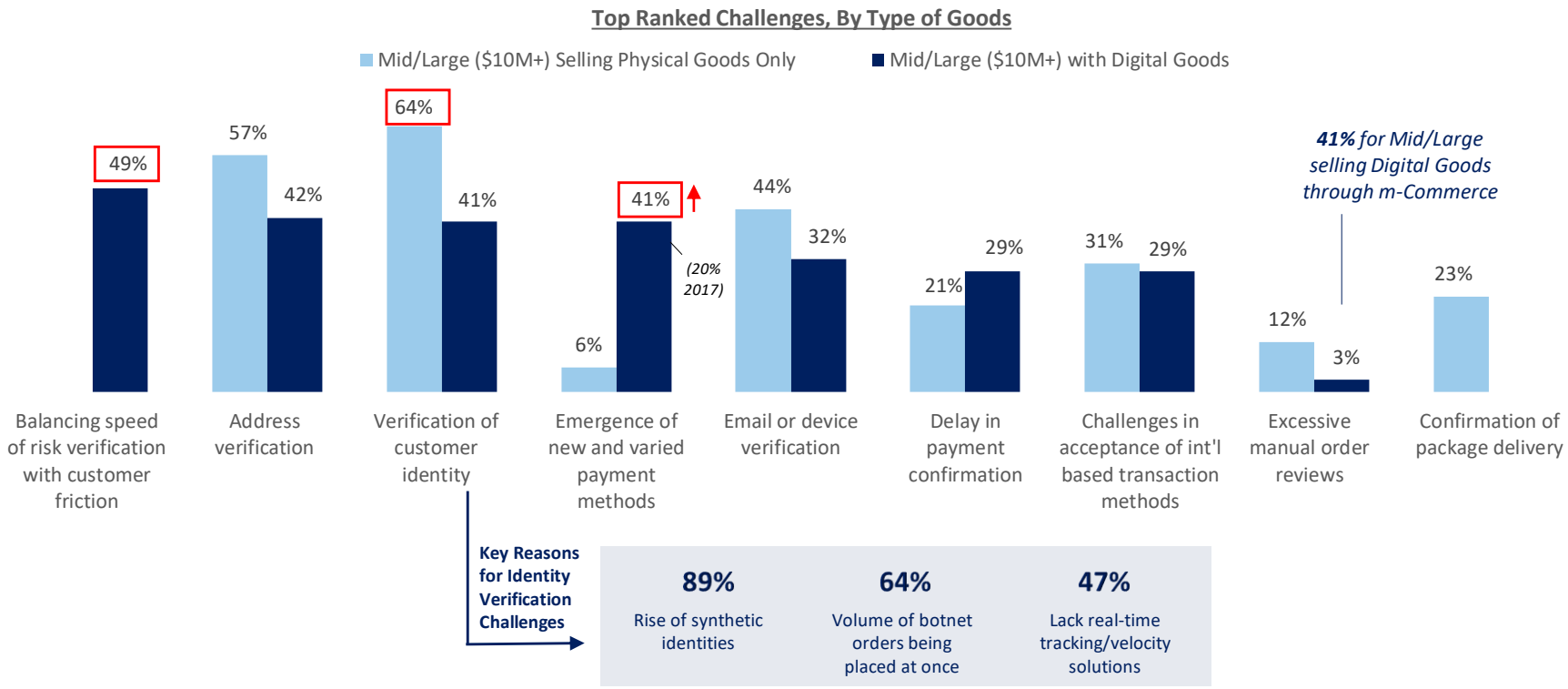
* Those ranking e-mail / device / address verification as a challenge

Significantly different from other segment within category at the 95% Confidence Interval

Mid/Large e-Commerce merchants selling digital goods are similarly challenged by minimizing customer friction while verifying identities, particularly with the use of newer payment methods.

For these merchants, increased synthetic identities and botnet activity, along with a lack of real-time tracking, are significant impediments to identity verification.

E-COMMERCE – Mid/Large ($10M+) Merchants Selling Digital Goods



LexisNexis® RISK SOLUTIONS

Q19a: Please rank the top 3 challenges related to fraud faced by your company when selling physical goods . . . when selling digital goods.
Q19a/b_2: Please rank the top 3 factors that make customer identity verification a challenge when selling digital goods inside/ outside the US.

Significantly different from other segment within category at the 95% Confidence Interval ↑ Significantly different than 2017 within Segment

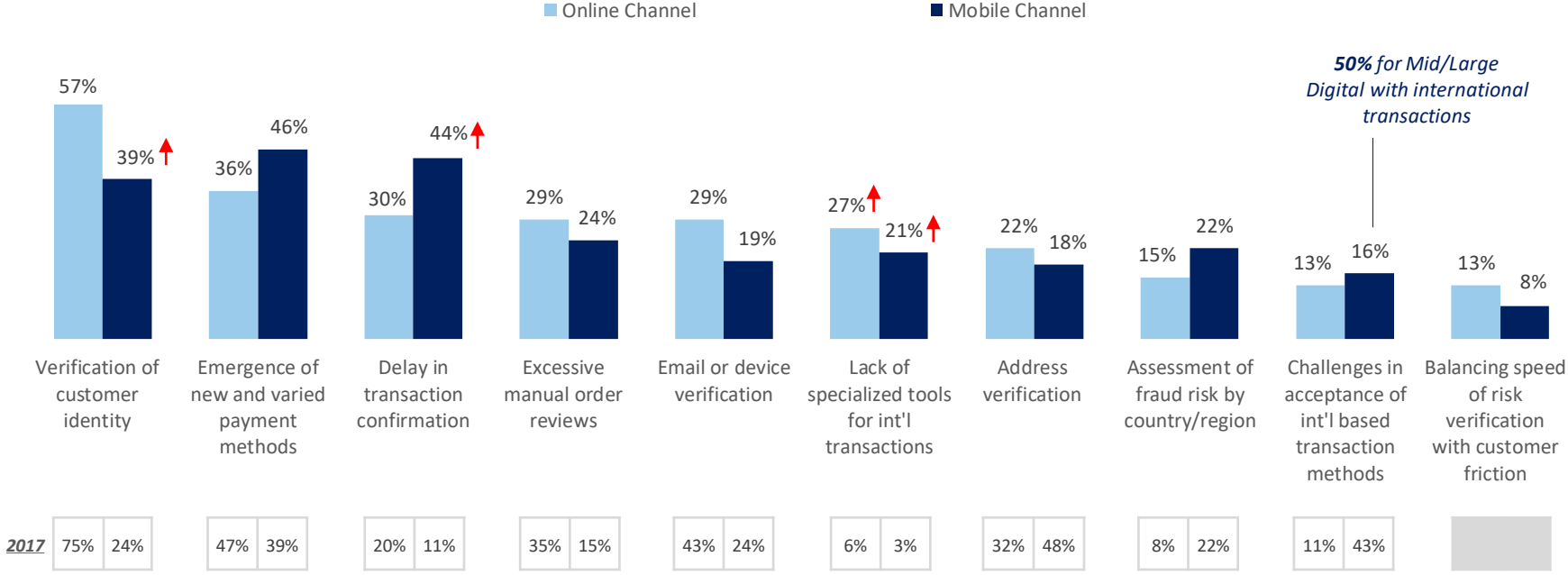
And identity verification remains the top challenge for Mid/Large Financial Services firms when transacting online and has grown since 2017 as a mobile channel challenge.

