



# LexisNexis® Risk Solutions 2019 True Cost of Fraud™ Study

Financial Services  
and Lending Edition



2019

TRUE COST OF FRAUD™  
FINANCIAL SERVICES  
AND LENDING EDITION



Overview



Key Findings



Attacks & Costs



Trends



Challenges



Impacts



Tracking &  
Solution Usage



Strategic Approaches



Recommendations

# Contents

**1** Overview

**3** Key Findings

**4** Key Finding #1 – Attacks & Costs

**11** Key Finding #2 – Trends

**27** Key Finding #3 – Challenges

**37** Key Finding #4 – Impacts

**48** Key Finding #5 – Tracking & Solution Usage

**57** Key Finding #6 – Strategic Approaches

**60** Recommendations





# The LexisNexis® Risk Solutions True Cost of Fraud™ Study helps companies grow their business safely by navigating the growing risk of fraud.

## The research provides a snapshot of:



Current fraud trends in the U.S. financial services and lending market



Key pain points related to adding new payment mechanisms, transacting though online and mobile channels, and expanding internationally

Legend:

- Significantly or directionally different from other segments within category
- ↑<sub>D</sub> Directionally different than 2018 within Segment
- ↑ Significantly different than 2018 within Segment



## Fraud Definitions

- 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
- Fraudulent applications (e.g., purposely providing incorrect information about oneself, such as income, employment, etc.)
- Account takeover by unauthorized persons
- Use of accounts for money laundering

## 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



2019



TRUE COST OF FRAUD™  
FINANCIAL SERVICES  
AND LENDING EDITION

Overview

Key Findings

Attacks & Costs

Trends

Challenges












Impacts

Tracking &  
Solution Usage

Strategic Approaches

Recommendations

# The study included a comprehensive survey of 205 risk and fraud executives in **financial services** and **lending** companies in the U.S.

Financial Services Companies Include:					
# of Survey Completions <b>102</b>	 <ul style="list-style-type: none"><li>• Retail/Commercial Banks</li><li>• Credit Unions</li></ul>	 <ul style="list-style-type: none"><li>• Investments</li><li>• Trusts</li><li>• Wealth Management</li></ul>			
Lending Institutions Include:					
# of Survey Completions <b>103</b>	 Auto Lenders	 Finance Companies	 Mortgage Companies	 Non-Bank Credit Card Issuer	 Non-Bank Personal Loan Issuer
Segments					
Segment definitions:	 <b>Small</b> Earns less than \$10 million in annual revenues	 <b>Mid/Large</b> Earns \$10 million+ in annual revenues	 <b>Non-Digital</b> Less than 50% of transactions through the online and/or mobile channels	 <b>Digital</b> 50% or more of transactions through the online and/or mobile channels	
# of Survey Completions	<b>69</b>	<b>139</b>	<b>117</b>	<b>88</b>	

Research was conducted in from mid June to early August 2019.



Overview



Key Findings



Attacks & Costs



Trends



Challenges



Impacts



Tracking &  
Solution Usage



Strategic Approaches



Recommendations

# Key Findings

- 1 Attacks & Costs:** Fraud has grown significantly during the past year for U.S. financial services and lending firms.
- 2 Trends:** A number of trends are increasing fraud risk for financial services and lending institutions. This is being driven in part by a stronger focus on optimizing the customer experience.
- 3 Challenges:** These trends are increasing the challenges with identity verification and customer friction.
- 4 Impacts:** All of this is increasing fraud volume and costs for digital financial services and lending firms that conduct mobile and/or international transactions.
- 5 Tracking & Solution Usage:** Financial services and lending firms most at-risk for attack may not be optimizing solutions and approaches to fight newer and more complex types of fraud.
- 6 Strategic Approaches:** Study findings show that those financial services and lending firms which use a layered solution approach involving identity authentication and transaction verification, including digital identity / behavior biometric tools, experience a lower cost of fraud.





## Key Finding #1: Attacks & Costs



1

Fraud has grown significantly during the past year for U.S. financial services and lending firms.

- Fraudsters are targeting a broader set of financial services and lending firms.
- Fraud attempts have spiked year-over-year across all financial services and lending segments, and are particularly high for larger banks and credit lenders.
- This has resulted in a sharp rise in the cost of fraud across these firms.

**Survey Questions:**  
**Q22:** In a typical month, approximately how many fraudulent transactions are prevented by your company?  
**Q24:** In a typical month, approximately how many fraudulent transactions are successfully completed at your company?

# Fraud attempts have increased significantly among financial services firms during the past year, with more than twice the number of attempts and an 85% increase in fraud success rates.

