LexisNexis® Risk Solutions 2017 True Cost of Fraud℠ Study – Financial Services Edition

October 2017

LexisNexis® RISK SOLUTIONS

The LexisNexis® Risk Solutions 2017 True Cost of Fraud℠ Study helps **financial services companies** navigate the growing risk of fraud.

The research provides a snapshot of current fraud trends in the United States and spotlights key pain points that financial services companies 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 navigate and manage the cost of fraud while strengthening customer trust and loyalty?

LexisNexis® RISK SOLUTIONS

The study included a comprehensive survey of 185 risk and fraud executives in **financial services** companies.

Fraud Definitions

- Fraud is defined as the following:
  - Fraudulent transactions due to identity fraud, which is the misuse of stolen payments methods (such as credit cards) or personal information
  - Fraudulent requests for refunds/returns, bounced checks
- 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 firm occurs based on the actual dollar value of a fraudulent transaction

Research was conducted March & April 2017.

Financial Services Companies Include:

- Retail/Commercial Banks
- Credit Unions

- Investments
- Trusts
- Wealth Management

Segments Include:

Mid/Large Digital

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

Mid/Large Non-Digital

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

	Company Type		Company Type by Revenues		Digital	
	Banks	Investments	Mid/Large Banks ($10M+)	Mid/Large Investments ($10M+)	Mid/Large Digital ($10M+)	Mid/Large Non-Digital ($10M+)
# Completions	108	77	78	45	50	100

LexisNexis® RISK SOLUTIONS

Executive summary: key findings

LexisNexis®
RISK SOLUTIONS

Key findings

1

There is risk of increasing fraud in the Financial Services sector as digital channel use grows.

- For those generating 50% or more revenues digitally, the cost and proportion of monthly fraud is higher than for others.
- Among mid/large digital firms ($10M+ annual revenues), every $1 of fraud costs them $3.04 on average compared to $2.35 for others. Fraud costs as a percentage of mid/large digital revenues are 2.79% compared to 2.04% for non-digital.
- And, over one-third of monthly transactions are fraudulent among mid/large digital firms.

2

Digital challenges will likely be heightened as more firms adopt the mobile channel.

- There are concerns that it adds significant risk, with less confidence in the security of mobile device transactions.
- But as more consumers use their mobile devices for financial transactions, demand will require financial firms to offer this channel.
- For those who already offer it, there is concern about the impact of new transaction methods and verifying location to determine if a transaction is fraudulent. For mid/large digital firms, there is nearly as much fraud occurring through mobile apps as a mobile browser.

3

The challenges associated with verifying mobile device location and newer transaction methods can increase customer friction.

- This relates not only to processes for establishing customer credentials and location, but transaction risks and losses to the customer.
- As ATMs have become riskier with skimming, card data malware and other threats, and as consumers use mobile apps such as cardless transactions, any losses or data breaching experienced by them reflects negatively on the financial firm – regardless of where the fault lies.

Key findings (continued)

4

Identity fraud is a significant issue for financial services firms, particularly for larger digital banks.

- Larger ($50M+) banks report an average of 62% of fraud losses occurring based on identity fraud.
- Three-fourths of mid/large digital firms indicate identity verification as a top online challenge; they are also more likely to also cite device verification and excessive manual reviews than others.
- This further adds to customer friction for every transaction that is delayed or blocked until reviewed.

5

But, there are somewhat different key challenges between online and mobile channels.

- When having to select only the top three challenges, mid/large digital firms include identity verification more often for online than mobile.
- They are more likely to select address verification and challenges of accepting international based transactions with the mobile channel.

6

Mid/large digital firms are getting hit harder by fraud based on not efficiently tracking it or fully embracing solutions which can help them fight it most effectively.

- Few mid-sized digital firms are tracking prevented or successful fraud, with limited tracking of fraud costs as well. Findings show that those who do track by both methods experience a lower cost of fraud.
- But it's not just that; it's also how solutions are used (or not).
    - On average, mid/large digital firms use more solutions than non-digital firms, but not layered effectively. Identity authentication by either KBA questions or challenges / shared secrets is used by two-third of mid/large digital firms, though there is significantly less use of other advanced identity-related solutions.
- And, there is only moderate use of transactional fraud verification solutions.

Key findings (continued)

7

Findings show that financial services firms who layer solutions by identity and fraud transaction solutions experience fewer issues and cost of fraud.

- They experience fewer false positives.
- There are fewer manual reviews required.
- The cost of fraud is less.

8

However, mid/large digital firms may not be thinking of risk mitigation solutions in terms of layering for best protection.

- When asked to identify solutions to prevent online / mobile fraud, answers were fragmented.
- At the same time, they use more solutions (avg. 6.3) such that bundling may not be as coordinated as it is a la carte.

Fraud observations reveal challenges for digital financial services firms.

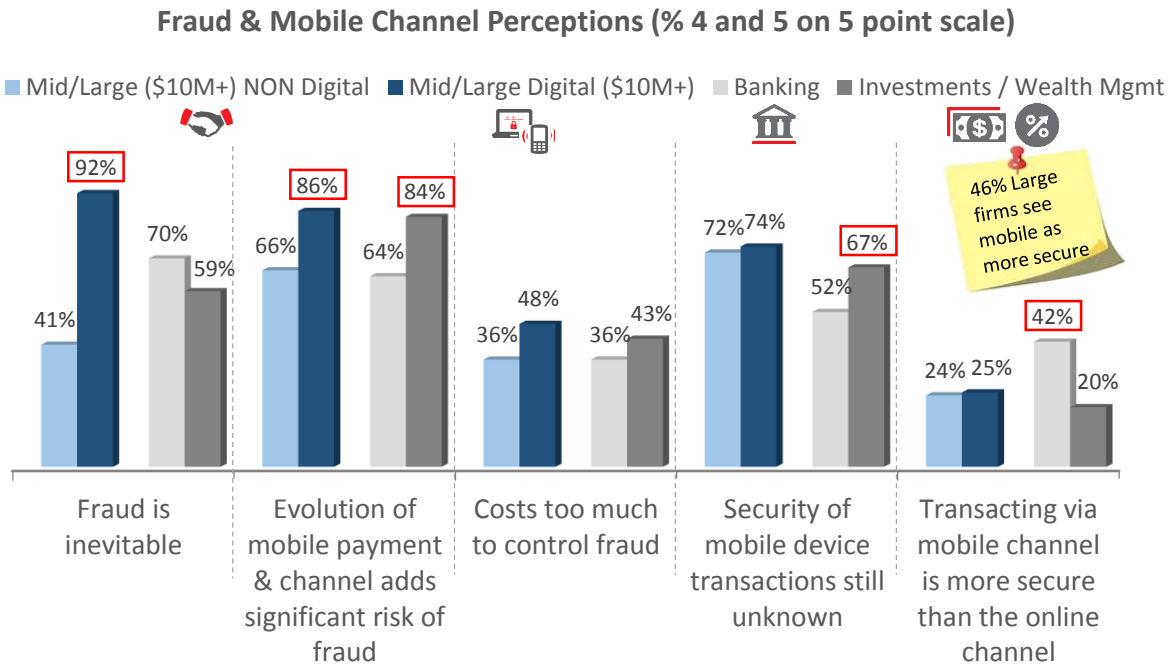
LexisNexis®
RISK SOLUTIONS

There is concern about risk and security of the mobile channel among financial services firms, which influences perceptions that fraud is inevitable.

Mid/large digital firms are particularly resigned to seeing fraud as being inevitable.

Many banks have concerns about the mobile channel, though significantly more investment / wealth management firms are sensitive to its risk and security. Access to customer accounts can cause not only financial wealth damage, but fraudsters also seek to steal personally identifiable information for use elsewhere and for other reasons – including information on high-profile and high net-worth individuals.[1]

[1] Threats to the Financial Services Sector, PwC, Financial Services sector analysis 2014 Global Economic Crime Survey; https://www.pwc.com/gx/en/financial-services/publications/assets/pwc-gecs-2014-threats-to-the-financial-services-sector.pdf



LexisNexis® RISK SOLUTIONS

Q33: Using a 5-point scale, where "5" is "agree completely" and "1" is "do not agree at all", please rate the extent to which you agree or disagree with the statements below.

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

Having a sizeable digital presence can increase fraud costs if not effectively managed.

For every $1 of fraud, it costs mid/large digital financial services firms $3.04 compared to $2.35 for non-digital mid/large firms.

Further, fraud costs as a percentage of revenues is higher among mid/large digital firms than non-digital ones.

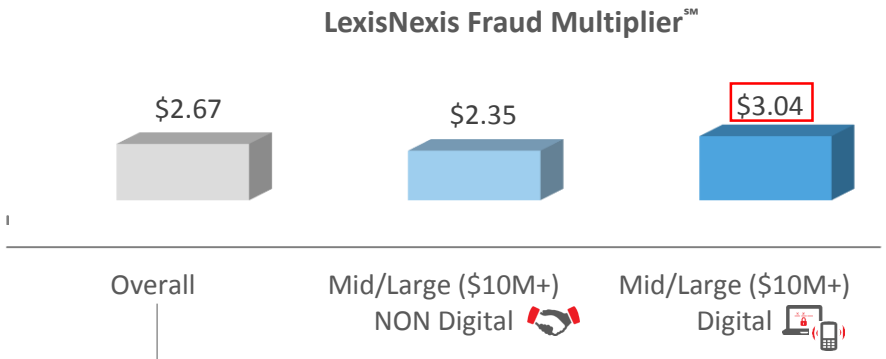


Illustration: Calculating the LexisNexis Fraud Multiplier℠

Description: the total cost for every $1 of fraud, calculated as total losses divided by the amount of fraudulent transactions for which the firm is held liable

Step 1: Obtain average revenue	$57,558,739,932*
Step 2: Obtain fraud as % of annual revenue from Q10	2.39%
Step 3: Calculate total cost of fraud (Steps #1 x #2)	$313,032,747
Step 4: Obtain % of total losses (amount for fraudulent transactions held liable) (Q16a)	37%
Step 5: Calculate value of "amount for fraudulent transactions been held liable" (Steps #3 x #4)	$117,105,550
Step 6: Calculate total cost for every $1 of fraud (total cost in Step 3) / (amount of fraudulent transactions) ($313,032,747 / $117,105,550)	$2.67

* Reflects weighted data accounting for census representation by small, mid and large-sized firms by employee

Q16: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various fraud costs over the past 12 months.

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 segments within category at the 95% Confidence Interval

LexisNexis® RISK SOLUTIONS

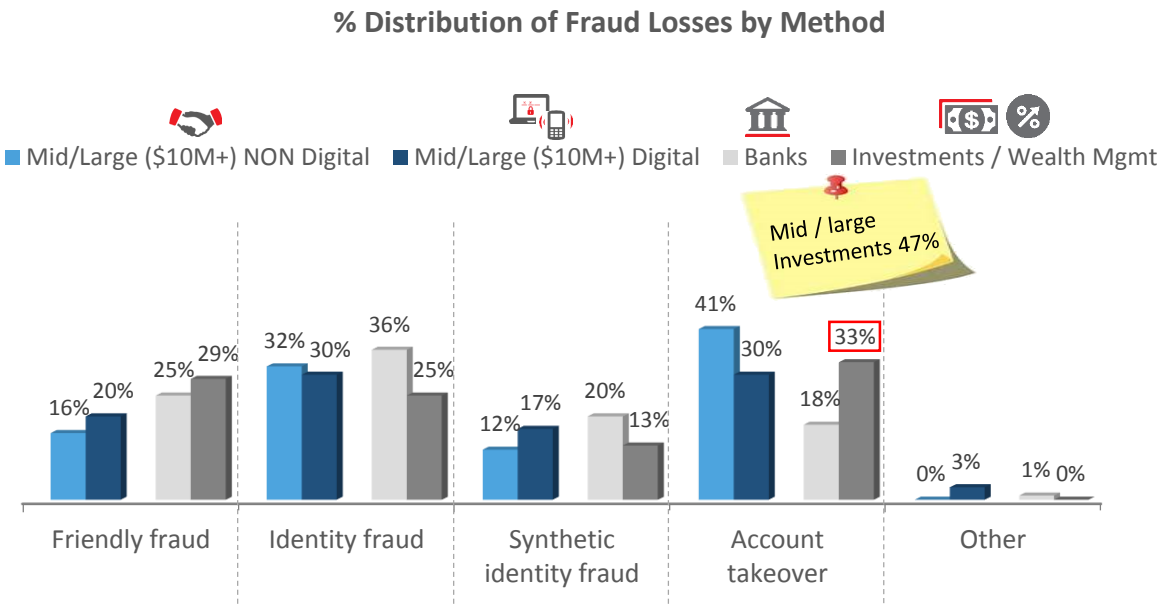
Identity fraud, including synthetic, accounts for directionally more fraud losses among large banks while account takeover is a threat to investment / wealth management firms.

For banks, over half (56%) of losses on average occur because of identity-related fraud. This grows to 62% among large banks ($50M+ revenues).

Fraud losses through account takeover are higher among investment firms, particularly mid / larger firms.