For those conducting business online, manual reviews and delayed confirmation are also ranked among top challenges. Since these digital firms rely heavily on the anonymous remote channel, any factors that cause customer friction, such as delayed transactions due to identity verification or manual reviews, can lead to significant longer term customer relationship issues (and potentially churn).

Noted decreases from 2017 for identity verification and e-mail/device verification do not indicate that these are less critical issues; since this is a ranking question (top 3), findings show that online transactions have generated a broader set of challenges (i.e., more concerns enter the top ranked mix, such as **lack of specialized tools for international transactions**). As a result, identity verification "has to share" top ranking with other issues.

FINANCIAL SERVICES – Mid/Large ($10M+) Digital

Top Ranked Fraud Challenges, By Channel



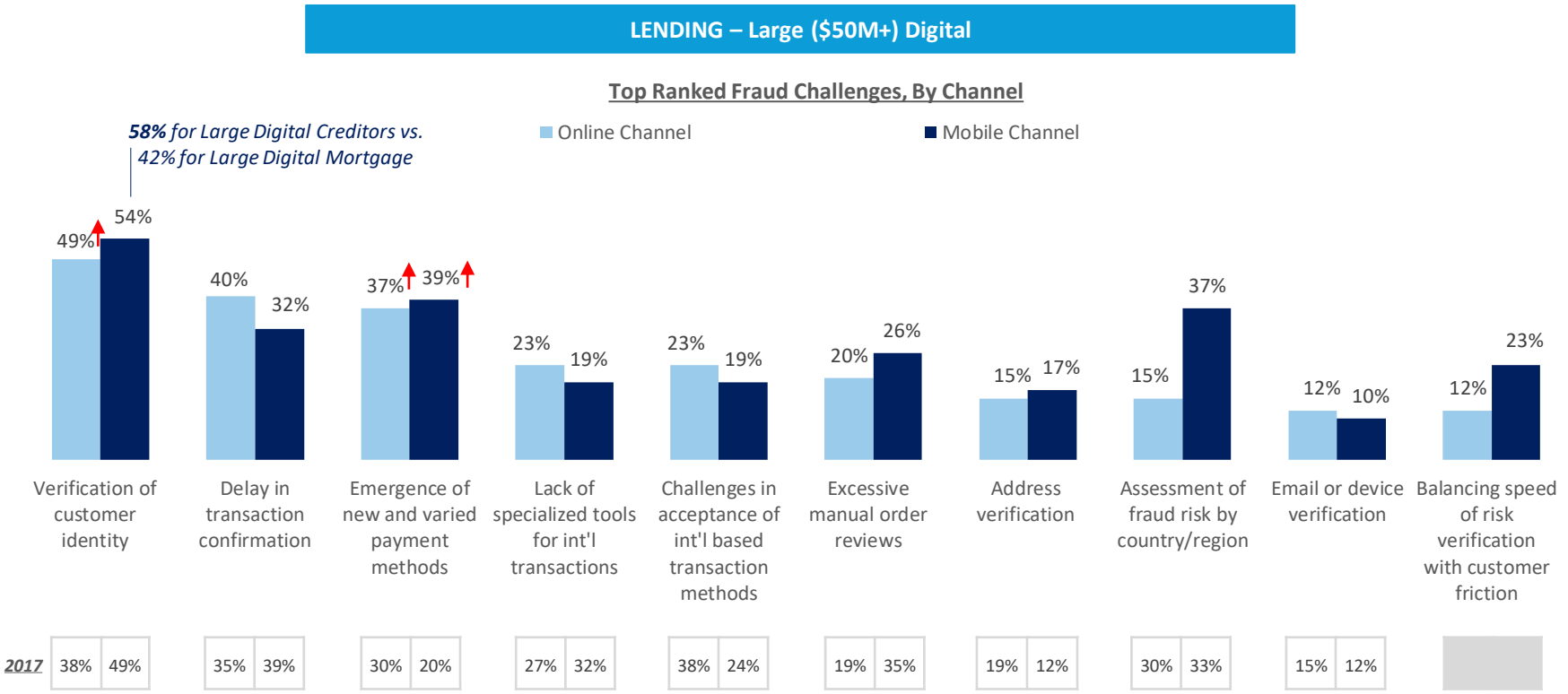
Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers in the Online/Mobile Channel.

↑ Significantly different than 2017 within Segment

For Large Digital Lenders, identity verification remains a top challenge when conducting mobile transactions and has actually grown since last year as an issue for the online channel.

And like with Financial Services, manual reviews and delayed confirmation as a result of difficulties in verifying identity can lead to significant longer-term customer relationship issues (and potentially churn).

These issues likely impact Large Digital Creditors more so than Mortgagees, with identity verification and botnet fraud activity being bigger challenges for them, especially through the mobile channel.



74% of Large Digital Creditors using the mobile channel agree that combatting automated botnet fraud activity is overwhelming (compared to only 24% of Large Digital Mortgage firms)

LexisNexis® RISK SOLUTIONS

Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers in the Online/Mobile Channel.

↑ Significantly different than 2017 within Segment

6

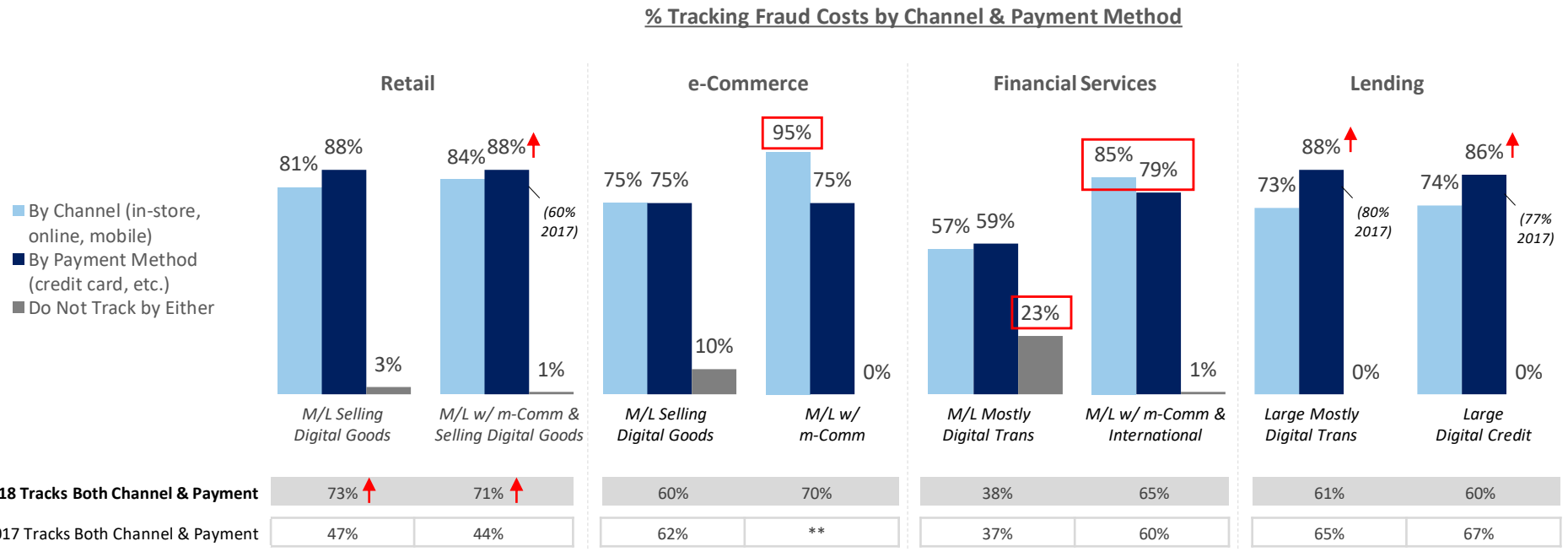
Tracking of fraud has increased, but for those hit harder by fraud, it still isn't optimal.