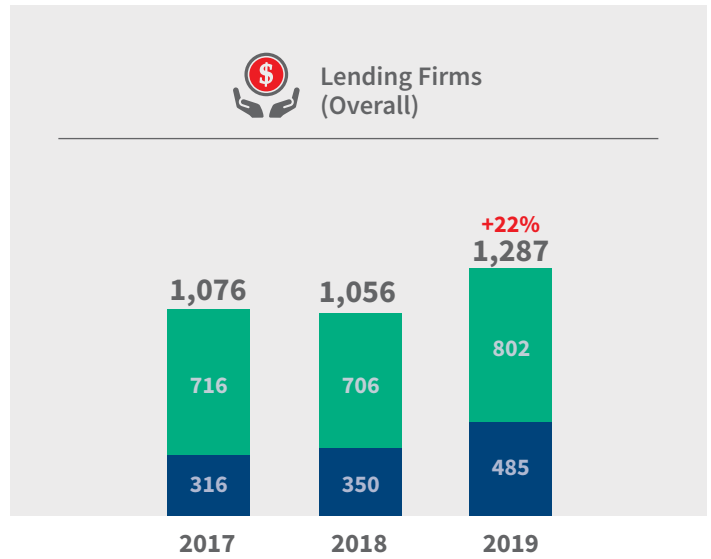
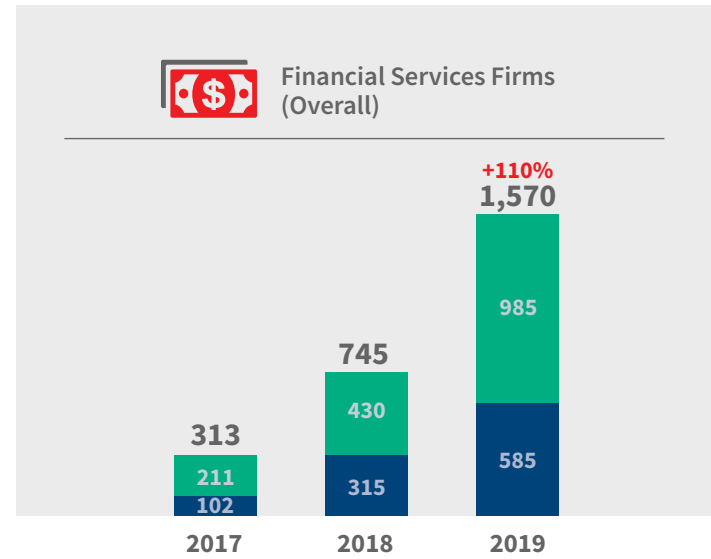
Whereas lending firms have traditionally been exposed to significantly more average monthly fraud attempts, the volume for financial services firms has slightly surpassed the average volume as of 2019, including for those attempts which have succeeded.

However, as shown later, mortgage lending fraud is also on the rise and gets hidden when viewing lending data at an overall level.



## Average # of Total Fraud Attempts Per Month

■ Average Number of Fraudulent Attempts PREVENTED per Month
 ■ Average Number of Fraudulent Attempts That SUCCEEDED per Month



**Survey Questions:**  
Q22: In a typical month, approximately how many fraudulent transactions are prevented by your company?  
Q24: In a typical month, approximately how many fraudulent transactions are successfully completed at your company?

# This sharp rise in financial services fraud attempts is found across segments, though particularly larger banks.

Mid/Large banks have the highest average monthly fraud attempts, which has been a long-standing trend. That said, this gap has widened compared to other firms, with successful fraud attempts for these banks rising 2.35 times on average over 2018. This places them on par with the level of successful fraud attacks experienced by investment / wealth

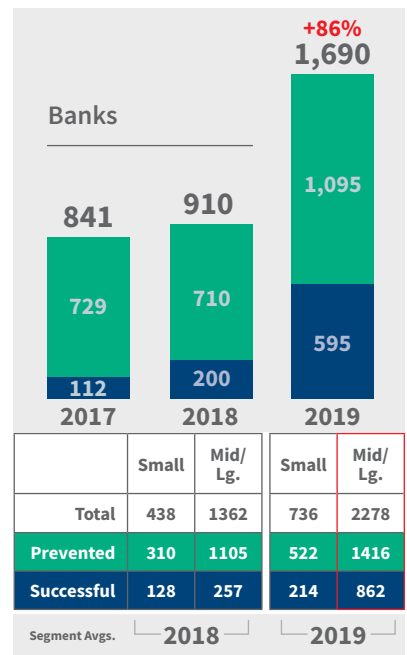
management firms, though significantly higher in terms of overall attacks. Smaller financial services firms have experienced a dramatic increase as well, which shows that fraudsters are targeting a broader range of firms than in the past.



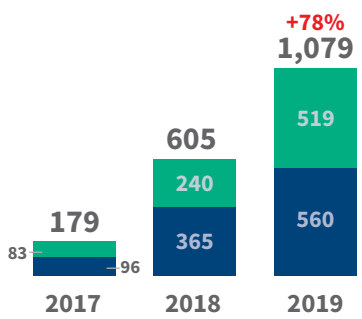
## Average # of Total Fraud Attempts Per Month: Financial Services Firms

Average Number of Fraudulent Attempts PREVENTED per Month

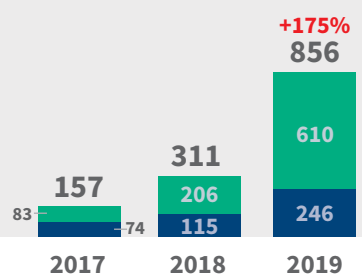
Average Number of Fraudulent Attempts That SUCCEEDED per Month



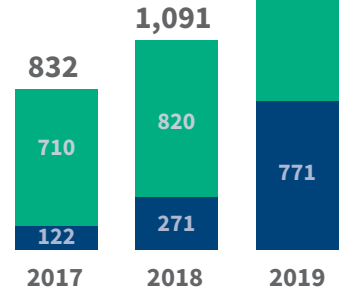
### Investment/ Wealth Management Firms



### Small Financial Services Firms (Overall) (<\$10M Revenues)



### Mid/Large Financial Services Firms (Overall) (\$10M+ Revenues)



# Successful fraud attempts have also risen sharply for mortgage lending firms and remain high for credit lenders.

Mid/Large lending firms continue to experience a higher number of average monthly fraud attempts compared to smaller organizations, though the volume among small mortgage firms has risen significantly. *Directionally*, this has occurred most among smaller mortgage lenders.