Among Large ($50M+) Banks, 62% of losses relate to identity fraud

- **42% identity fraud**
- **20% synthetic identity fraud**

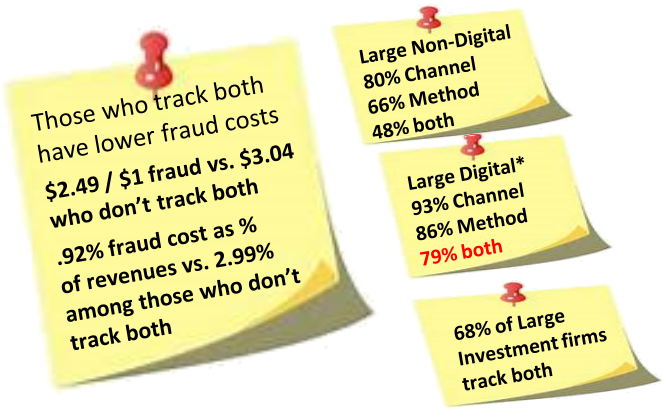


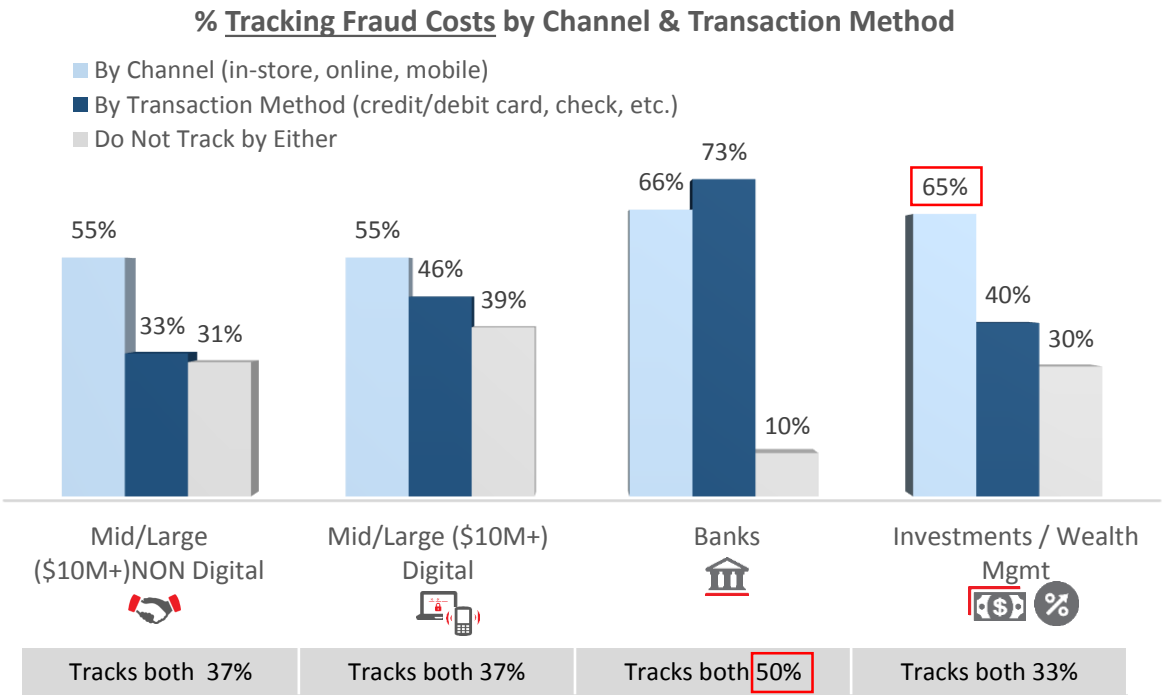
Q12: Please indicate the percentage distribution of the following fraud methods as attributed to your total annual fraud loss over the past 12 months.

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

Large digital firms are more likely to track fraud costs by both channel and payment method; it's the mid-sized firms ($10 to <$50M) that still lag on tracking fraud costs.

Financial services firms that do track fraud costs by both channel and payment method tend to experience lower fraud costs.





* CAUTION – Low N of 29

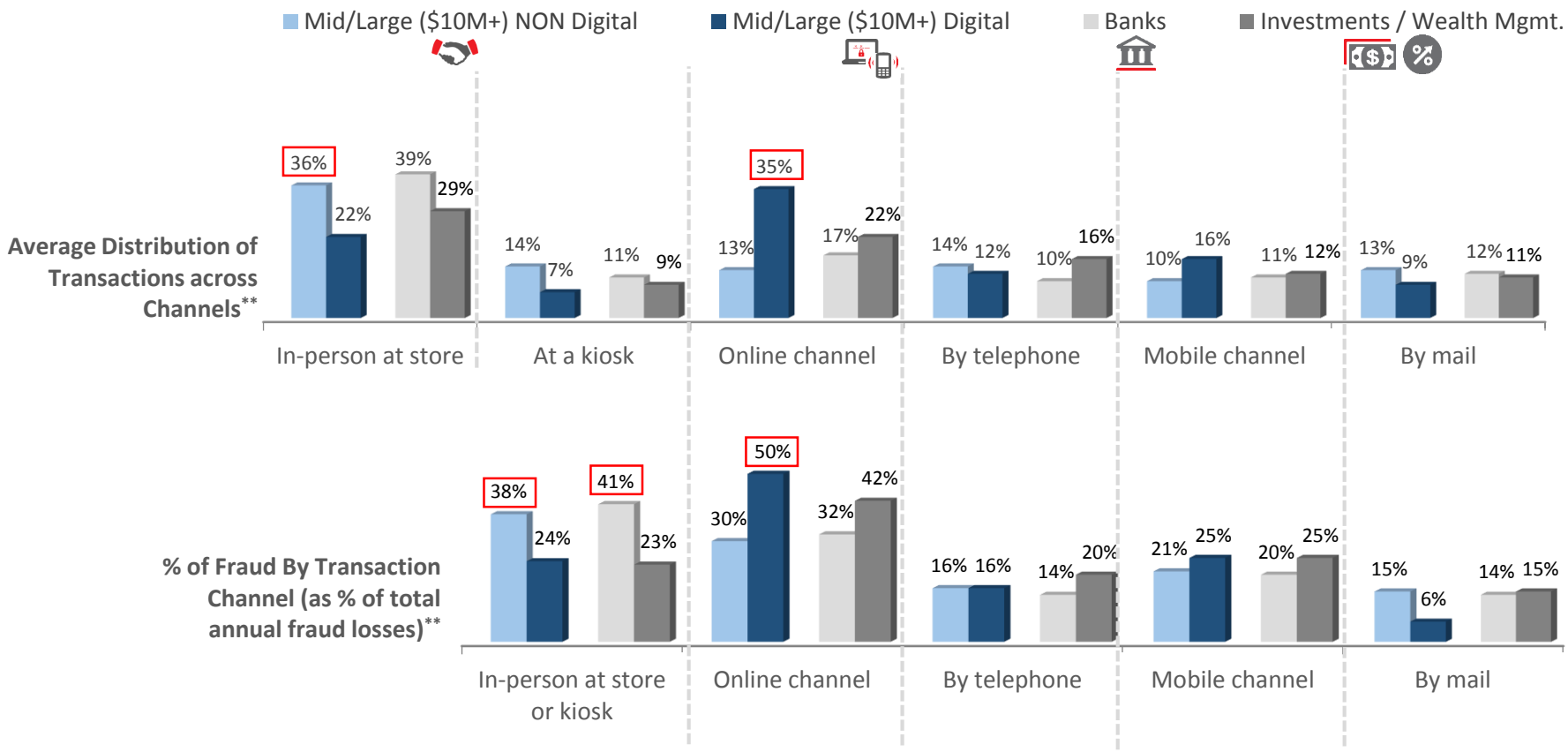
Q14: Does your company track the cost of fraudulent transactions by channels or methods?

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

Remote fraud also proves challenging.

LexisNexis®
RISK SOLUTIONS

While more online transactions occur among digital firms, online fraud is being experienced across organization type.



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

LexisNexis® RISK SOLUTIONS

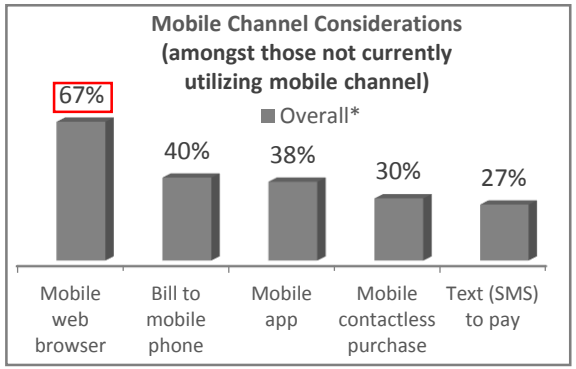
Q2: Please indicate the percentage of accounts or transactions that were originated through each of the following channels used by your company (over the past 12 months)
Q15: Please indicate the percent of fraud costs generated through each of the following transaction channels currently used by your company (as a percentage of total annual fraud losses)

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

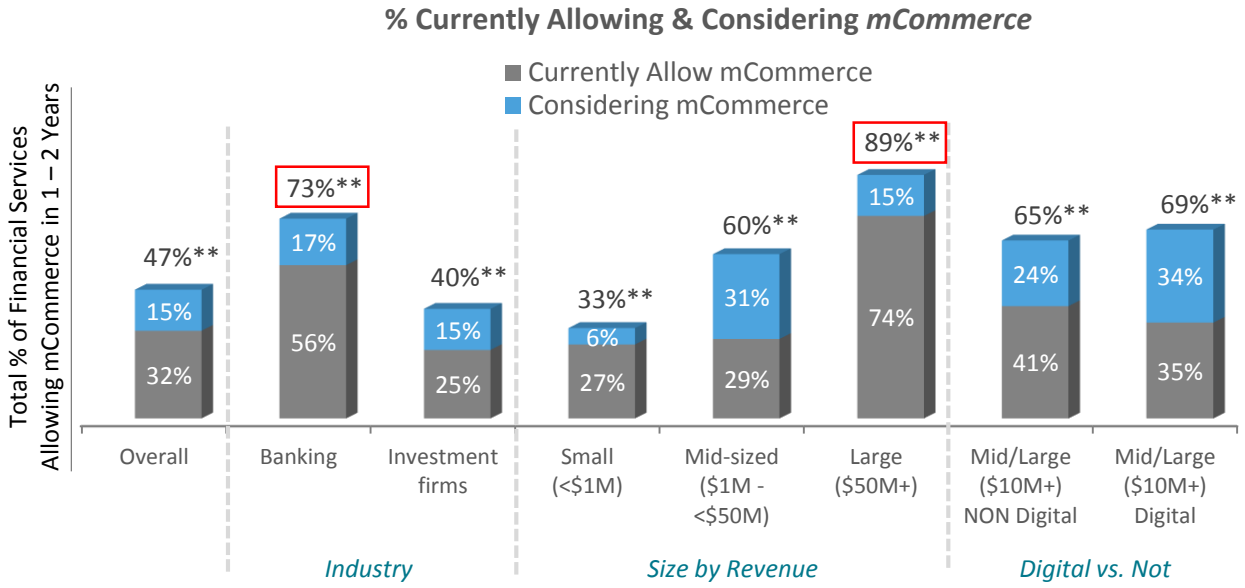
Mobile channel use is still emerging among financial services firms. Larger banks are more likely to be allowing it at this point, with anticipated growth from the mid/large segment.

Smaller firm mobile channel use is limited, with little anticipated near-term growth.

Lower mobile channel use among investment firms aligns with their heightened concerns about its security.



Q7: (For those with no current mobile channel, but considering) Which of the following types of transactions is your company considering offering in the next 12 months?



**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.

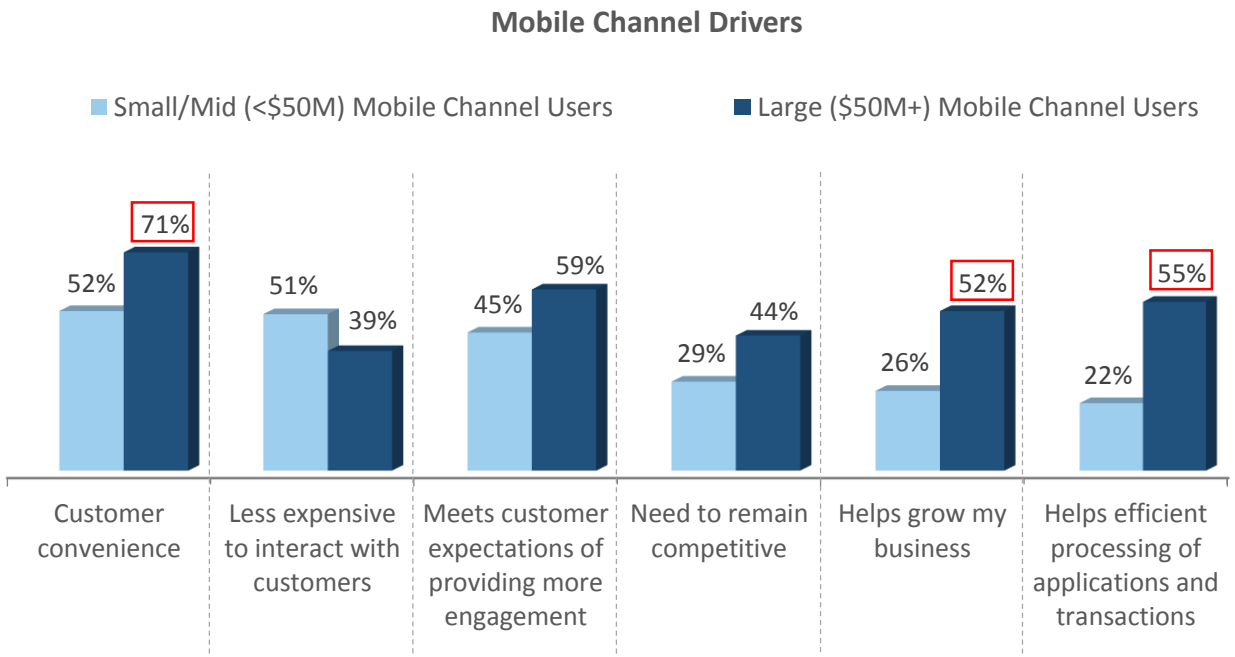
Q4: Please indicate the percentage of transactions completed (over the past 12 months) for each of the following payment channels currently accepted by your company.
Q6: Is your company considering accepting payments by mobile device over the next 12 months?

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

LexisNexis® RISK SOLUTIONS

Drivers for adopting the mobile channel differ by size of firm.

Large financial services firms using the mobile channel are doing so based on a range of reasons, including customer need / convenience which may also translate into growing the business. Further, adding an additional remote channel is viewed as providing more applications and transactional efficiencies.