LexisNexis®
RISK SOLUTIONS

Segments with the highest fraud costs, to a large degree, track fraud costs by both channel and payment/transaction method.

It is important to track from both perspectives, since this involves different types of fraud approaches and scenarios. There is certainly a difference in how fraudsters can exploit the anonymity of the remote channels versus in-person purchases/transactions. There are also different techniques they will apply when using stolen credit cards or identities versus account takeovers through third-party providers. Keeping track of both attack perspectives makes fraud management more effective.

That said, these segments – Mid/Large Retailers selling digital goods and using m-Commerce, Mid/Large e-Commerce merchants using m-Commerce, Mid/Large Financial Services transacting internationally and using m-Commerce, and Large Digital Creditors – have high fraud costs nonetheless.



	Retail		e-Commerce		Financial Services		Lending	
2018 Tracks Both Channel & Payment	73% ↑	71% ↑	60%	70%	38%	65%	61%	60%
2017 Tracks Both Channel & Payment	47%	44%	62%	**	37%	60%	65%	67%

LexisNexis® RISK SOLUTIONS

Q14: Does your company track the cost of fraudulent transactions by channels or methods?

☐ Significantly different from other segment within industry category at the 95% Confidence Interval

↑ Significantly different from 2017 within segment at the 95% Confidence Interval

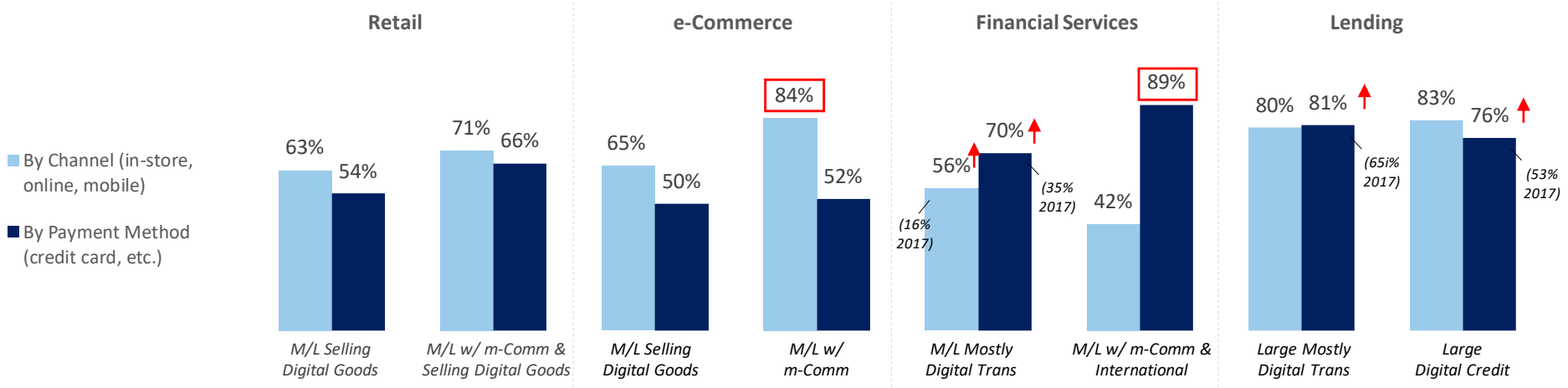
*** Incidence too low for Mid/Large m-Commerce in 2017; base size too small to show comparison findings*

That said, these harder hit segments are more likely to be tracking where fraud has been *successful* rather than also tracking where they've been able to prevent it.

At-risk Financial Services firms are even less likely than others to be tracking successful or prevented fraud by channel and transaction method.

Not holistically tracking by prevented/successful fraud attempts for both channel and payment method lessens the overall effectiveness of managing fraud given that fraudsters are adept at testing for areas that become less of a focus to at risk firms and, thereby, changing their attack points accordingly.

% Tracking SUCCESSFUL Fraud Transaction By Channel & Payment Method



SUCCESSFUL Fraud												
2018 Tracks Both Channel & Payment	53% ↑	53% ↑	55%	51%	41% ↑	43% ↑	62% ↑	60% ↑
2017 Tracks Both Channel & Payment	33%	40%	56%	**	18%	30%	46%	43%
2018 Tracks Both Successful & Prevented By Channel & Payment	42%	40%	43%	27%	28%	23%	38%	37%

LexisNexis® RISK SOLUTIONS

Q26: Does your company track successful fraudulent transactions by channels or payment methods?

☐ Significantly different from other segment within industry category at the 95% Confidence Interval

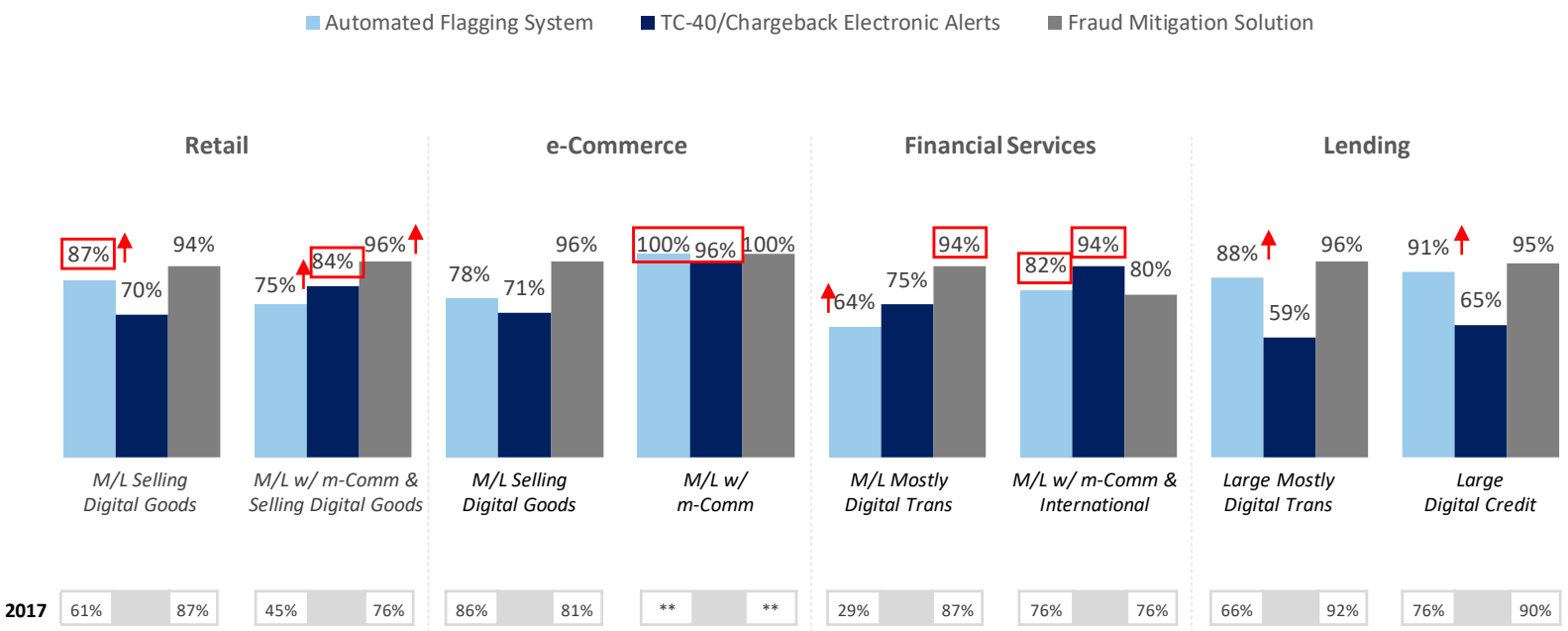
↑ Significantly different from 2017 within segment at the 95% Confidence Interval