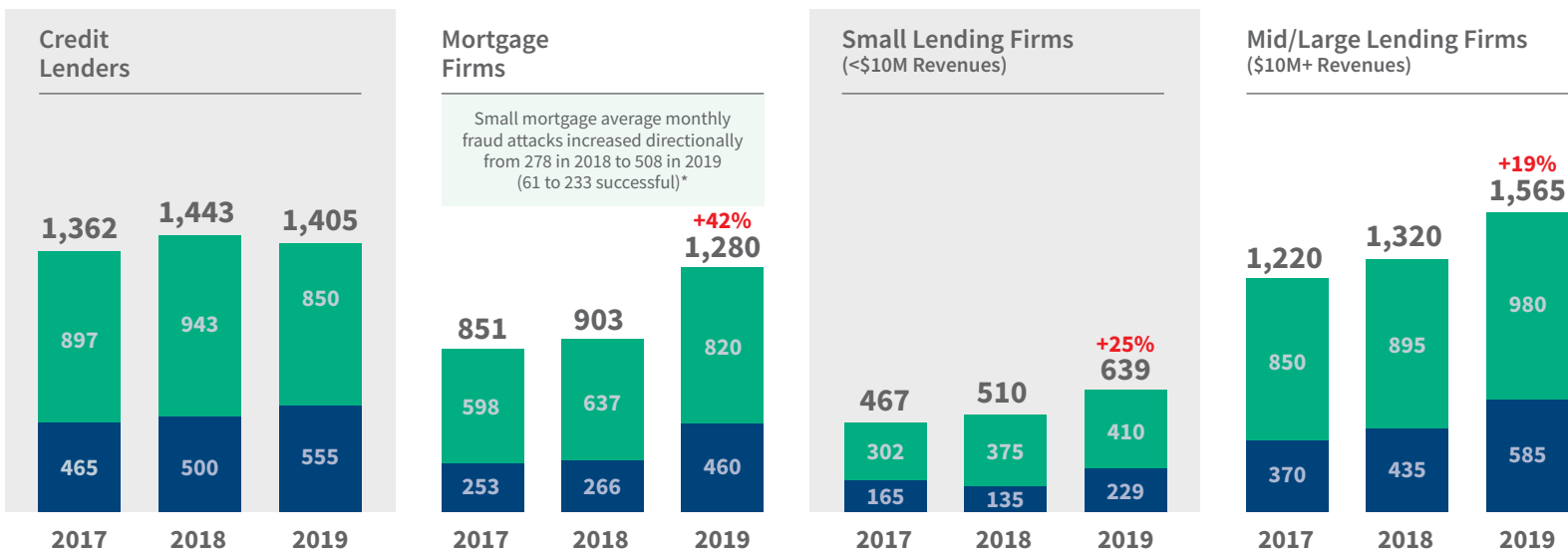
As shown later, smaller mortgage firms indicate a significantly higher distribution of fraud losses due to identity fraud than any other financial services or lending firm segment, with a majority of this is related to account takeover. Further, significantly more smaller mortgage firms have incorporated the mobile transactions into their business model since last year, which contributes to higher fraud risk.



## Average # of Total Fraud Attempts Per Month: Lending Firms

■ Average Number of Fraudulent Attempts PREVENTED per Month

■ Average Number of Fraudulent Attempts That SUCCEEDED per Month



Small mortgage average monthly fraud attacks increased directionally from 278 in 2018 to 508 in 2019 (61 to 233 successful)\*

**Survey Questions:**  
Q22: In a typical month, approximately how many fraudulent transactions are prevented by your company?  
Q24: In a typical month, approximately how many fraudulent transactions are successfully completed at your company?