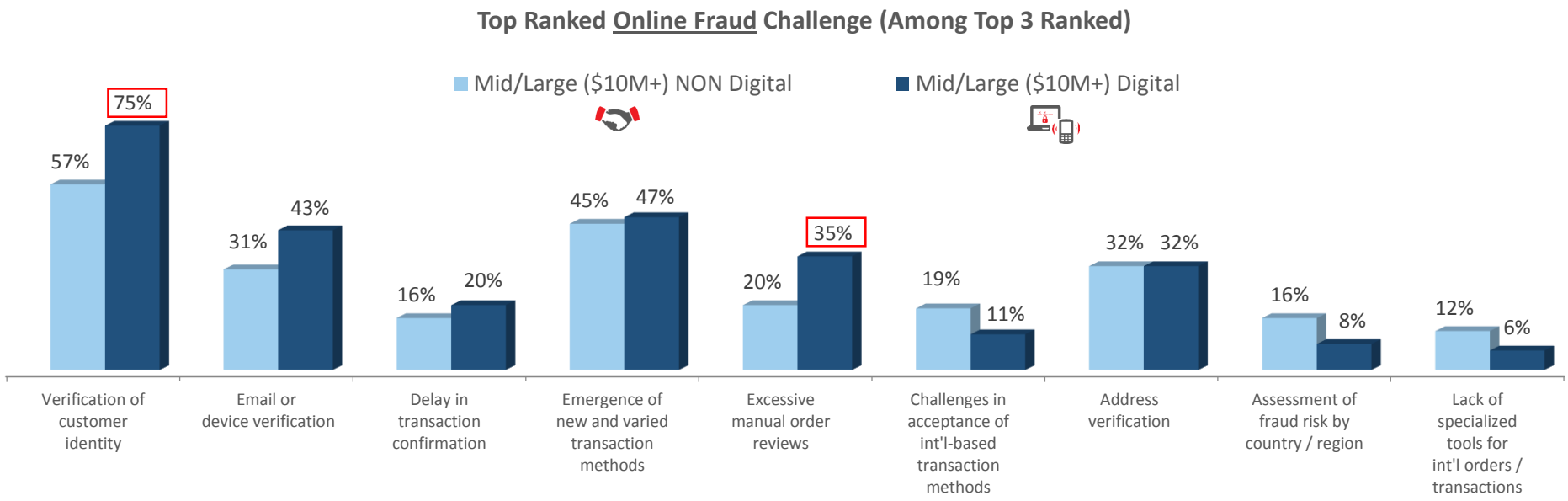


LexisNexis® RISK SOLUTIONS

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

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

Identity verification is significantly more of an online challenge for mid/large digital than non-digital firms, as are manual reviews and, directionally, e-mail / device verification.



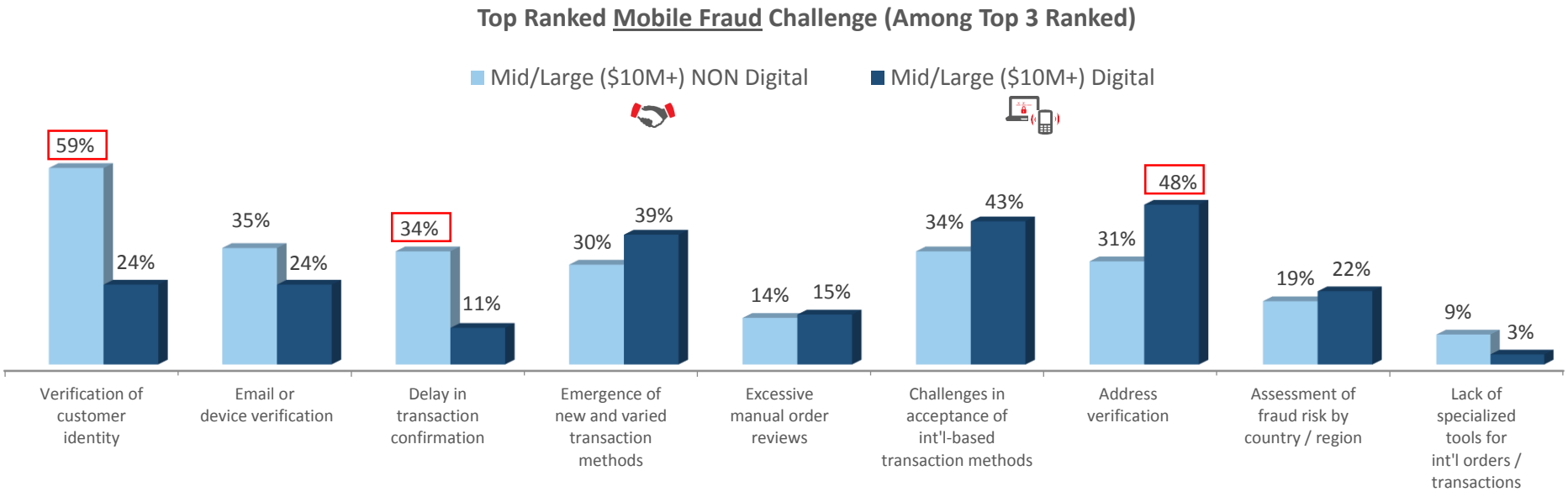
For financial services firms overall, KYC requirements can impact challenges with identity verification. The emergence of new and varied transaction methods can make this more challenging, particularly through remote channels. The larger online volume among digital likely explains a part of the reason that this is more of a challenge than among non-digital firms.

LexisNexis® RISK SOLUTIONS

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

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

With the mobile channel, identity verification is much more of a challenge among non-digital firms while address verification is a key issue for digital firms.



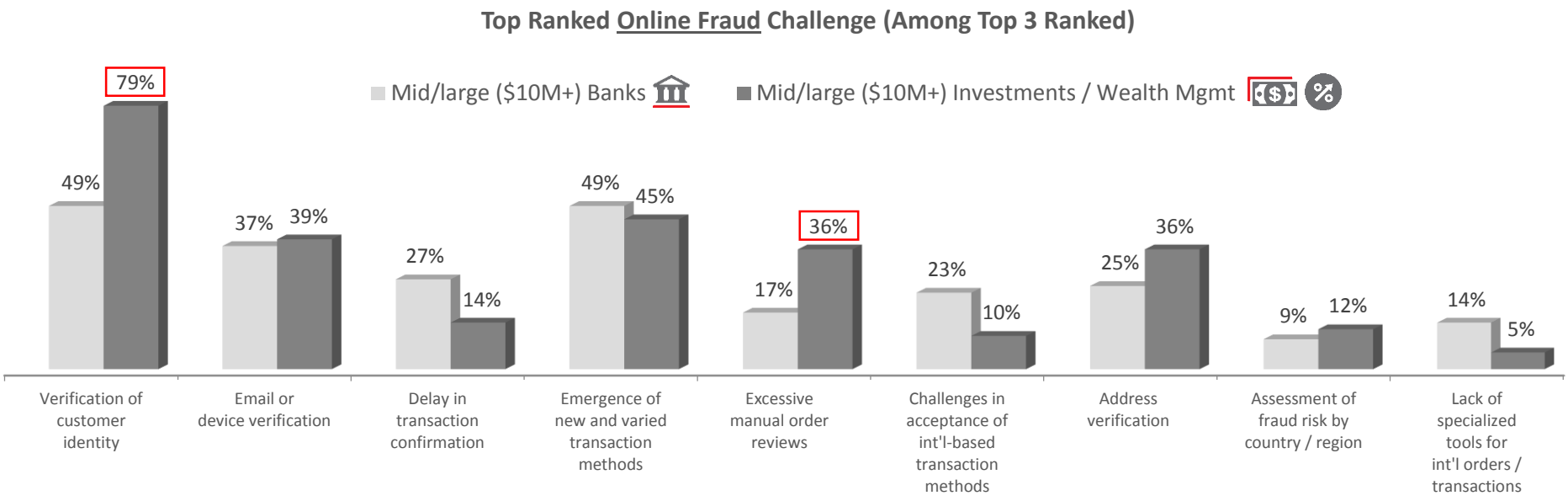
Non-digital firms may not have processes and solutions developed as much as those who conduct a majority of volume digitally. The emergence of new transaction methods can include apps that allow cardless ATM transactions, which adds risk.

LexisNexis® RISK SOLUTIONS

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

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

Identity verification and new / varied transaction methods are top online challenges for mid/large banks and wealth management firms, though identity is significantly more challenging for the latter.



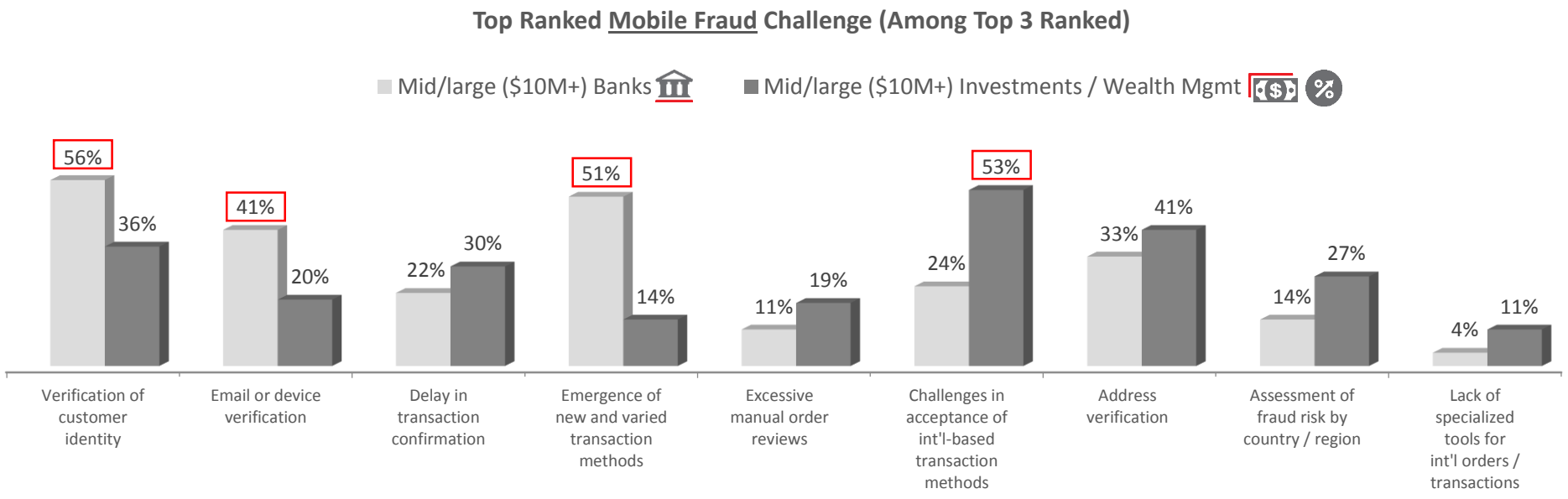
As shown later, many investment / wealth management firms are not using advanced identity verification solutions, which could relate to a higher percentage of fraud losses attributed to account takeover than cited by others. Excessive manual reviews are also more of a challenge for this segment, which could also be related to less use of these solutions.

LexisNexis® RISK SOLUTIONS

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

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

With the mobile channel, identity verification and new / varied transaction methods remain a top challenge for mid/large banks while challenges with international transactions is tops for investment firms.



With banks, new transaction methods accompany new ways that customers can pay for products and services. Just as with traditional card payment methods, these newer channels are not without risk of breaching by fraudsters.

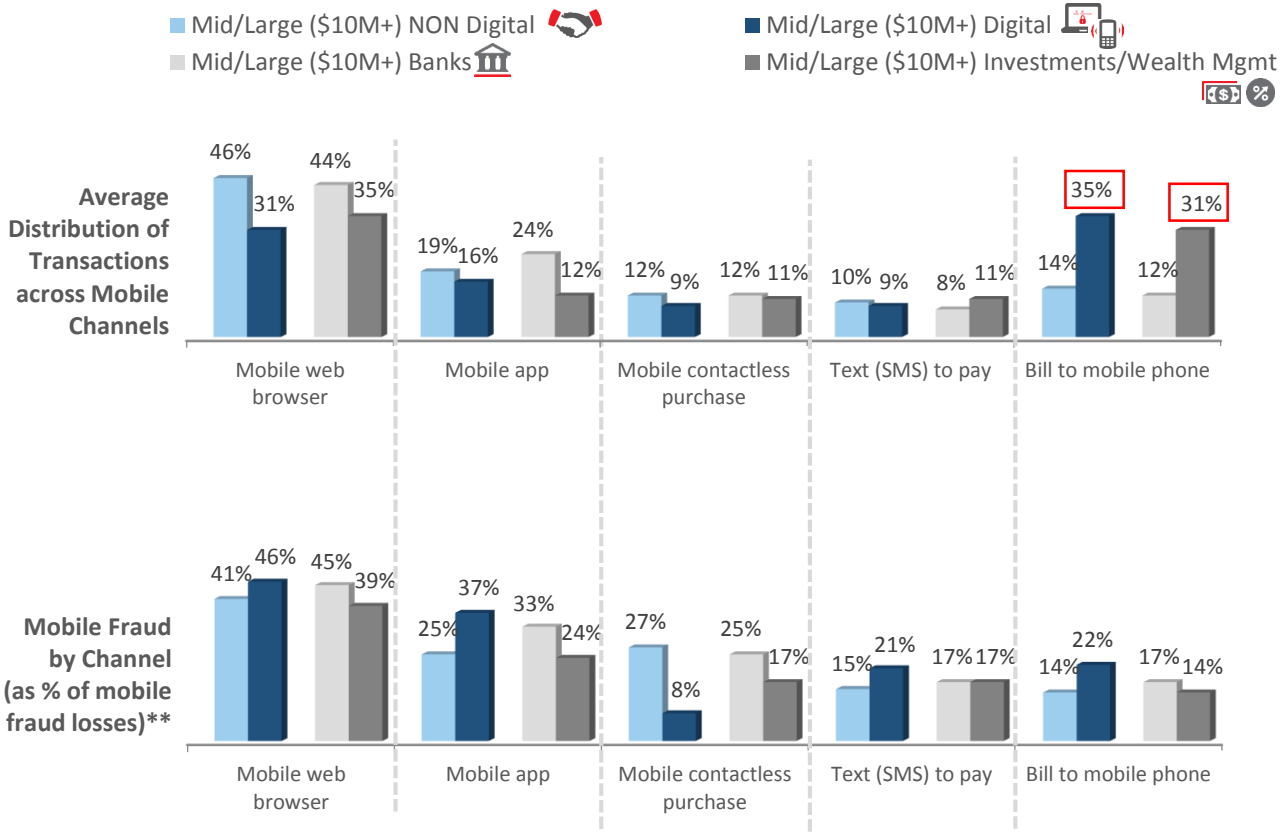
LexisNexis® RISK SOLUTIONS

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

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

A mobile browser is somewhat more common for mobile transactions, with also the larger share of mobile fraud losses.