*** Incidence too low for Mid/Large m-Commerce in 2017; base size too small to show comparison findings*

And combined fraud solution and automated alert system usage remains high or has increased among these at risk segments.

Large Digital Lenders, particularly Creditors, and Mid/Large Retailers selling digital goods and using the mobile channel appear to have made investments in automated flagging systems since last year. This could be related to issues experienced with fraud through the mobile channel and/or internationally.

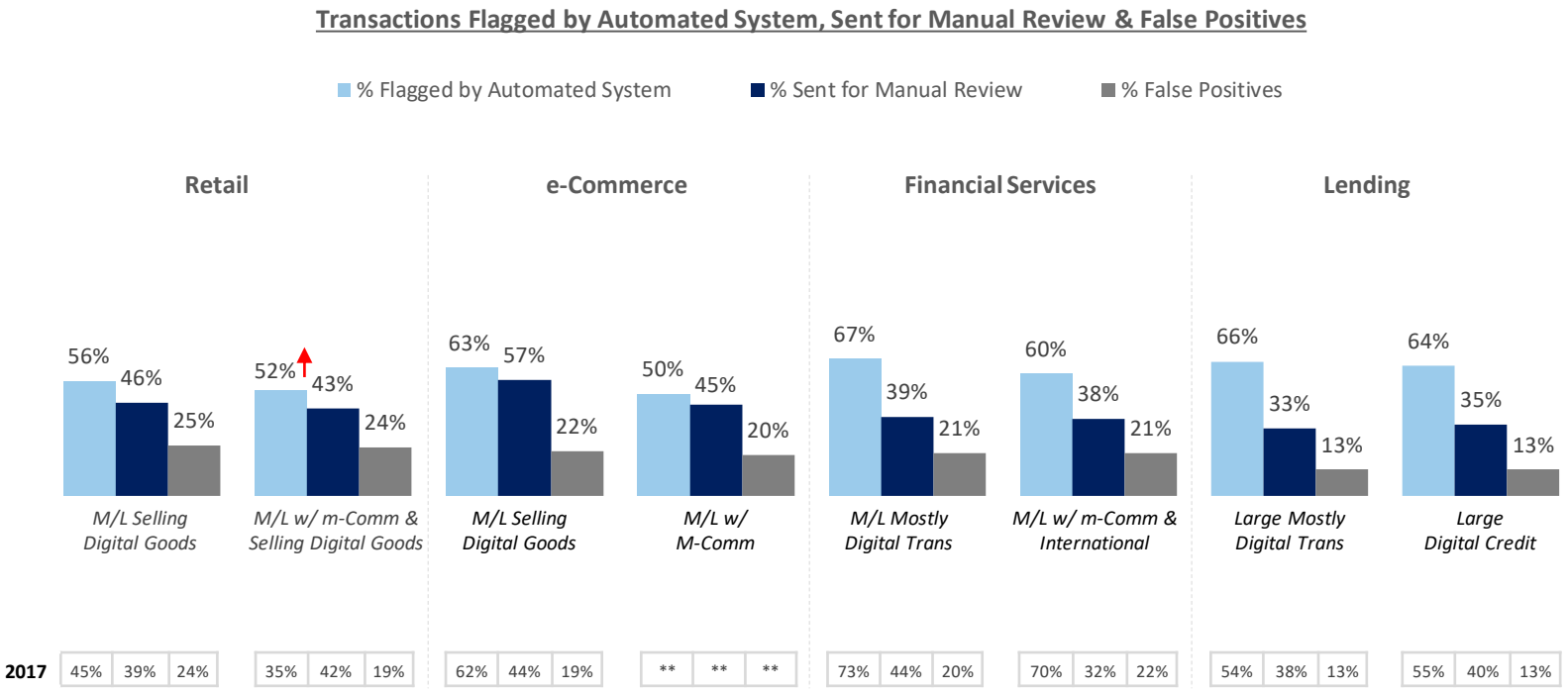
% Merchants Who Use Automated Flagging System, TC-40/Chargeback Electronic Service Alerts, or Fraud Mitigation Solution



*** Incidence too low for Mid/Large m-Commerce in 2017; base size too small to show comparison findings*

But this doesn't seem to improve the accuracy or efficiency of the fraud identification process.

Just as many transactions are being sent for manual review as last year and the volume of false positives hasn't decreased, regardless of segment. Both of these factors have cost, lost revenue, and longer-term customer relationship ramifications.



** Incidence too low for Mid/Large m-Commerce in 2017; base size too small to show comparison findings

LexisNexis® RISK SOLUTIONS

Q36: Of all the transactions your company flagged as potentially fraudulent in the past 12 months, what percentage was flagged by your auto system?
Q37: Of this (…), what proportion are sent for manual review?
Q39: What percentage of declined transactions turned out to be false positives?

↑ Significantly different from 2017 within segment at the 95% Confidence Interval

7

A number of higher risk firms are using fraud prevention solutions, but not necessarily the right combination to successfully prevent fraud.