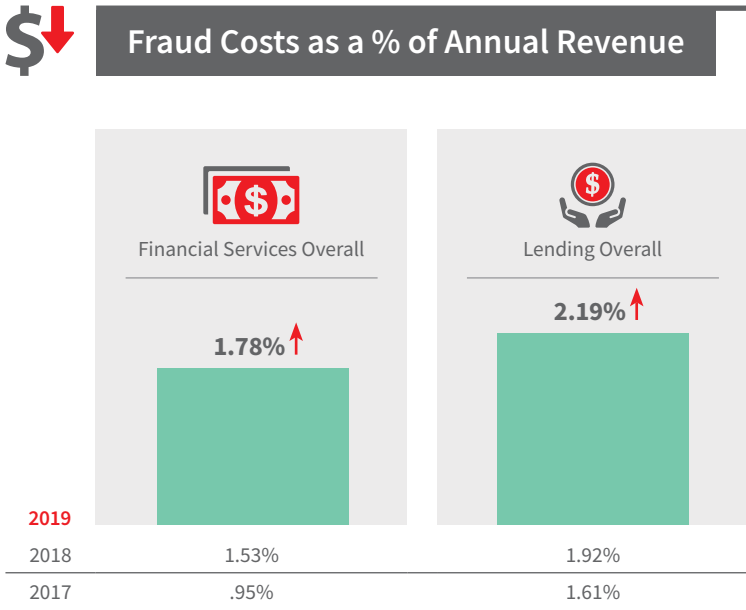
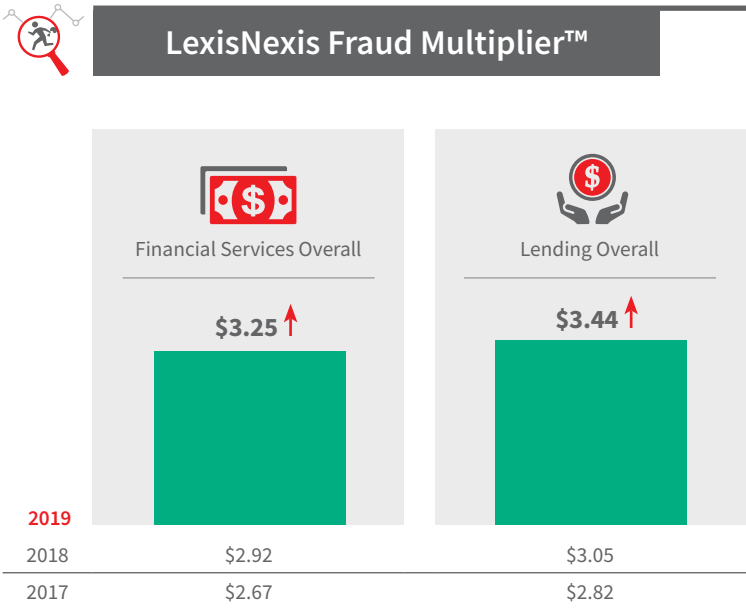
**Survey Questions:**  
**Q16:** In thinking about the total fraud losses suffered by your company, please indicate the distribution of various fraud costs over the past 12 months.  
**Q10:** What is the approximate value of your company's total fraud losses over the past 12 months, as a % of total revenues?

# Relatedly, the cost of fraud has increased across financial services and lending firms by up to nearly 13% over 2018.

For every \$1 of fraud, it costs financial services firms \$3.25 compared to \$2.92 last year (an 11.3% increase); for lenders, this is even higher at \$3.44 compared to \$3.05 in 2018 (a 12.8% increase). Since 2017, the cost of fraud has risen approximately 21%. While fraud is not the same as financial crime / money laundering, this steep increase mirrors that for the latter during the same time period.<sup>1</sup>

Such fraud costs involve losses related to the transaction face value for which firms are held liable, plus fees/interest incurred during applications/underwriting/processing stages, fines/legal fees, labor/investigation and external recovery expenses.

Together, this represents an increase in the percentage that hits bottom line revenues.



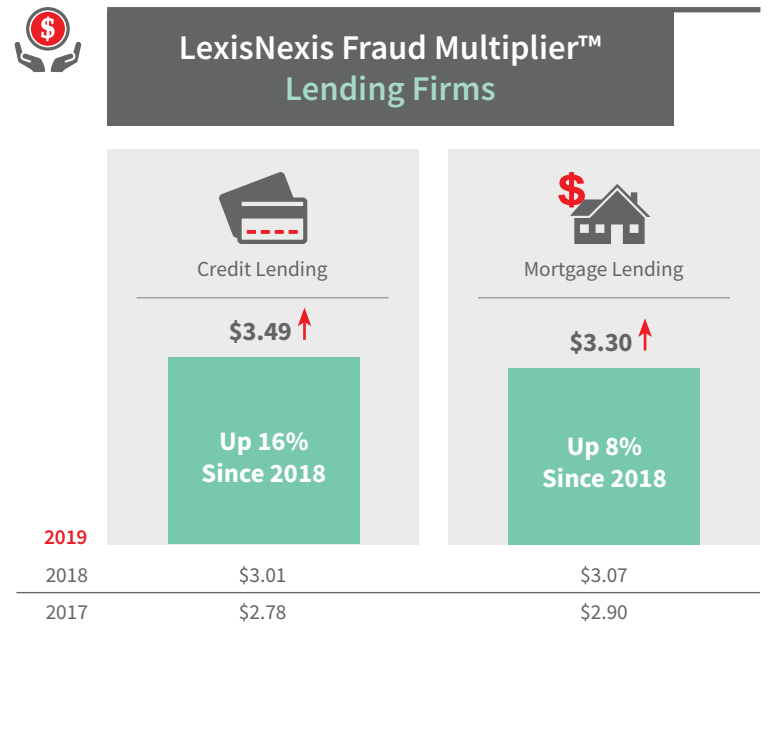
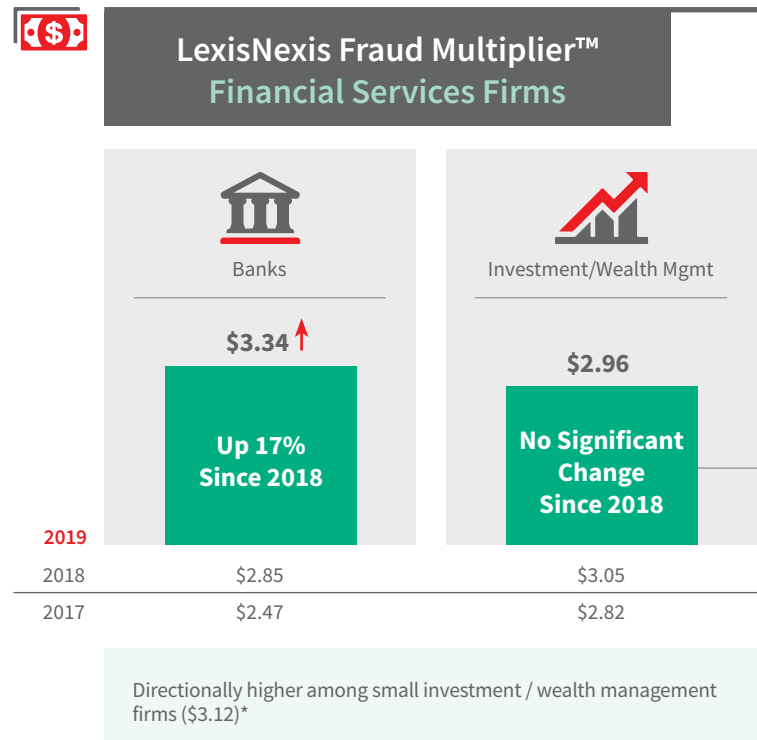
<sup>1</sup> LexisNexis® Risk Solutions 2019 True Cost of Compliance, U.S. & Canada Edition