Mid/large banks are somewhat more limited in their use of a mobile app compared to transactions through a mobile web browser. However, mobile apps accounts for nearly as much fraud losses; this could be related to card-less ATM transactions that permit customers to withdraw funds via their mobile phone.



*** % 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.

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

LexisNexis® RISK SOLUTIONS

Ineffective fraud prevention can be costly.

LexisNexis®
RISK SOLUTIONS

Fraud represents a significant portion of mid/large digital firms' monthly transactions.

Non-digital banks have significantly more monthly transactions on average than others. However, the percentage of fraudulent transactions is significantly higher among large ($50M+) investment firms – just under half, as well as mid/large digital firms.

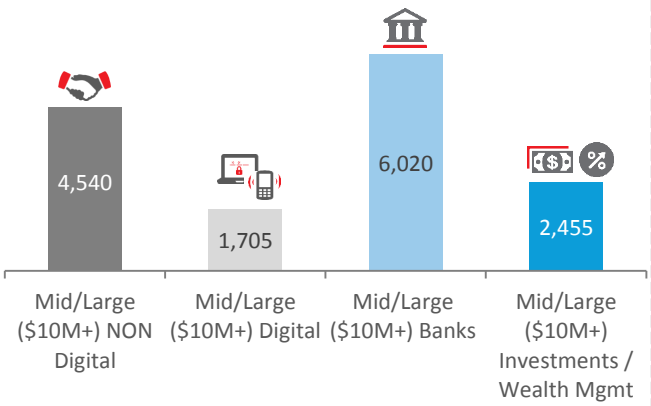
Also, while investment firms tend to have a smaller volume of monthly fraud attempts, 36% of those are successful.

Large Bank
- Avg. Mo. Trans. 5,150*
- Avg. Trans/Mo. That Are Fraud 1,630* (32%)

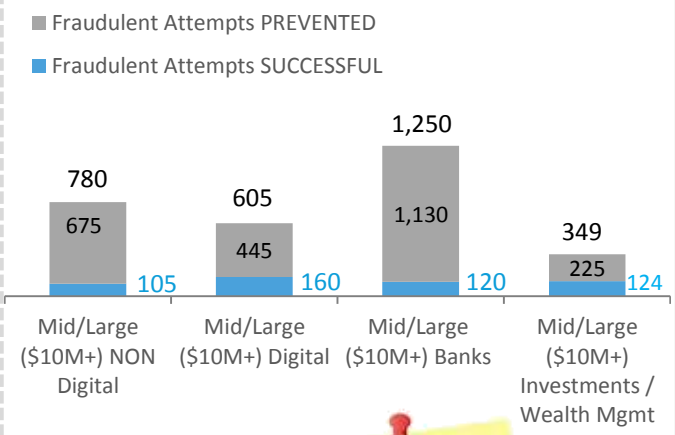
Large Investments
- Avg. Mo. Trans. 1,995*
- Avg. Trans/Mo. That Are Fraud 875* **(44%)**

Volume

Average Reported # Transaction Completions per Month *
(Rounded to Nearest 5 or 10 interval)



Average Reported Fraud Transactions per Month *



% Monthly Transactions That are Fraud

17%	**35%**	21%	9%

Mid/Large Investments
- Avg. 124 of 349 monthly fraud is successful; that's 36% of fraud attempts

LexisNexis® RISK SOLUTIONS

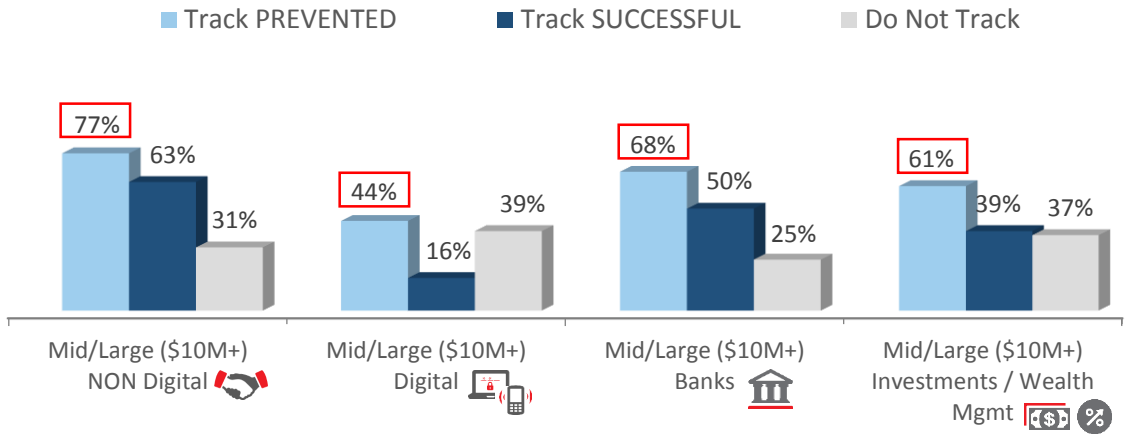
* Based on self-reported numbers and likely recall; not meant to be exact; may increase or decrease based on seasonality
Q21: In a typical month, what is the average number of transactions completed by your company?
Q22: In a typical month, approximately how many fraudulent transactions are prevented by your company?
Q23: Thinking of the fraudulent transactions that are prevented, what is the average value of such a transaction?
Q24: In a typical month, approximately how many fraudulent transactions are successfully completed (not prevented) at your company?
Q25: Thinking of the fraudulent transactions that are successfully completed (not prevented), what is the average value of such a transaction?

As with fraud costs, financial services firms also don't optimally track prevented and successful fraud transactions. This leaves gaps for fraudsters to leverage.

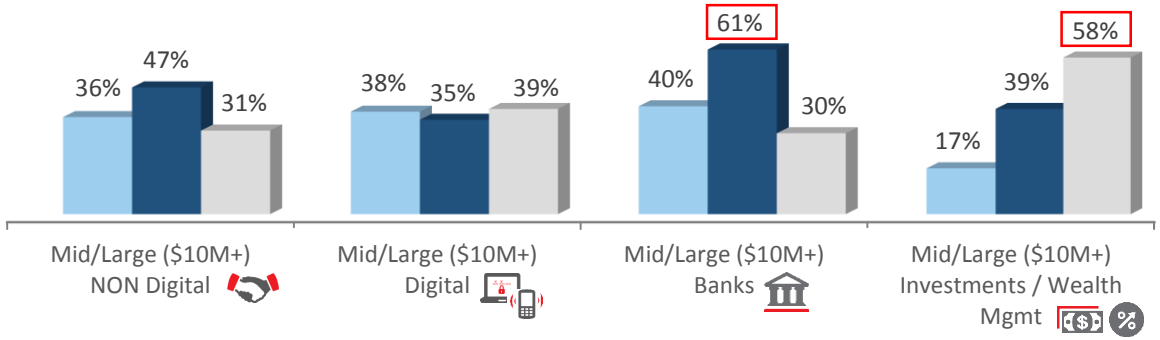
A majority of financial services firms are not tracking prevented and successful fraud by both transaction type and channel, which leaves the door open to fraudsters.

Mid/large digital firms are most at-risk by particularly not tracking successful fraud as much by channel; most of these firms are multi-channel, with heavy transaction risk through remote channels.

% Financial Services Tracking Prevented and Successful Fraud Transactions by Type



% Financial Services Tracking Prevented and Successful Fraud Transactions by Channel



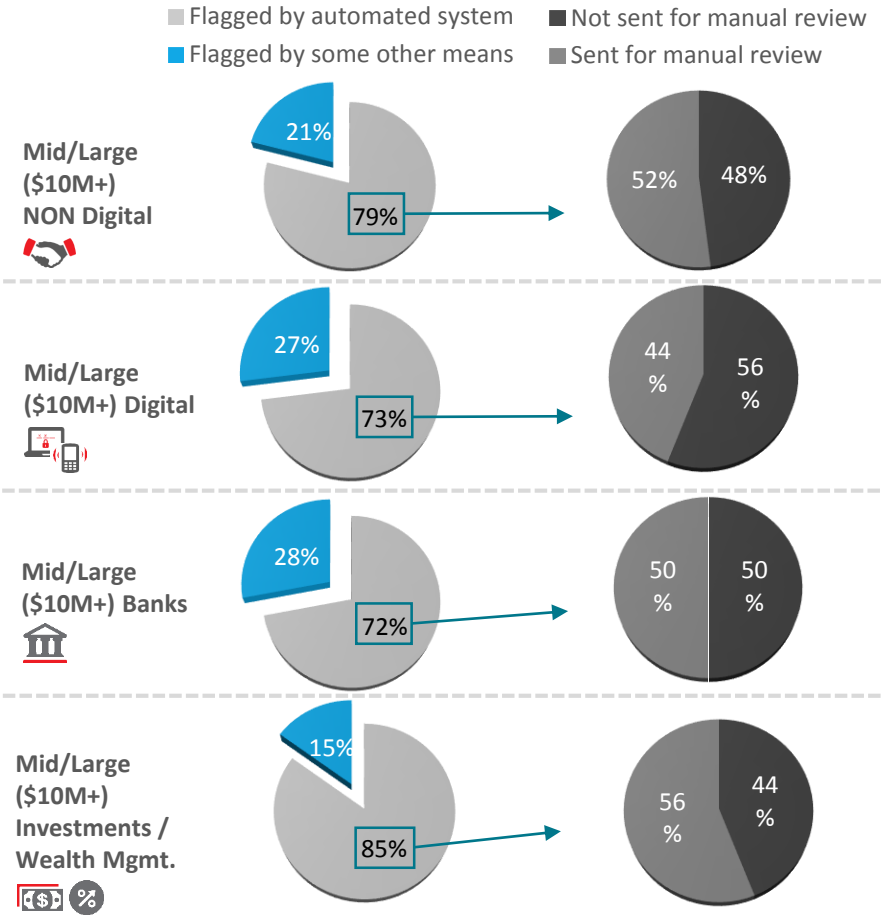
LexisNexis® RISK SOLUTIONS

Q26a: Does your company track prevented vs. successful transactions by type or channel?

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

A sizeable portion of financial services firms' flagged transactions are sent for manual review. But mid/large investment firms send considerably more.

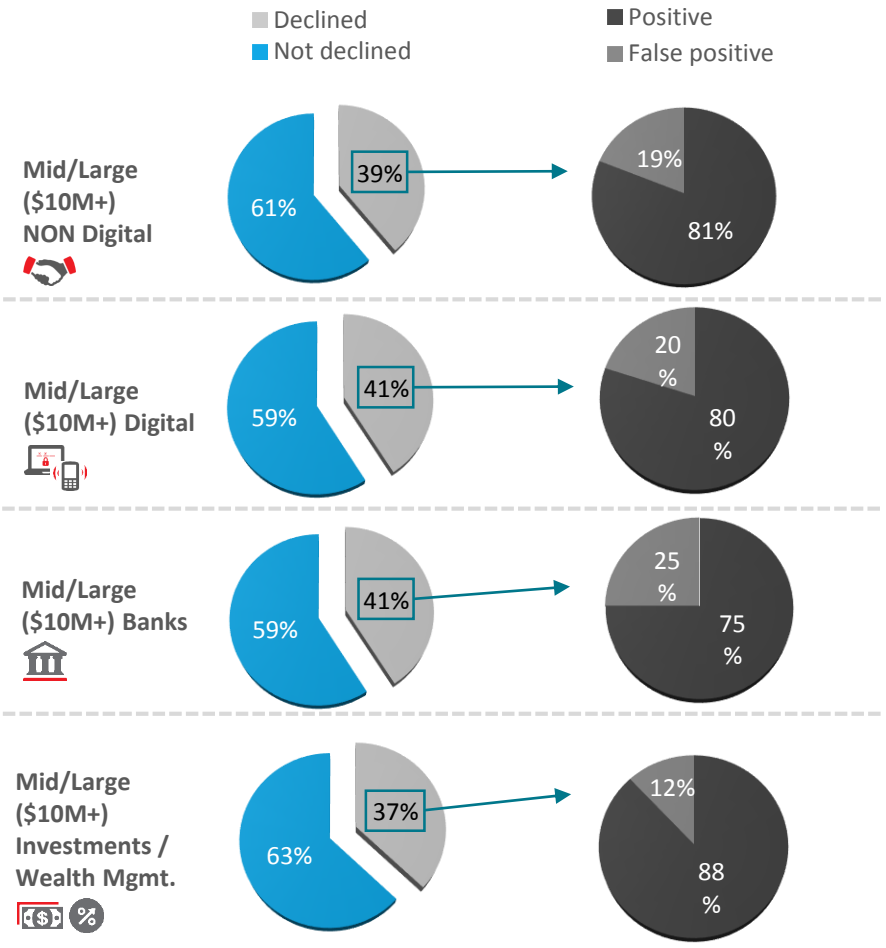
Of the 85% of investment firm transactions flagged by an automated system as potentially fraudulent, over half are sent for manual review.