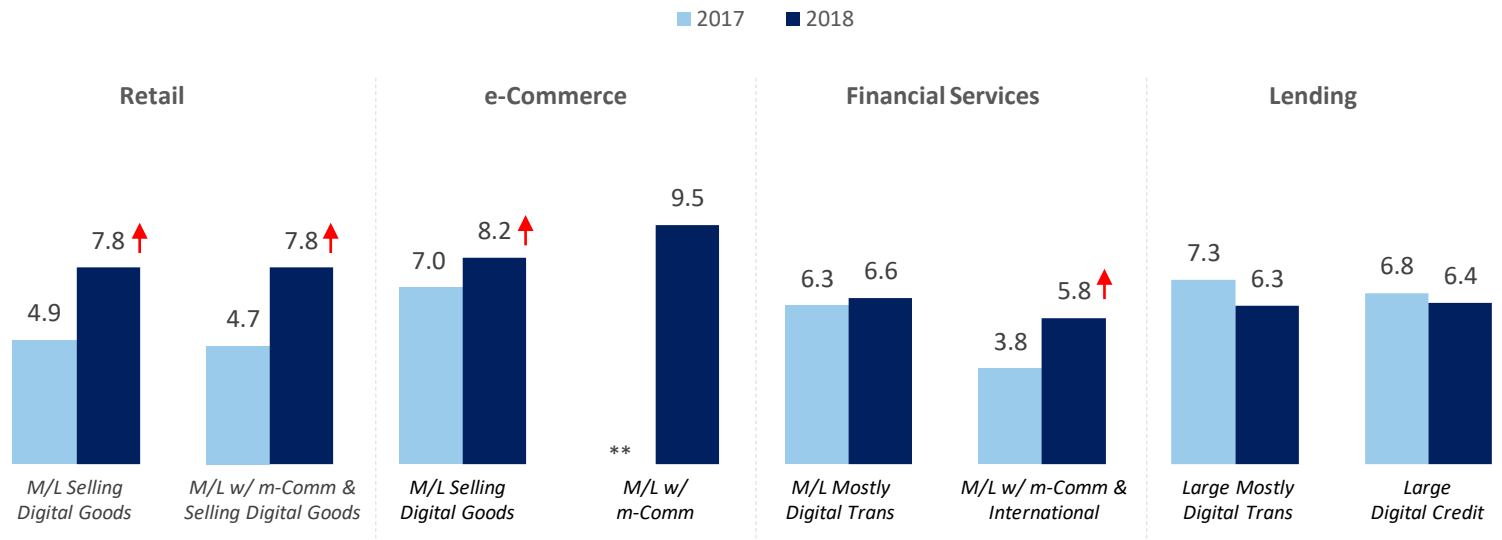
LexisNexis®
RISK SOLUTIONS

The average number of reported solutions used has increased or is on par with 2017 for segments hit hardest by fraud.

Mid/Large e-Commerce and Retail merchants selling digital goods and/or using m-Commerce now use a few more solutions than Financial Services and Lending firms.

The fact that all at-risk segments now report using at least 6 different solutions suggests they are taking steps to address and fight against remote/fast fraud.

Average Number of Fraud Mitigation Solutions Currently Used



LexisNexis® RISK SOLUTIONS

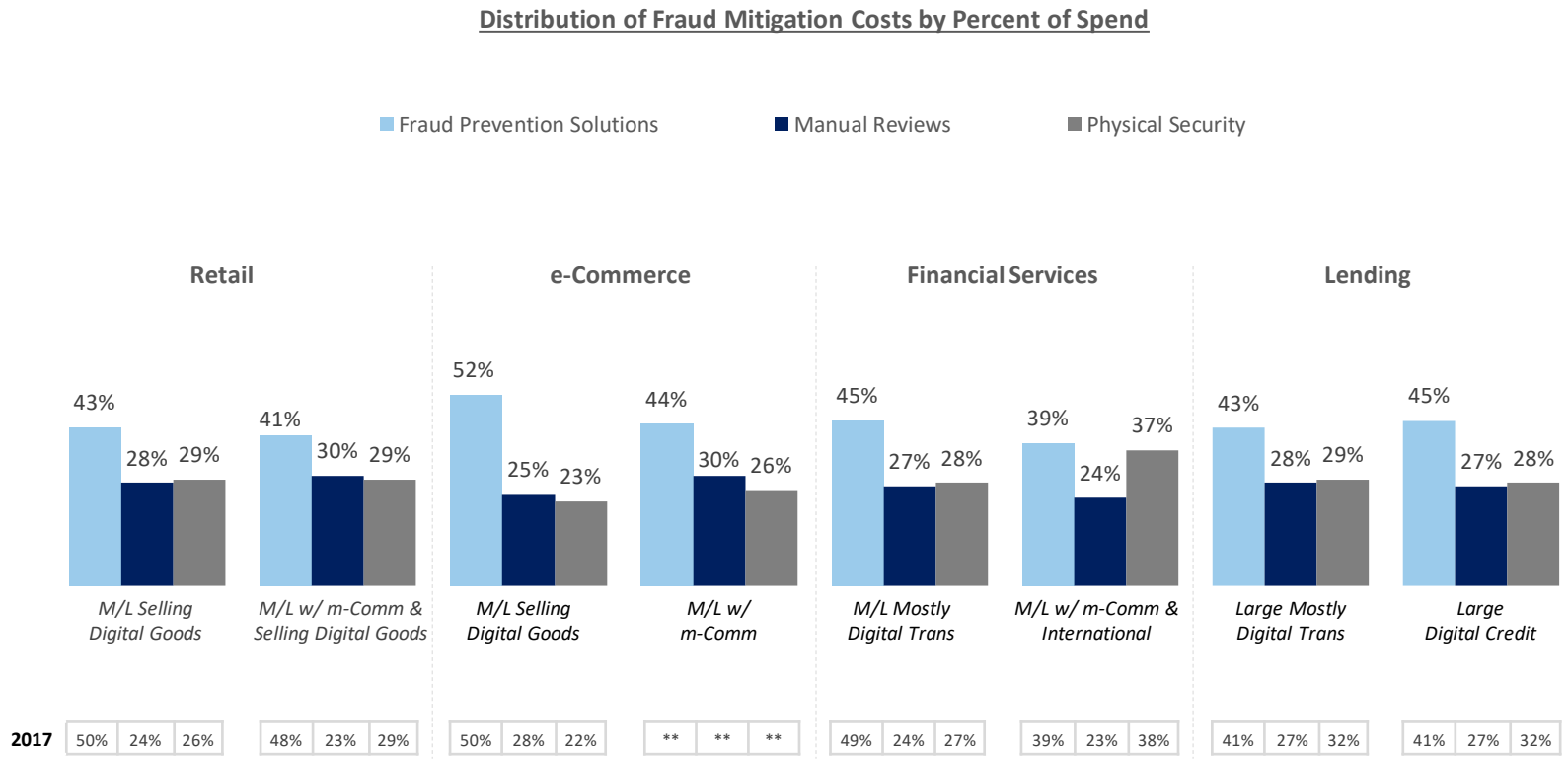
Q27: Which of the following best describes your awareness and use of the fraud solutions listed below?

↑ Significantly different from 2017 within segment at the 95% Confidence Interval

*** Incidence too low for Mid/Large m-Commerce in 2017; base size too small to show comparison findings*

But while solutions continue be the major component of fraud mitigation spend for these segments, a sizeable portion is still budgeted for manual reviews.

This is the case regardless of sector.