**Survey Question:**  
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.

## Credit lending firms continue to have a higher cost of fraud; these firms plus banks have seen a double-digit jump since last year.

While the cost of fraud has not changed significantly for investment/wealth management firms, a number of those which are larger digital organizations have made investments in risk mitigation solutions designed to address the above types of risks.

Smaller firms which have not done so report a *directionally* higher cost of fraud than shown below.

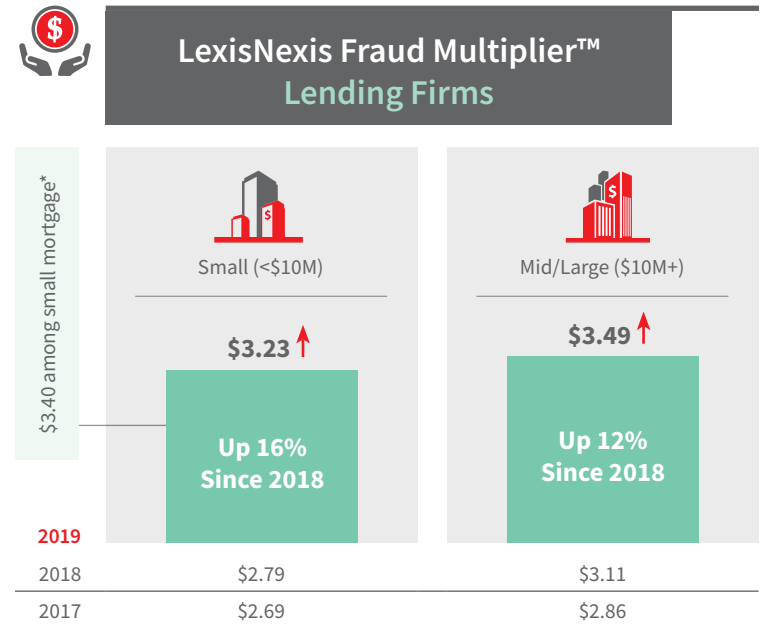
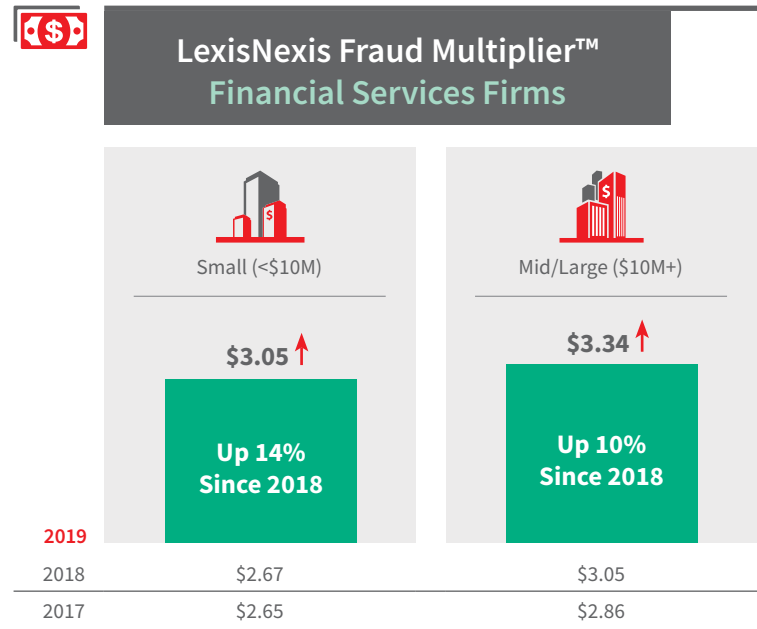


**Survey Question:**  
Q16: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various fraud costs over the past 12 months.