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 automated system?
Q37: Of this (…), what proportion are sent for manual review?
Significantly different from other segments within category at the 95% Confidence Interval

Banks deal with directionally more false positives than others.



LexisNexis® RISK SOLUTIONS

Q38: What percentage of transactions that your company initially flags as potentially fraudulent are ultimately declined?
Q39: What percentage of declined transactions turned out to be false positives?
Significantly different from other segments within category at the 95% Confidence Interval

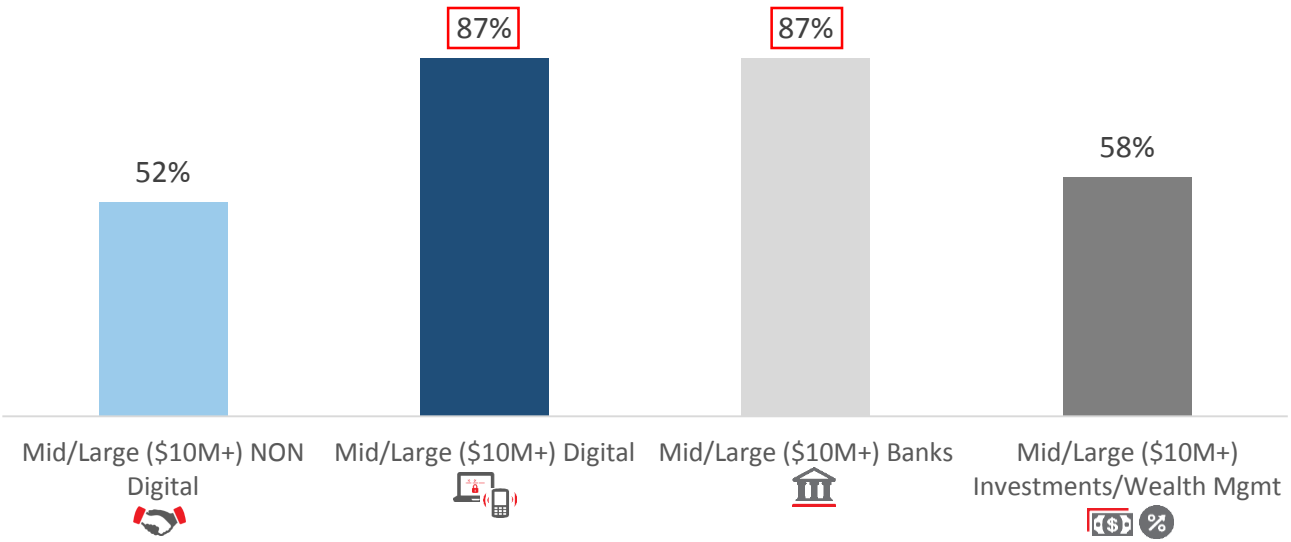
Some financial services firms are not using the RIGHT mix to successfully prevent fraud.

LexisNexis®
RISK SOLUTIONS

Digital financial services firms, particularly mid/large banks, are very likely to use more fraud mitigation solutions than are others, though not always optimally.

While using more risk mitigation solutions, digital firms still get hit with higher fraud costs and a higher percentage of monthly transactions that are fraudulent. Less effective tracking can contribute to this, but it could also be related to not using the right mix of solutions as well.

% Financial Services Who Use a Fraud Mitigation Solution



Average Number of Fraud Mitigation Solutions Currently Used

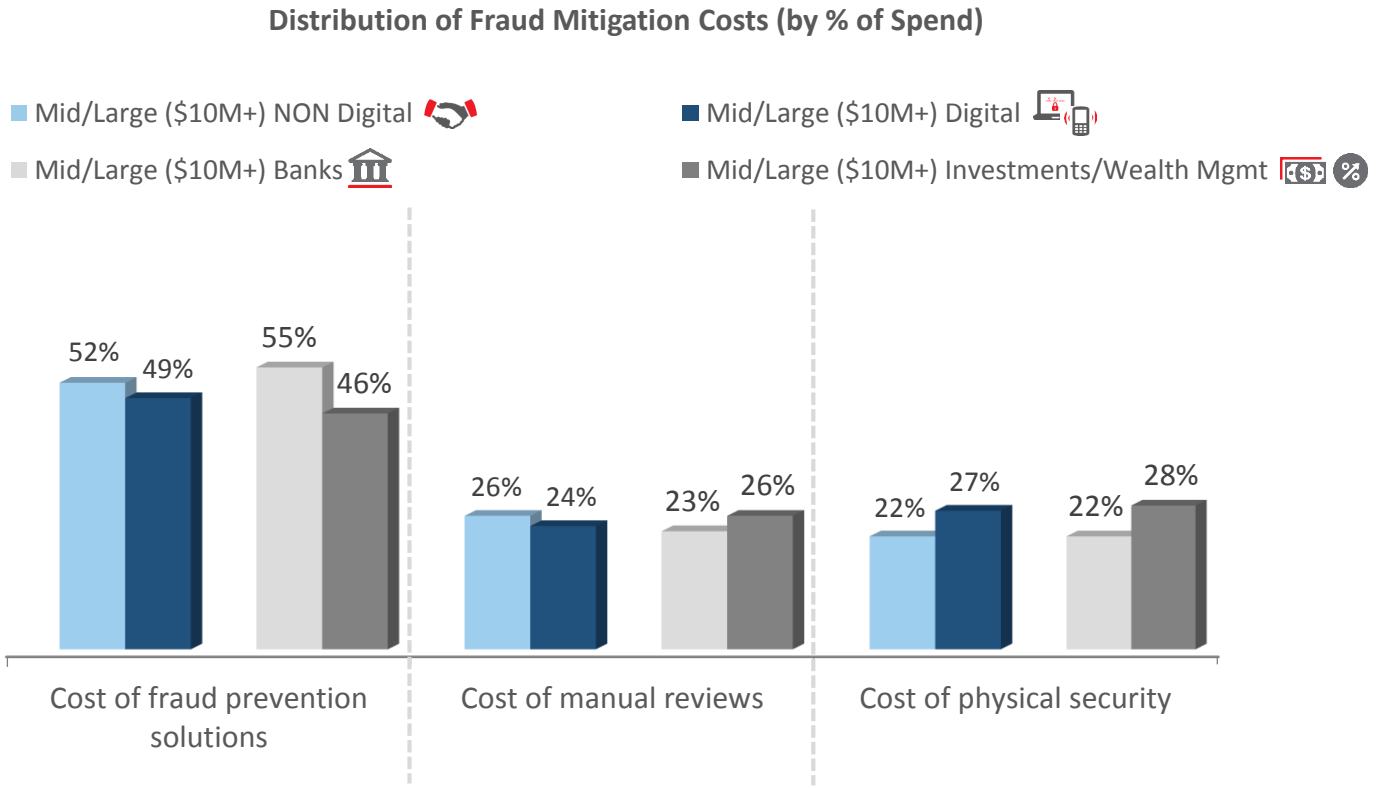
3.5	6.3	6.4	3.9

LexisNexis® RISK SOLUTIONS

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

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

Solutions are a significant portion of financial services firms' fraud mitigation budgets. However, manual reviews still take a sizeable bite out of their budgets as well.

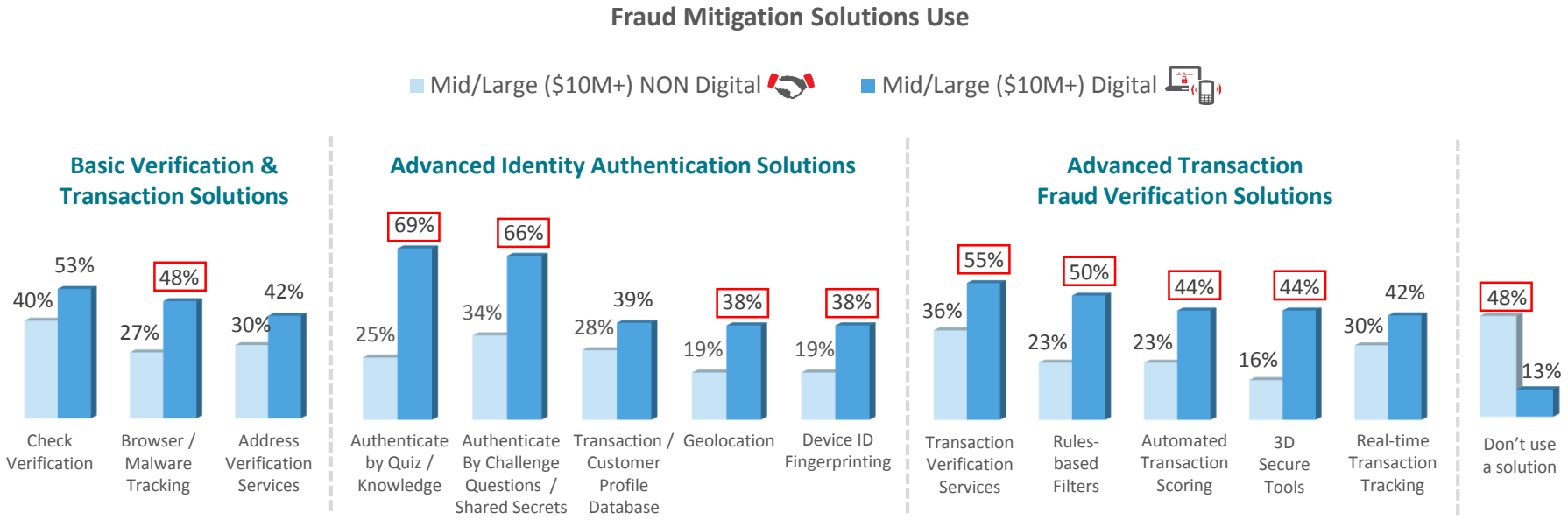


LexisNexis® RISK SOLUTIONS

Q41b: What is the percentage distribution of mitigation costs across the following areas in the past 12 months?

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

Quiz/challenge-based identity authentication solutions are prevalently used by mid/large digital firms, though other identity solutions are used less often.



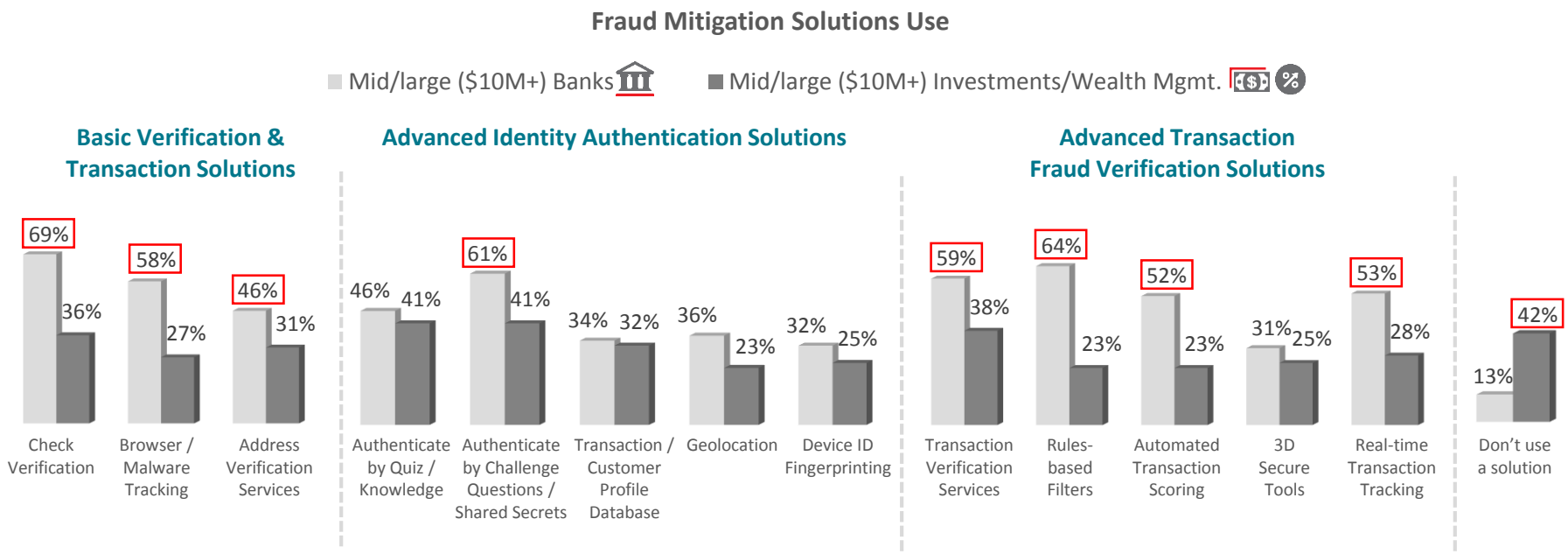
With moderate use of fraud transaction solutions and some identity authentication ones, many digital firms are on the right path towards managing fraud; however, since they are getting hit harder by fraud, it also suggests that they could further optimize the ways in which they bundle or layer solutions. Mid/large non-digital firms using a solution (average of 3.5) vary considerably in those which are chosen, suggesting less consensus around which solutions are most effective for specific fraud types and events.

LexisNexis® RISK SOLUTIONS

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

Many transaction-based solutions are used by just over half of mid/large banks, while identity-based solutions use is more limited.