*** Incidence too low for Mid/Large m-Commerce in 2017; base size too small to show comparison findings*

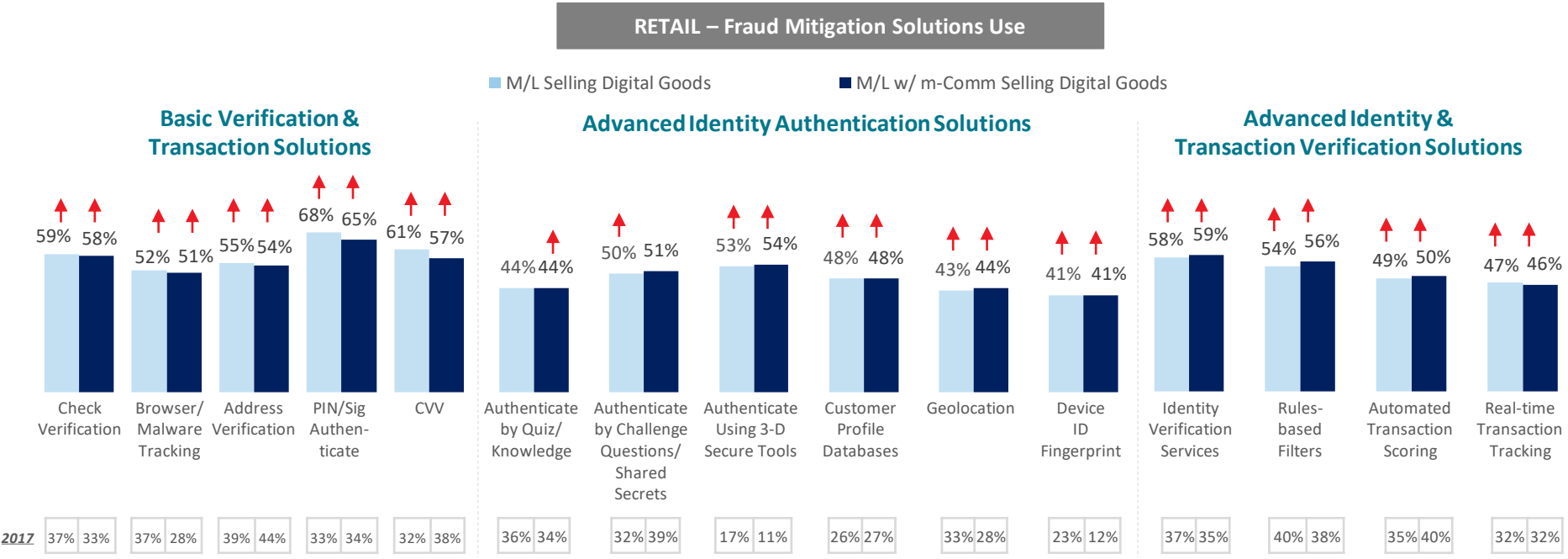
LexisNexis® RISK SOLUTIONS

Q39: What percentage of declined transactions turned out to be false positives?

Harder-hit Retailers might not be fully optimizing the use of risk mitigation solutions, even though they use more of them than others.

There has been an increase in both identity authentication and verification solutions use among many Mid/Large Retailers that sell digital goods and use the mobile channel, which shows an understanding of the need for both types - including to support digital identity proofing. But not everyone has caught up to that; the use of many of these is still at or under 50% of the market.

Also, an increase in some solutions/services, such as check verification and PIN/signature authentication, reminds us that these merchants are using multiple channels – and may be trying to use the same types of solutions in different channels that present different types of risks.



LexisNexis® RISK SOLUTIONS

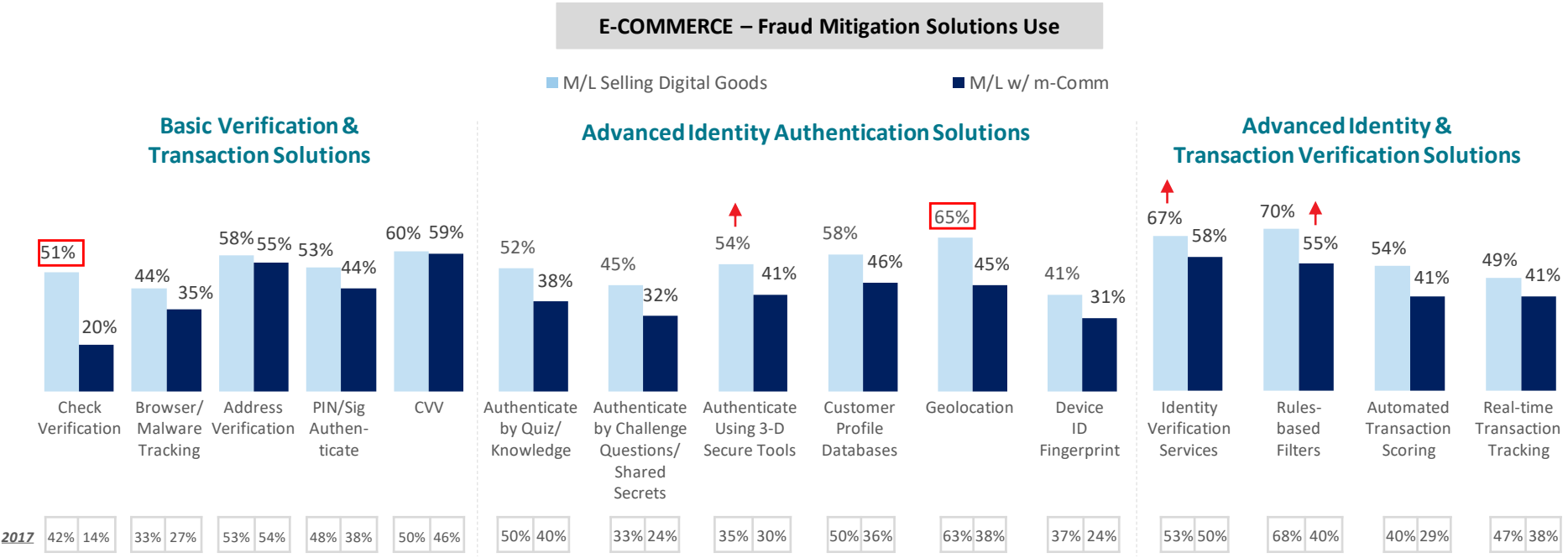
Q27: Which of the following best describes your awareness and use of the fraud solutions listed?

↑ Significantly different than 2017 within Segment

There is also only marginally directional growth with reported use of some solutions among Mid/Large e-Commerce selling digital goods and those using m-Commerce.

There is still strong use of rules-based filters, identity verification services, and geolocation. But there is more moderate use of other advanced identity and transaction verification solutions, including real-time transaction tracking, automated transaction scoring, and device ID/fingerprinting that are especially useful for catching fraud with digital goods. Digital transactions occur quickly, increasing the risk of "fast fraud" before it can be caught; these solutions can support this.

Again, this can explain the reason that these merchants continue to experience rising fraud costs and volume while actively employing tools and approaches to fight it.



LexisNexis® RISK SOLUTIONS

Q27: Which of the following best describes your awareness and use of the fraud solutions listed?