# The cost of fraud has risen across organization size and continues to be higher among mid/large firms. However, smaller institutions have experienced the sharpest rise over 2018.

Small mortgage firms have a *directionally* higher cost of fraud than other small-sized financial services and lending firms. But with sizeable cost increases across smaller organizations, findings show that more of them are recognizing the need to allow mobile channel transactions; among those doing so, more of these firms are defined as digital (50% or more revenues generated from online or mobile channels).

As shown later, fewer small financial services and lending firms are using solutions designed to mitigate fraud risks that are unique to the mobile / digital environment.



\* CAUTION – low number of respondents; directional only

# Key Finding #2: Trends

- Overview
- Key Findings
  - #1 Attacks & Costs
  - #2 Trends
  - #3 Challenges
  - #4 Impacts
  - #5 Tracking & Solution Usage
  - #6 Strategic Approaches
- Recommendations



**2** A number of trends are increasing fraud risk for financial services and lending institutions. This is being driven in part by a stronger focus on optimizing the customer experience.

- Mobile channel and mobile app use is expanding.
- International transactions remain sizeable among some segments and are increasing in number among others.
- More botnet activity is occurring.
- Synthetic identities continue to be prevalent.
- Digital financial services and lending firms are often leading the way with the above.

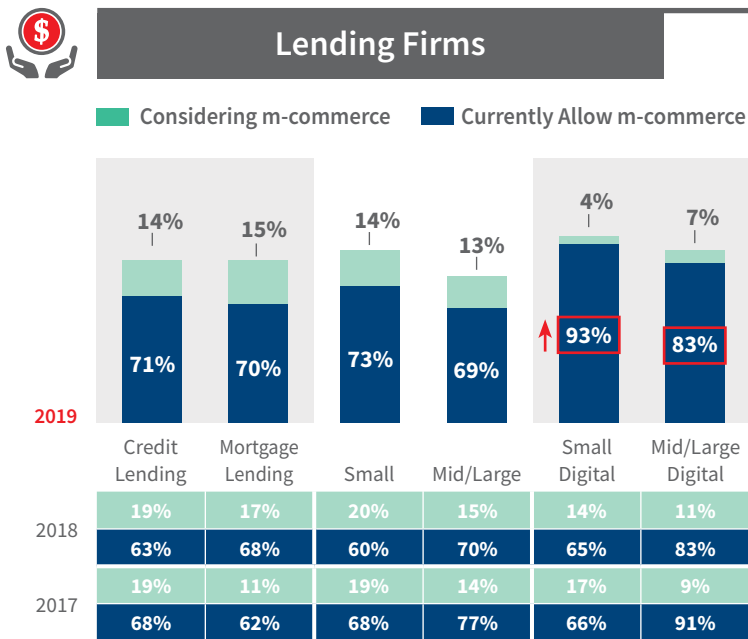
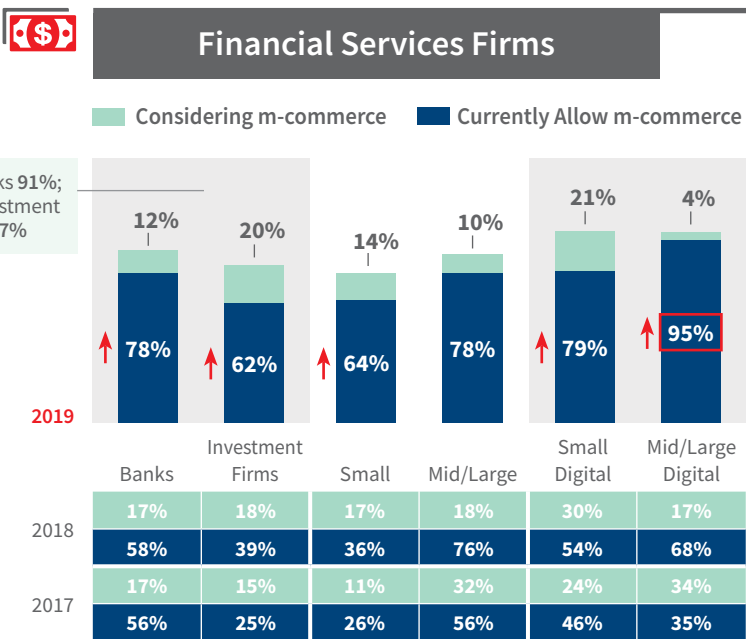
**Survey Questions:**  
**Q4:** Please indicate the percentage of transactions completed (over the past 12 months) for each of the following payment channels currently accepted by your company.  
**Q6:** Is your company considering accepting payments by mobile device over the next 12 months?

# Trend #1: More Mobile – There has been a significant increase in use of the mobile channel over 2018, with a sizeable majority now offering this option.

Growth came from small financial services firms and digital financial services and lending firms.