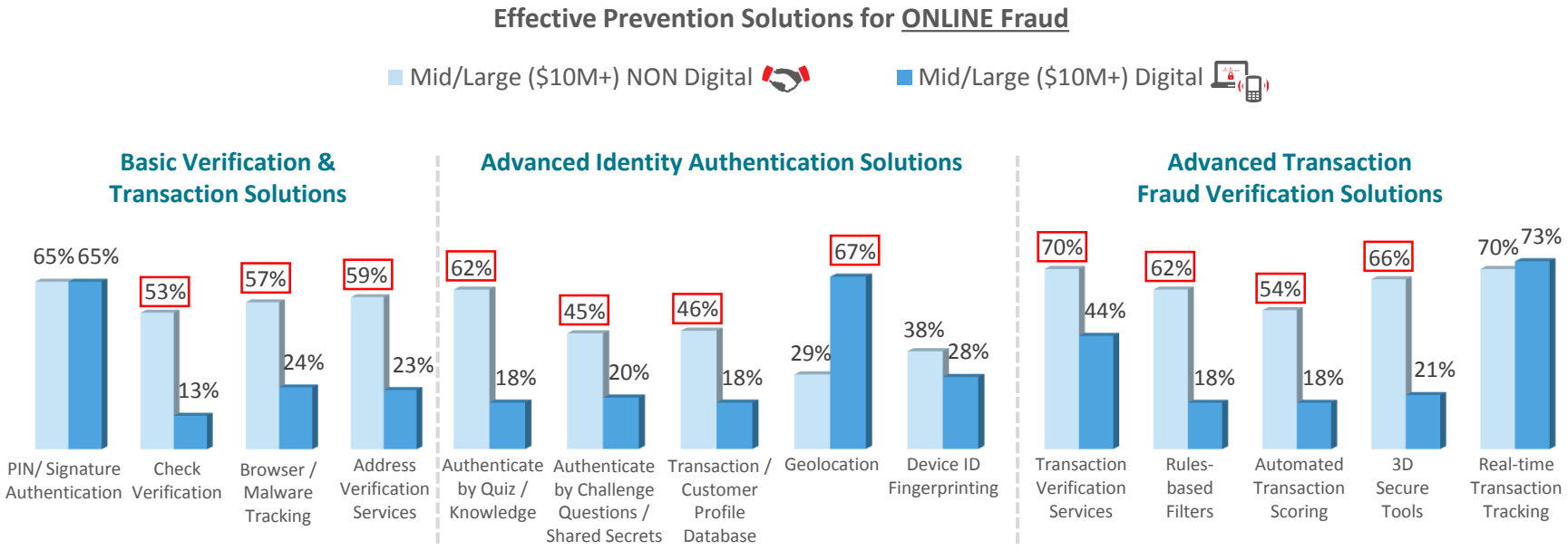
This could explain, in part, the challenge that banks cite with identity verification and the higher percentage of fraud losses related to this. It also suggests variation with bundling rather than a layered approach.

LexisNexis® RISK SOLUTIONS

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

Interestingly, there is little consensus among mid/large digital firms about which solutions effectively prevent online fraud.



Given the fragmentation of solutions indicated by digital firms, it suggests that they are not thinking about a layered approach but rather a select few which will solve their issues. That creates opportunity for customer education.

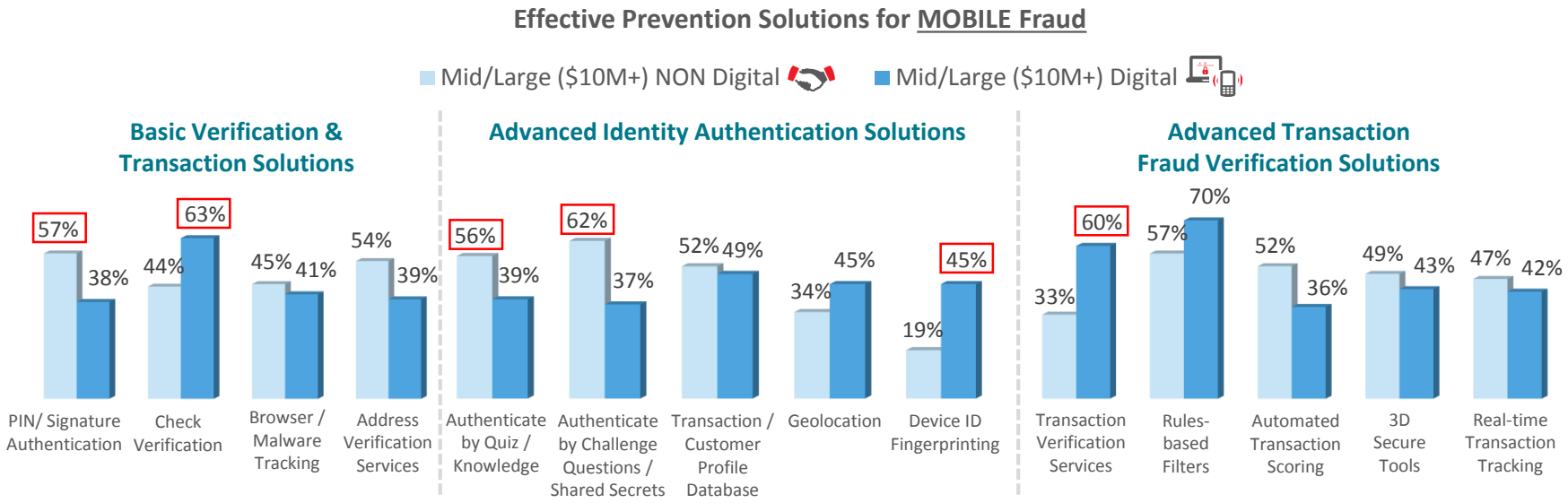
LexisNexis® RISK SOLUTIONS

*CAUTION – low base size N = 31

Q29: Which of the following fraud solutions do you believe are effective for preventing online fraud?

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

Mid/large digital firms lean more towards some transaction-based solutions as effective for preventing mobile fraud, with fewer including advanced identity solutions in this mix.



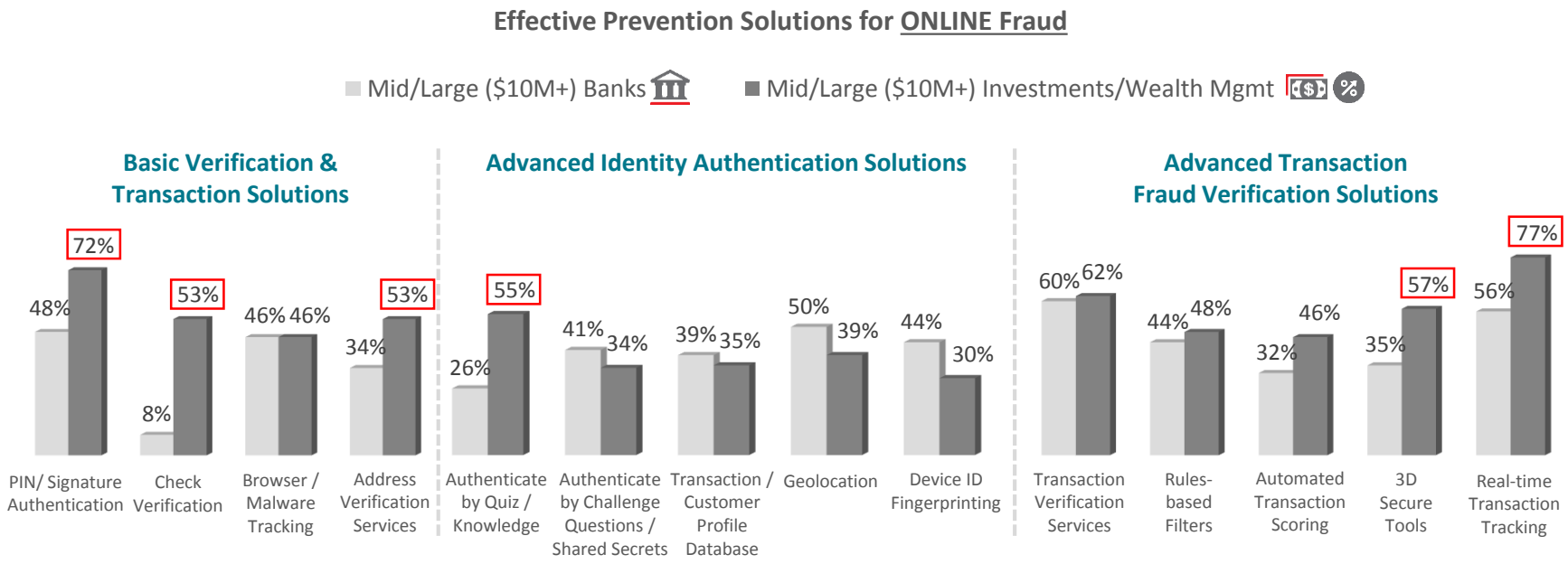
Mid/large non-digital firms vary, though with half or more pointing to advanced identity authentication by quiz / challenge questions. Again, this suggests that they are not thinking in terms of solutions layering.

LexisNexis® RISK SOLUTIONS

Q29: Which of the following fraud solutions do you believe are effective for preventing mobile fraud?

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

There is little consensus among mid/large banks as to which solutions can best prevent online fraud.



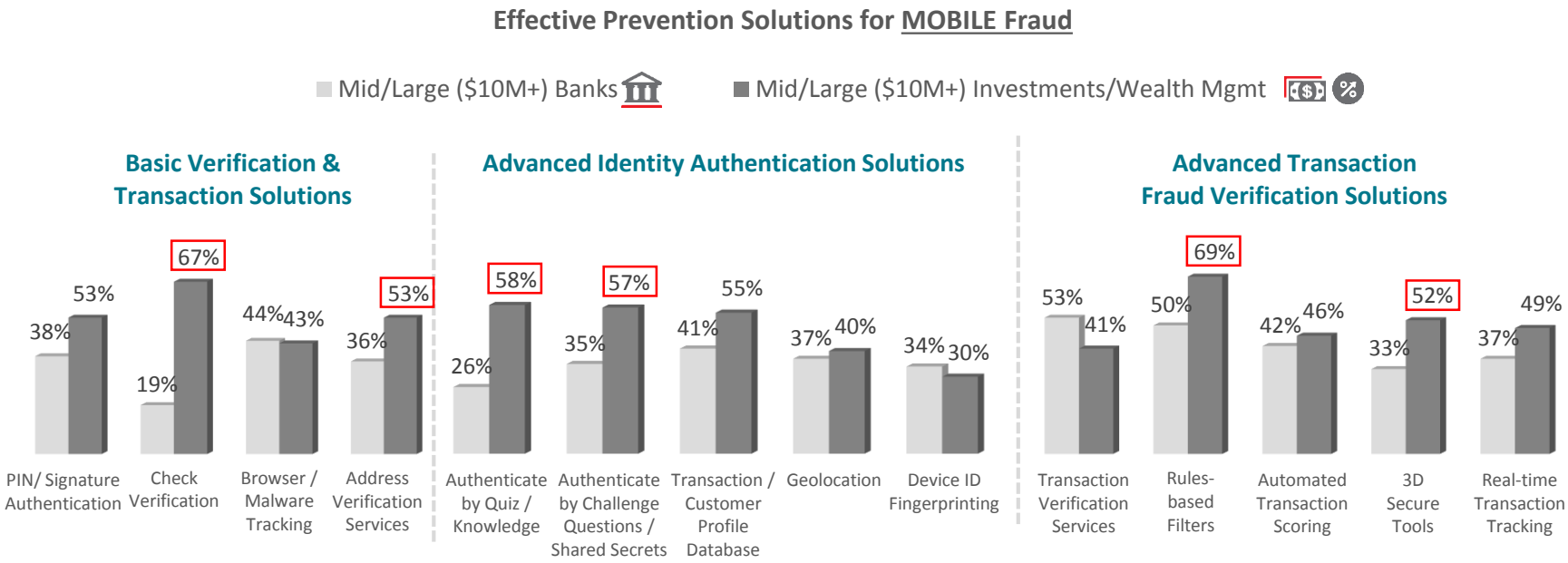
Over half of mid/large investment firms cite different fraud transaction verification solutions while also selecting more traditional PIN/signature, check and address verification. Fewer banks and investment firms think about identity verification solutions.

LexisNexis® RISK SOLUTIONS

Q29: Which of the following fraud solutions do you believe are effective for preventing online fraud?

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

There is also less consensus among mid/large banks regarding which solutions can best prevent mobile fraud.



For mobile, over half of mid/large investment firms cite identity verification solutions – more so than they did for online fraud prevention.

LexisNexis® RISK SOLUTIONS

Q29: Which of the following fraud solutions do you believe are effective for preventing mobile fraud?

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

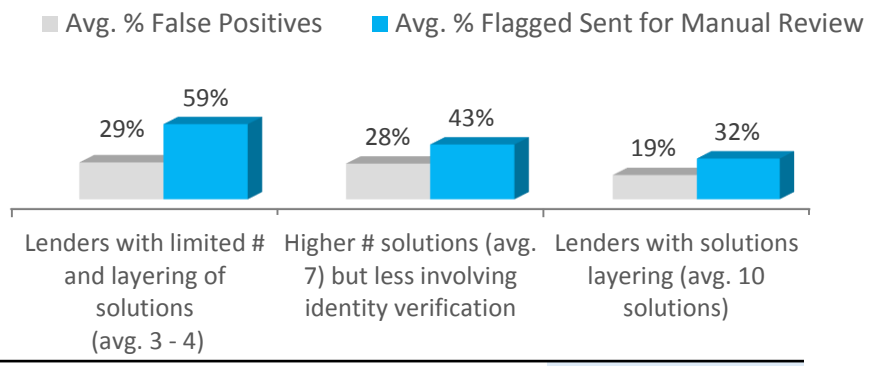
Using the right combination of tools is crucial.

LexisNexis®
RISK SOLUTIONS

Financial services firms which layer identity & fraud transaction-based solutions experience fewer false positives and need for manual reviews.

Survey findings show that it's not just about having a high number of solutions, but rather the right mix that layers advanced identity verification and fraud transaction solutions. Survey respondents who have many solutions, but are light on bundling all three layers, have more false positives and manual reviews than those bundling all three layers.