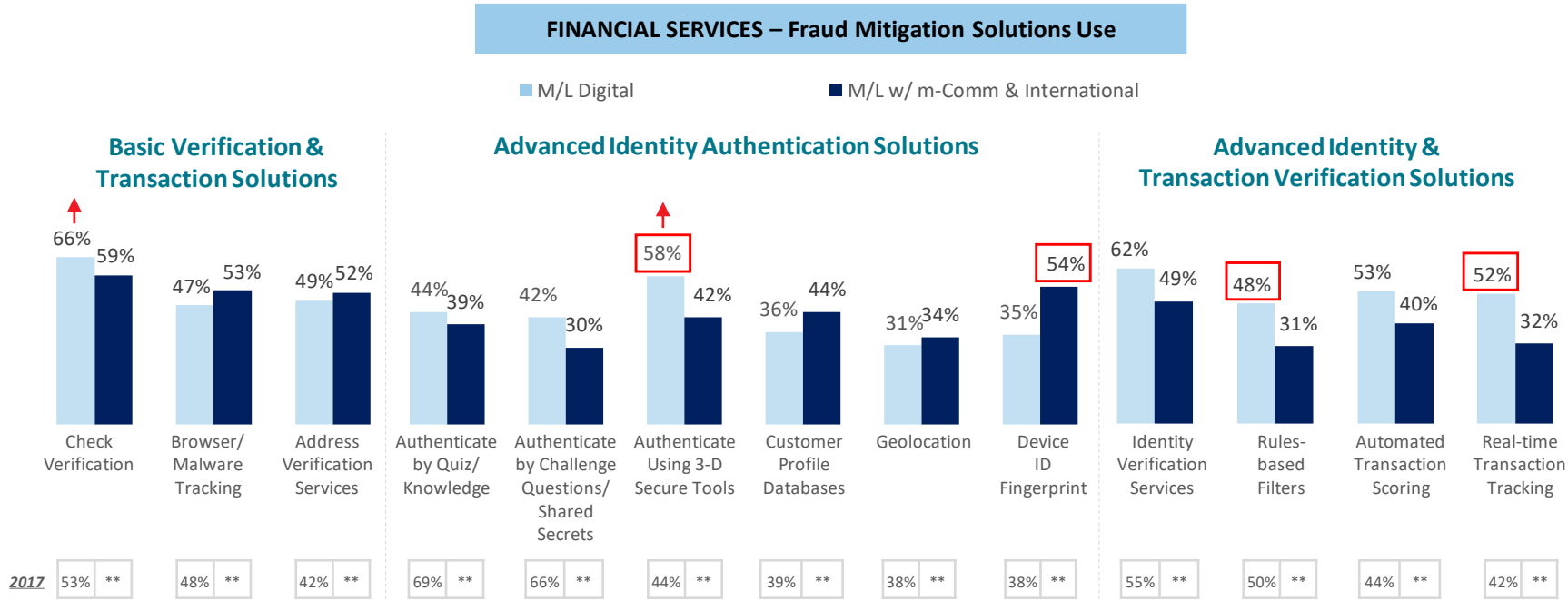
↑ Significantly different than 2017 within Segment

☐ Significantly different from other segment within industry category at the 95% Confidence Interval

The use of advanced identity and transaction verification solutions remains fairly limited for Mid/Large Financial Services firms conducting digital transactions. Those that also have international transactions are even more limited in their efforts.

With an average of 5.8 solutions, Mid/Large Financial Services firms that conduct international and mobile channel transactions vary considerably on the types of fraud mitigation solutions being used. While just over half report using device ID/fingerprinting, which is useful for mobile channel fraud detection, there is more limited use of other identity authentication and transaction verification solutions; even less so than Mid/Large Digital firms in general.

This weakens fraud prevention efforts and very likely correlates to having higher fraud costs than others.



LexisNexis® RISK SOLUTIONS

** Incidence too low in 2017; base size too small to show comparison findings

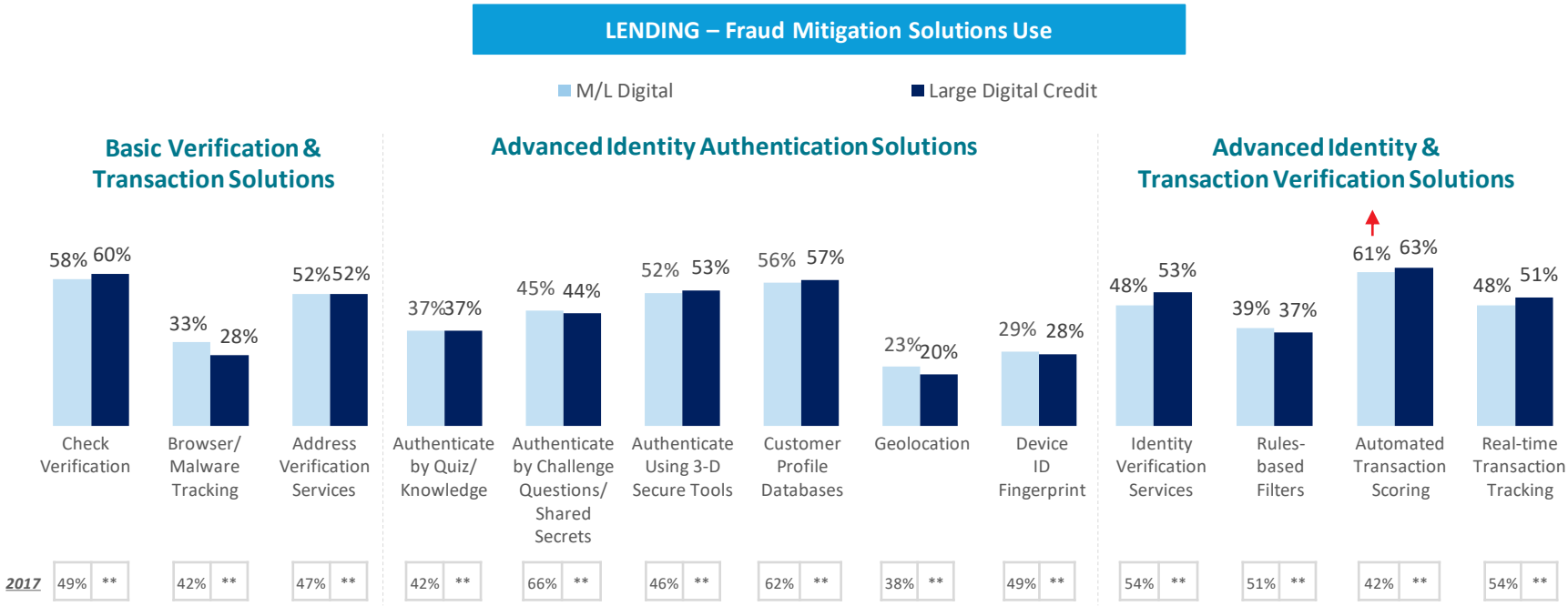
Q27: Which of the following best describes your awareness and use of the fraud solutions listed?

Significantly different from other segments within category at the 95% Confidence Interval

Significantly different than 2017 within Segment

While a good share of Large Digital Lenders, particularly Large Digital Creditors, report using authentication by 3-D secure tools and customer profile databases, the use of other advanced identity authentication solutions remains somewhat limited.

Even though the average number of solutions used by these segments is relatively high (6.3/6.4), they continue to get hit harder by fraud. This suggests the need to further optimize which types of solutions are used and layered/bundled together to meet specific fraud risks.