Looking at the percent of segments from 2018 that said they expected to adopt the mobile channel within the next 1-2 years (light blue row), those projections exceeded expectations for most. That

was not the case from 2017, where 2018 mobile channel growth was more limited. This suggests that firms have recognized the need to incorporate m-commerce into their business models and that, for many, this has taken time to implement operationally; it is also likely that there has been hesitation given risks associated with mobile channel transactions.



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

# Optimizing the customer experience has become even more important for financial services firms, with faster and lower friction transactions increasing as mobile channel drivers.

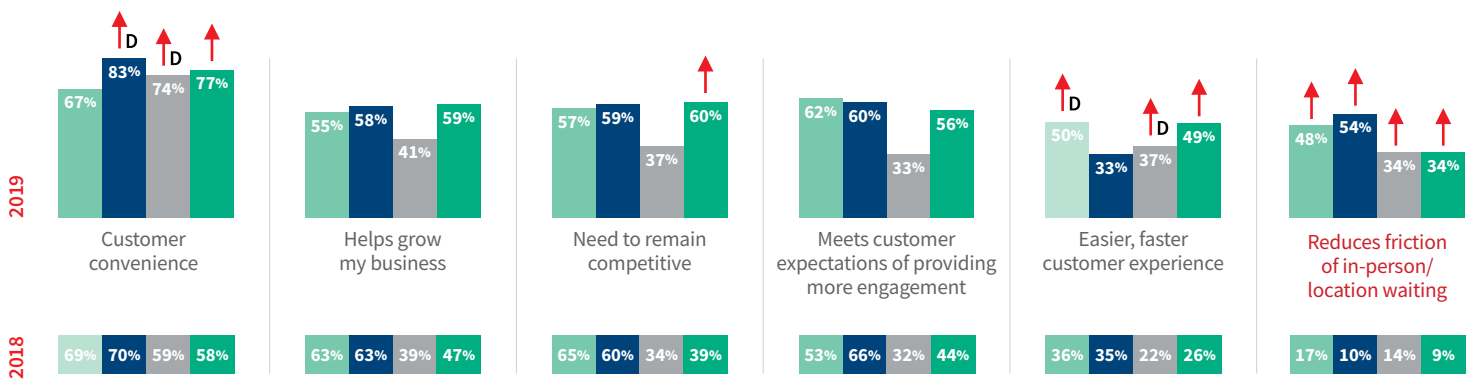
Reducing customer friction through an easier / faster experience has increased to be on par with growing the business and remaining competitive. Digital financial services firms in particular have come to place more emphasis on this as a means of remaining competitive; this suggests that firms which do not reduce customer friction will be at a competitive disadvantage.

Given that investment / wealth management firms have a different value proposition (to grow assets), mobile channel adoption tends to be less about competitiveness / business growth or even customer expectations; instead, it appears that this is offered as a convenience to the degree that customers prefer it as an option.



## Mobile Channel Drivers: Financial Services Firms

Small Banks    Mid/Large Banks    Investment Firms    Digital Financial Services Firms



**Survey Question:**  
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.

## However, there continues to be a perception among financial services firms that the mobile channel adds significant fraud risk and is becoming more difficult to manage bots and customer friction.

Therefore, they continue to understand the trade-off between needing to allow mobile transactions while also paying attention to the heightened fraud risks.

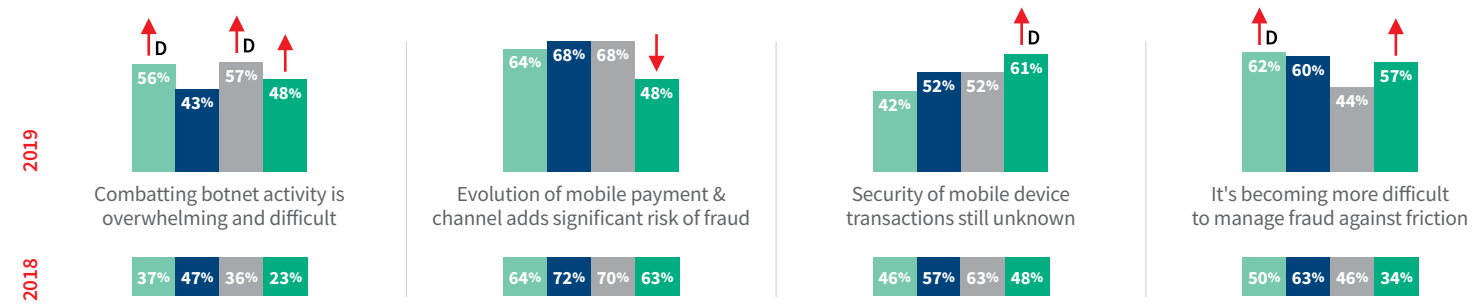
As more smaller banks and digital financial services firms have adopted the mobile channel, the sense of feeling overwhelmed by botnet activity and managing customer friction against fraud detection has increased.

There are mixed perceptions about mobile channel security among digital financial services firms. While fewer indicate that the evolution of mobile payments adds significant risk of fraud compared to previous waves, more of them are likely to still question the security of mobile device transactions.