Effectiveness by Number & Layering of Fraud Mitigation Solutions



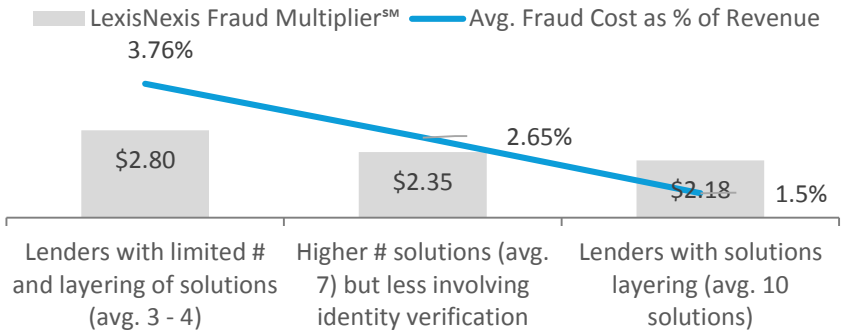
Layers of Protection		Limited	Limited	Multi-Layered
Common Core Solutions Used Most Often	Card verification, PIN/Signature, Check Verification, Browser Malware, Address Verification	Mostly	Many	✓
Layering of Advanced Identity Solutions	Device ID Fingerprinting, Geolocation, Authentication by Quizzes, Authentication by Challenge Questions, Customer Profile Database	Minimal	Minimal	✓
Layering of Fraud Transaction Risk Assessment Solutions	Automated Transaction Scoring, Real-Time Transaction Tracking, Transaction Verification, Rules-Based Filters, Authentication of Transaction by 3D Tools	Minimal	Many	✓

LexisNexis® RISK SOLUTIONS

And, there is less cost of fraud for financial services firms who layer identity & fraud transaction-based protection.

Those who layer core + identity + fraud transaction solutions have lower fraud costs ($2.18 for every $1 of fraud) than others (up to $2.80 per $1 of fraud). Relatedly, those who layer these solutions have lower fraud costs as a percent of annual revenues as well.

LexisNexis Fraud Multiplier℠ and 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 Solutions	Device ID Fingerprinting, Geolocation, Authentication by Quizzes, Authentication by Challenge Questions, Customer Profile Database	Minimal	Minimal	✓
Layering of Fraud Transaction Risk Assessment Solutions	Automated Transaction Scoring, Real-Time Transaction Tracking, Transaction Verification, Rules-Based Filters, Authentication of Transaction by 3D Tools	Minimal	Many	✓

LexisNexis® RISK SOLUTIONS

Recommendations

LexisNexis®
RISK SOLUTIONS

Recommendations

1

Financial services firms should consider a multi-layered solution approach that attacks different types of fraud.

- It is critical for merchants 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.

2

Mid/large financial services firms that allow online / mobile transactions need to embrace this multi-layered solution approach sooner rather than later.

- It is very likely that the volume of digital transactions will only grow over time, particularly via the mobile channel.
- The pain points and higher fraud costs experienced by these firms should increase accordingly, perhaps even more so as new and varied mobile payment methods place challenges on current legacy solutions and processes.
- On top of that, it is possible that increased channel options will increase transaction volumes; if left unaddressed, issues with identity verification and manual reviews could overwhelm digital financial services firms.
- And, as customers continue to seek the convenience of online and mobile transactions, particularly Millennials who are most accustomed to the digital space, it is likely that patience with customer friction will "wear thin".

Recommendations (cont.)

3

Digital financial services firms need to implement unique risk mitigation solutions for remote channels.

- While there are similarities between online and mobile channel challenges, they differ in terms of priorities.
- Additionally, there are unique challenges between channels.
- Therefore, the same solution may not be as effective in supporting both channels at the same time.

4

Financial services firms, particularly digital ones, need to track both payment and channel fraud – in terms of costs and successful attempts.

- Fraud occurs in multiple ways, particularly for multi-channel merchants (given overlap between use of online and mobile channels). The remote channel, of course, is important to monitor in comparison to physical POS locations since the anonymity of online and mobile make these channels more high risk. Additionally, there are different security issues and approaches between online and mobile channels.
- But, the rise of synthetic identities makes it easier for fraud via different transaction methods in remote channels.

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

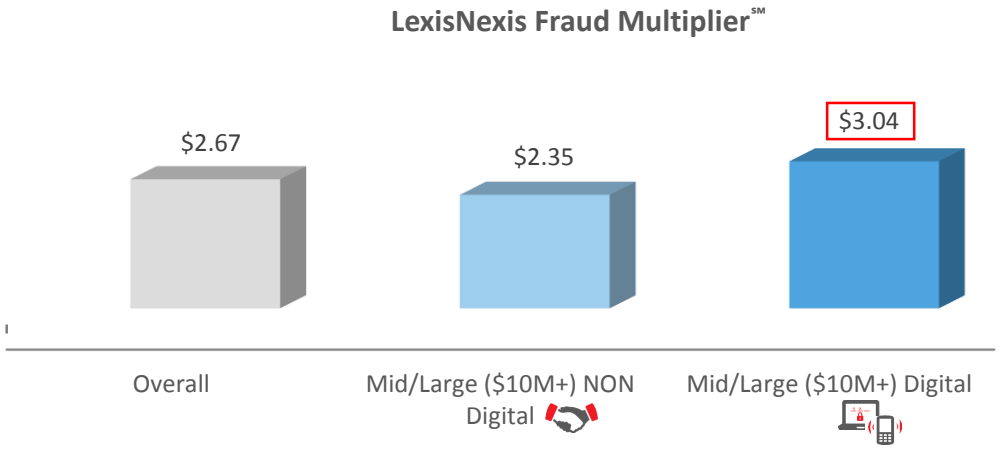
Appendix

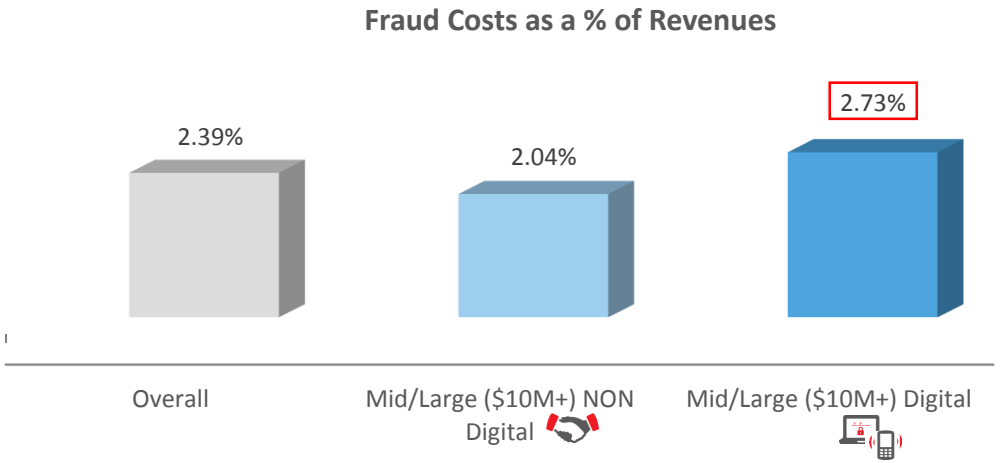
LexisNexis®
RISK SOLUTIONS

Having a sizeable digital presence can increase fraud costs if not effectively managed.

For every $1 of fraud, it costs mid/large digital financial services firms $3.04 compared to $2.35 for non-digital mid/large firms.

Further, fraud costs as a percentage of revenues is higher among mid/large digital firms than non-digital ones.





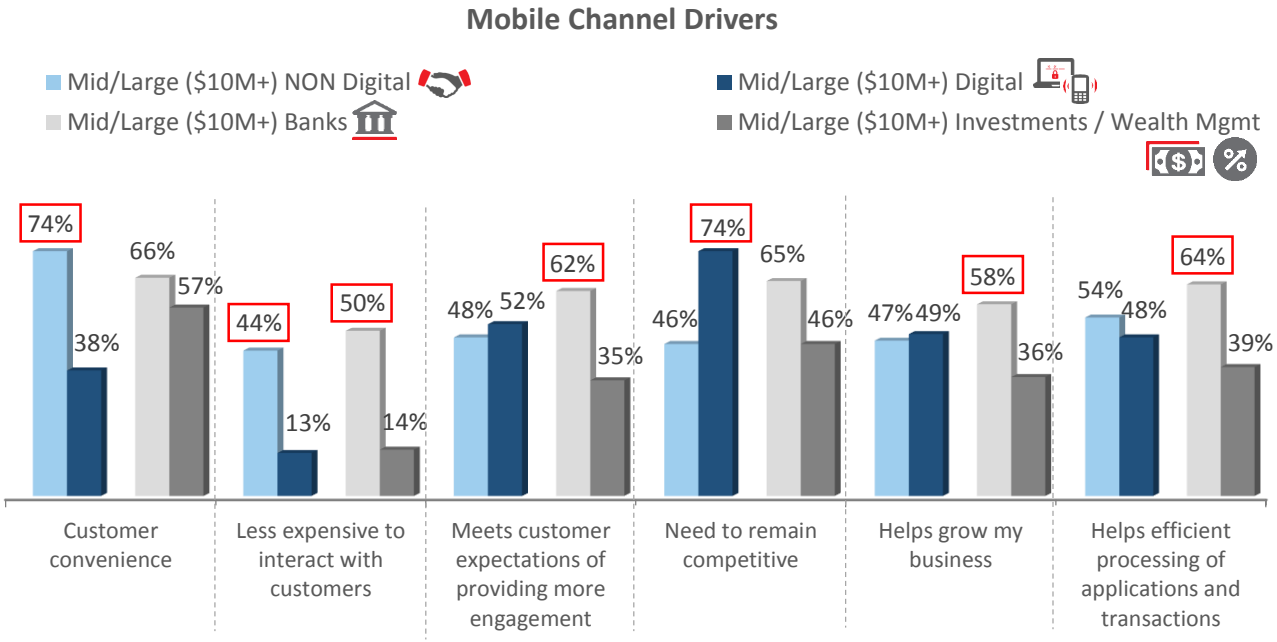
LexisNexis® RISK SOLUTIONS

Q16: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various fraud costs over the past 12 months.
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 segments within category at the 95% Confidence Interval

Drivers for adopting the mobile channel differ by type of firm, suggesting different environments and challenges impacting such decisions.

Mid/large digital commonly see it as a means of remaining competitive in their remote channel space, while non-digital are offering it for convenience but not necessarily as a growth strategy.

Even though larger banks have been quicker to adopt the mobile channel, for reasons related to both the customer, competition and internal efficiencies, they still have concerns about its security and risk.



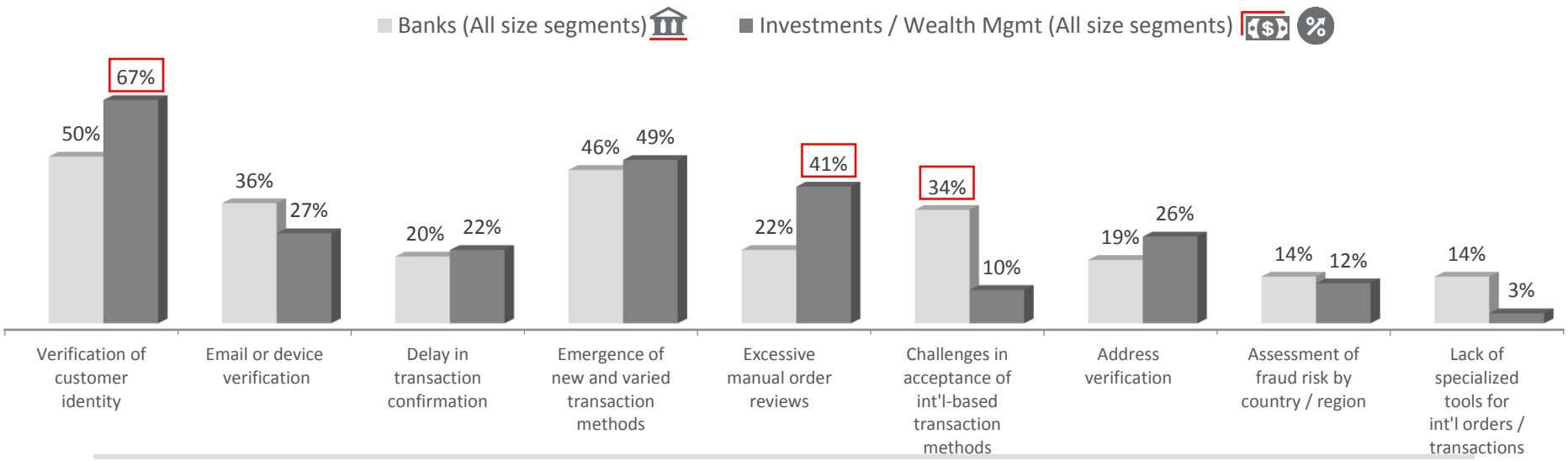
LexisNexis® RISK SOLUTIONS

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

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

Identity verification and new / varied transaction methods are top online challenges for both banks and investment/wealth management firms, with excessive manual reviews as a challenge for the latter.

Top Ranked Online Fraud Challenge (Among Top 3 Ranked)



Online identity verification is even more of a challenge among investment / wealth management firms, which could relate to a higher percentage of fraud losses attributed to account takeover than cited by others.