LexisNexis® RISK SOLUTIONS

** Incidence too low in 2017; base size too small to show comparison findings

Q27: Which of the following best describes your awareness and use of the fraud solutions listed?

Significantly different from other segments within category at the 95% Confidence Interval

Significantly different than 2017 within Segment

8

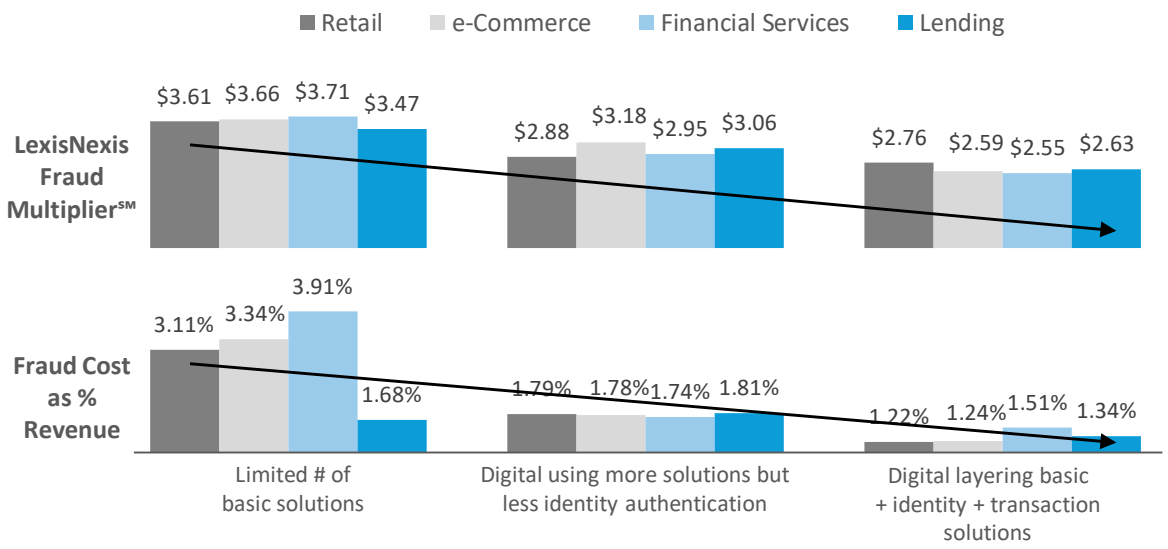
Findings show that using the right combination of tools is crucial to combatting fraud risks and cost.

LexisNexis®
RISK SOLUTIONS

Firms that use a multi-layered solution approach experience a lower cost of fraud.

Survey findings show that those who layer core + advanced identity authentication + advanced transaction/identity verification solutions have lower fraud costs than others per fraud event ($2.63 - $2.76 for every $1 of fraud versus $3.47 - $3.71) and as a percent of annual revenues.

LexisNexis Fraud Multiplier℠
Avg. Fraud Cost as % of Revenue
by Number & Layering of Fraud Mitigation Solutions



Layers of Protection		Limited	Limited	Multi-Layered
Common Core Solutions Used Most Often	Card verification, PIN/Signature, Check Verification, Browser Malware, Address Verification	Mostly	Many	✓
Layering of Advanced Identity Authentication Solutions	Device ID Fingerprinting, Geolocation, Authentication by Quizzes, Authentication by Challenge Questions, Authentication of Transaction by 3D Tools, Customer Profile Database	Minimal to None	Minimal to None	✓
Layering of Advanced Identity & Transaction Verification Solutions	Automated Transaction Scoring, Real-Time Transaction Tracking, Identity Verification Services, Rules-Based Filters	Minimal to None	Many	✓

LexisNexis® RISK SOLUTIONS

Recommendations

Recommendation #1

Firms selling digital goods or transacting digitally, in particular, should consider a multi-layered solution approach that attacks different types of fraud.

It is critical for firms 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.

LexisNexis® RISK SOLUTIONS

Recommendation #2

When layering solutions, it's important to implement a mix of different ones in order to address the unique risks generated from different channels and transaction methods. It's not about the number, but rather the right combination.

Solutions used to mitigate risk in the physical/at-location or for physical goods transactions won't fully mitigate risk with transactions conducted through remote channels or with digital goods. And, different issues and risks exist between the online and mobile channels; one "overall remote channel" solution may not address both environments.

Different challenges and risks also require specific solutions that support domestic versus international transactions.

LexisNexis® RISK SOLUTIONS

Recommendation #3

A multi-layered solution approach is particularly essential for mid/larger firms selling digital goods and/or transacting via the mobile channel in order to fight fraud generated by botnets and synthetic identities.

Botnets are challenging not just because of the volume of attacks, which they can adjust in order to minimize attention, but they can make identity verification challenging as well. They can attach themselves to mobile devices via malware, posing as the user. They also leverage synthetic identities based on pulling together various types of personally identifiable information – made available through various recent breaches.

This requires the need for a combination of data insights, including a person's footprint and identity, device assessment, geographic location, etc.; traditional solutions and those which work in isolation of each other will only pick up parts of this information, but not enough to support fraud decisions with such fast and anonymous transactions.

LexisNexis® RISK SOLUTIONS

Recommendation #4

Firms should seek external providers with deep data and analytics resources to most effectively address identity-based fraud challenges. This in particular includes those conducting international transactions.

Identity fraud can be complicated, with various layers of masks and connections in the background. Investing in a layered solution approach will be much more effective if from a solutions partner that provides unique linking capabilities which identify and match hidden relationships, shed light on suspicious activities or transactions and identify collusion. These patterns are not easily uncovered by a number of risk solutions on the market today.

International transactions and newer privacy regulations – such as the GDPR – will make it increasingly difficult for companies to access and store foreign customer data essential for effective identity verification and authentication (including digital identity data). This means that firms will need to rely more on external providers who already have deep reservoirs of current data on consumers and businesses.

LexisNexis® RISK SOLUTIONS

Recommendation #5

Firms need to holistically track fraud by both payment and channel type – including that which has been successful and prevented. But this needs to be part of a broader approach that involves fraud detection solutions.

Since fraud occurs in different ways, this creates multiple endpoints and approaches that fraudsters can use to attack. They continue to test for the weakest links and where they can operate undetected. Knowing where they've been successful is important for "plugging the gaps"; but also knowing where they've tried and failed is important in order to maintain vigilance.

That said, the rise of synthetic identities makes it easier for fraud to go undetected. Without the aid of risk mitigation solutions designed to identify fraudulent identity characteristics, tracking approaches will miss certain clues; this will weaken tracking efforts.

LexisNexis® RISK SOLUTIONS

LexisNexis® Risk Solutions can help

LexisNexis®
RISK SOLUTIONS

LexisNexis® Risk Solutions provides powerful identity verification, identity authentication and transaction scoring tools to combat fraud.

LexisNexis® Risk Solutions:

- Vast Data Resources
- \+
- Big Data Technology
- \+
- Linking & Analytics
- \+
- Industry-Specific Expertise & Delivery

=

Customer-Focused Solutions

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 failures

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 scenario
- Receive real-time pass/fail results

For more information: visit http://risk.lexisnexis.com or call 800.869.0751

LexisNexis® RISK SOLUTIONS