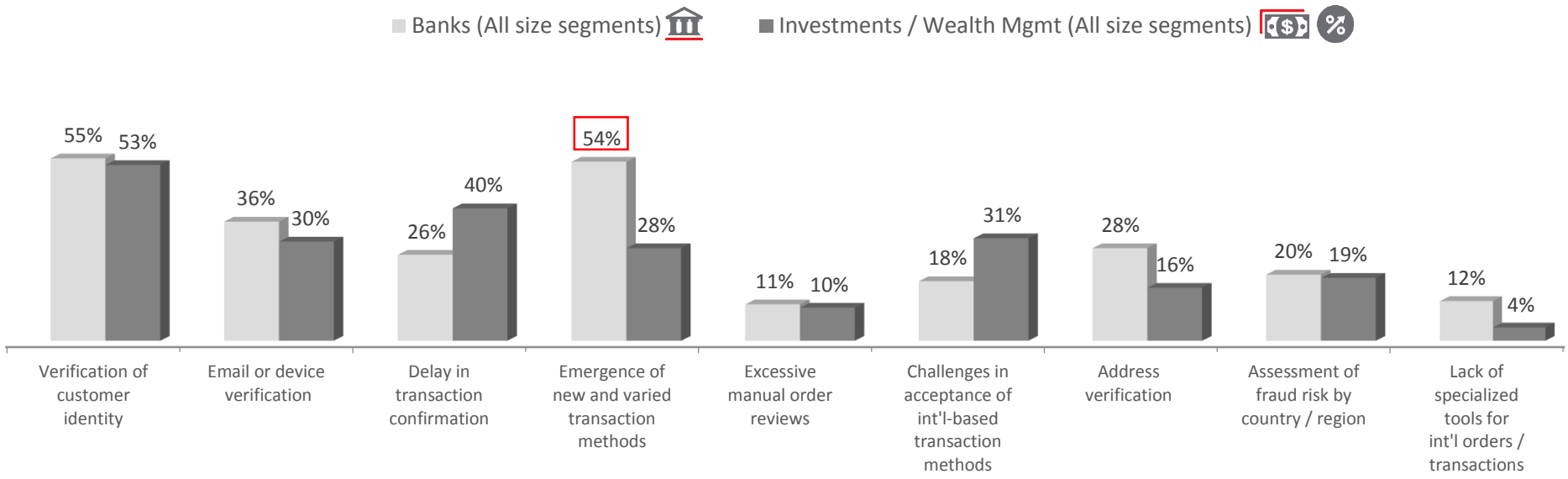
LexisNexis® RISK SOLUTIONS

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

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

With the mobile channel, identity verification remains a top challenge for both banks and investment/wealth management firms, with new / varied transactions methods remaining an issue for banks as well.

Top Ranked Mobile Fraud Challenge (Among Top 3 Ranked)



LexisNexis® RISK SOLUTIONS

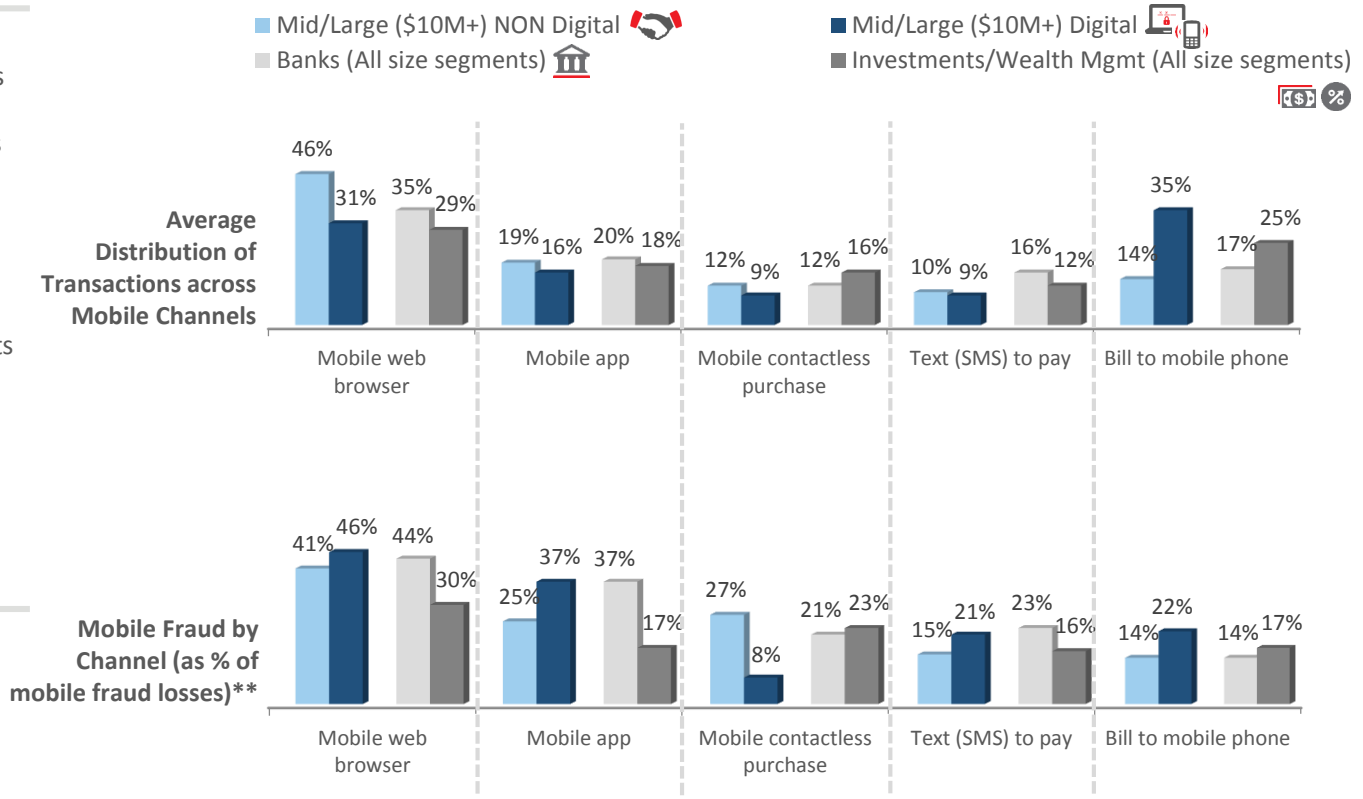
Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers in the Online Channel.

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

A mobile browser is somewhat more common for mobile transactions, with also the larger share of mobile fraud losses. A limited degree of transactions are also going through other mobile channels.

Mid/large digital firm transactions go through bill-to-mobile phone as often as through a mobile web browser. Interestingly, the mobile web browser is generating more fraud losses for them.

Banks are somewhat more limited in their use of a mobile app compared to transactions through a mobile web browser. However, mobile apps accounts for nearly as much fraud losses; this could be related to card-less ATM transactions that permit customers to withdraw funds via their mobile phone. Smartphone banking apps can also be hacked in the form of account takeover as well.



*** Standardized to 100%; actual % 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.

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

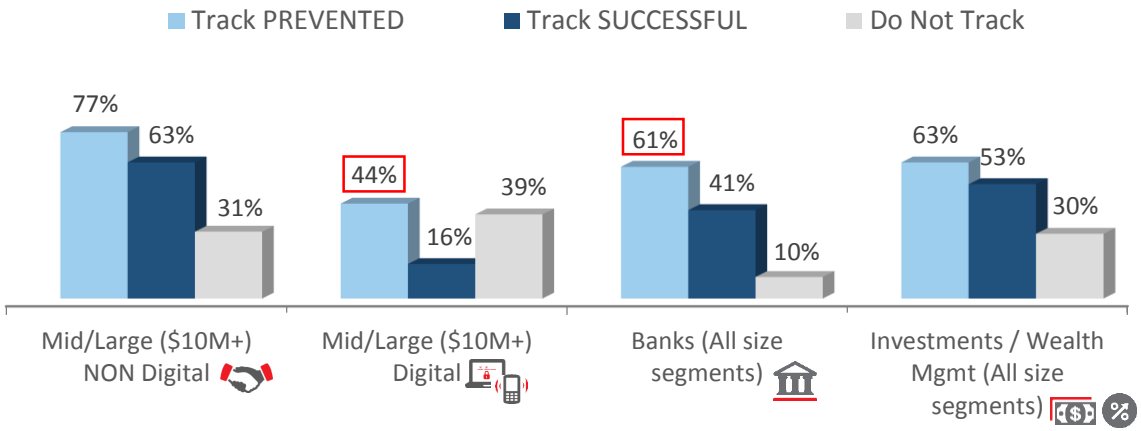
LexisNexis® RISK SOLUTIONS

As with fraud costs, financial services firms also don't optimally track prevented and successful fraud transactions. This leaves gaps for fraudsters to leverage.

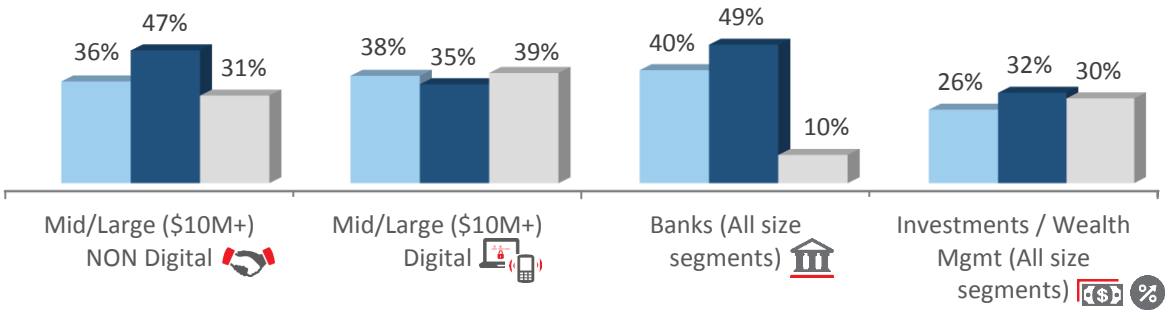
Fraudsters are adept at learning what works and what doesn't. When organizations start to prevent fraud by one means, fraudsters move to other approaches. But where less tracking leads to less prevention, then fraudsters will continue with current entry points.

A majority of financial services firms are not tracking prevented and successful fraud by both transaction type and channel, which leaves the door open to fraudsters. Mid/large digital firms are most at-risk.

% Financial Services Tracking Prevented and Successful Fraud Transactions by Type



% Financial Services Tracking Prevented and Successful Fraud Transactions by Channel



LexisNexis® RISK SOLUTIONS

Q26a: Does your company track prevented vs. successful transactions by type or channel?

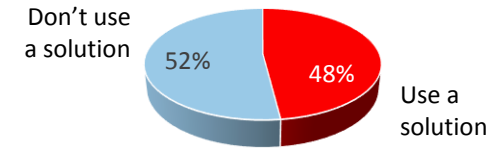
Significantly different from other segments within category at the 95% Confidence Interval

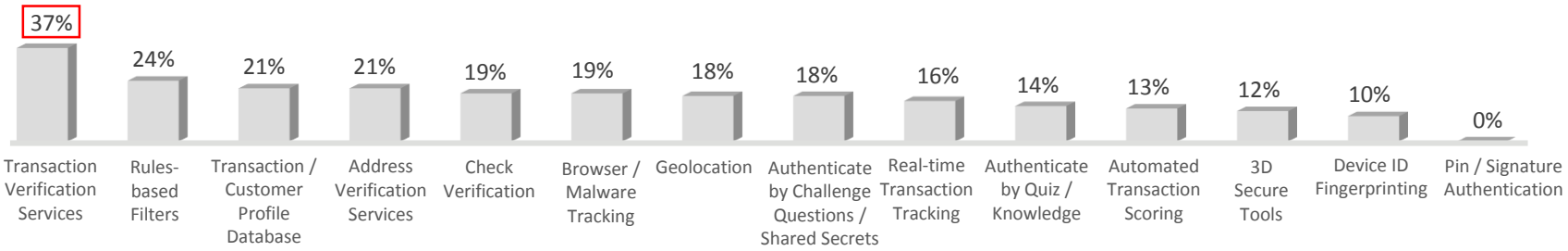
Solutions Use: Non-Digital Overall (all sizes)

Not Digital Fraud Mitigation Solutions Use

97% Large ($50M+) non-digital use a solution

Incidence of Solution Use (at least 1)



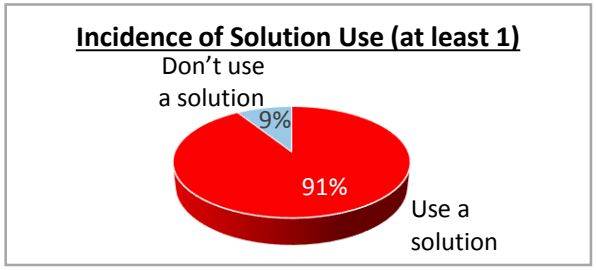


LexisNexis® RISK SOLUTIONS

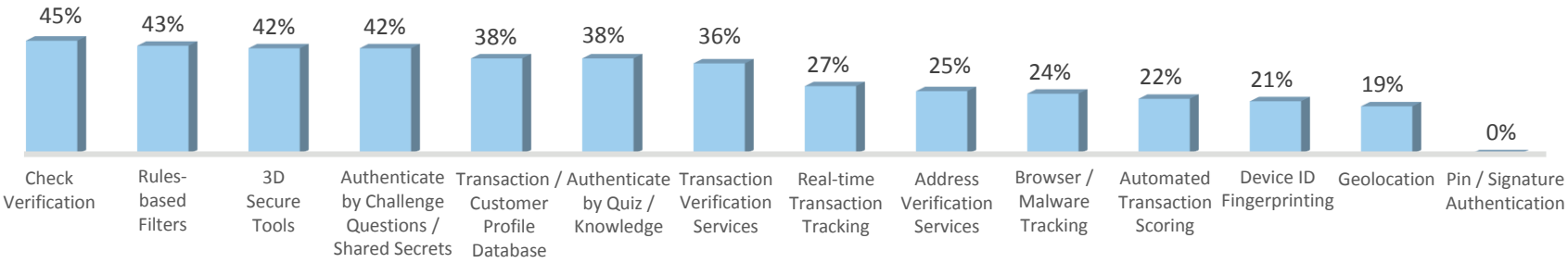
Q27: Which of the following best describes your awareness and use of the fraud solutions listed?

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

Solutions Use: Digital Overall (all sizes)



Digital Fraud Mitigation Solutions Use



LexisNexis® RISK SOLUTIONS

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