### Mobile Channel Perceptions: Financial Services Firms (% 4 and 5 on 5 point scale)

Small Banks    Mid/Large Banks    Investment Firms    Digital Financial Services Firms



- Overview
- Key Findings
- #1 Attacks & Costs
- #2 Trends
- #3 Challenges
- #4 Impacts
- #5 Tracking & Solution Usage
- #6 Strategic Approaches
- Recommendations

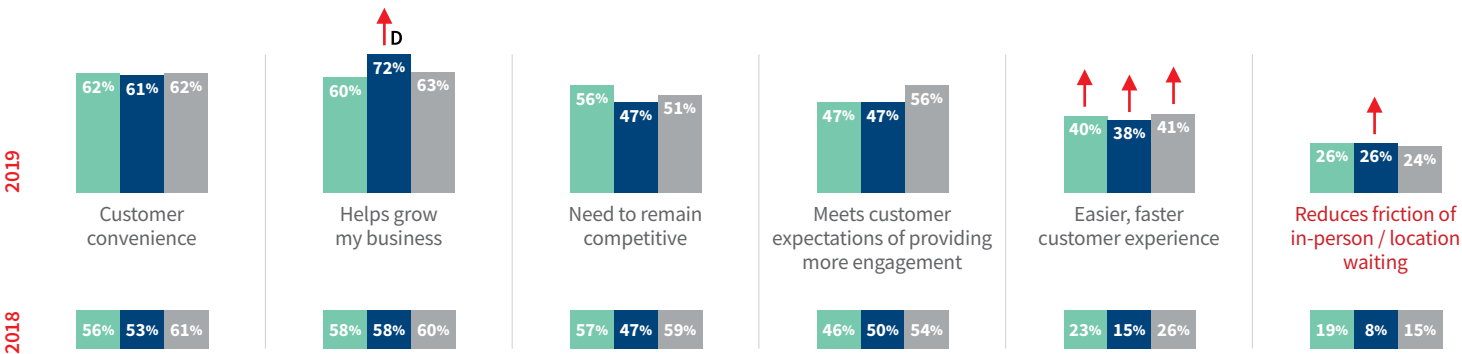
# The customer experience and business growth also continue to drive mobile channel adoption among lenders.

Providing an easier / faster customer experience has increased in importance as a key driver among just under half of lenders. Interestingly, reducing customer friction remains less of a driver while it has gained importance among financial services firms.



## Mobile Channel Drivers: Lending Firms

Credit Lending Firms Mortgage Lending Firms Digital Lending Firms



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

# Mobile channel perceptions among lenders haven't changed much during the past year, with a significant majority believing that these transactions add risk for fraud.

While fewer digital lending firms indicate that this year, a majority still do.

The biggest change has come from mortgage lending firms, with significantly fewer being concerned about security of mobile devices. That could become a false hope, since mobile apps are a prime target for fraudsters.



## Mobile Channel Perceptions: Lending Firms (% 4 and 5 on 5 point scale)

Credit Lending Firms

Mortgage Lending Firms

Digital Lending Firms

2019

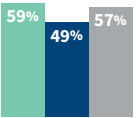
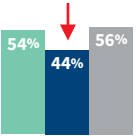
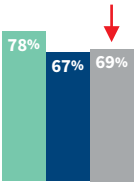
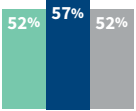
2018

Combating botnet activity is overwhelming and difficult

Evolution of mobile payment & channel adds significant risk of fraud

Security of mobile device transactions still unknown

It's becoming more difficult to manage fraud against friction



**Survey Question:**  
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.

**Survey Question:**  
Q4: what is the distribution of transactions through each of the mobile channels your company uses/accepts?

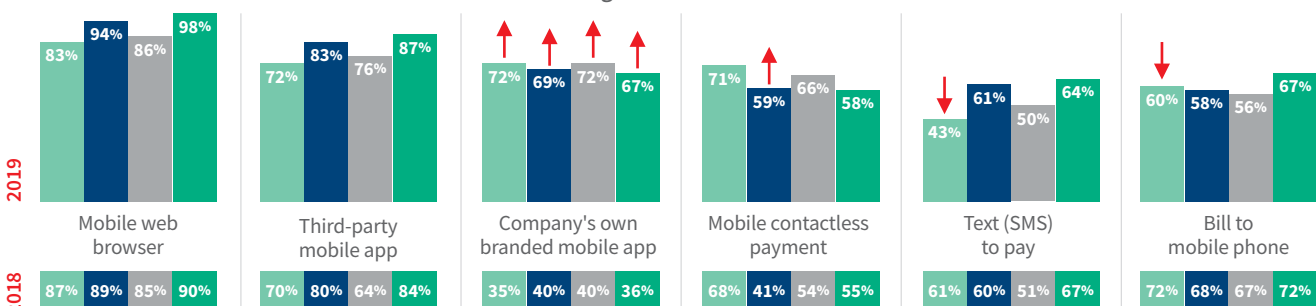
# Significantly more financial services have implemented use of their own company-branded mobile app.

With a similar number using mobile web browsers, third-party and company-branded mobile apps, along with a majority offering mobile contactless payment, this shows that financial services firms continue to expand options to meet consumer mobile banking preferences. This speaks to the change in consumer demand and behavior, including

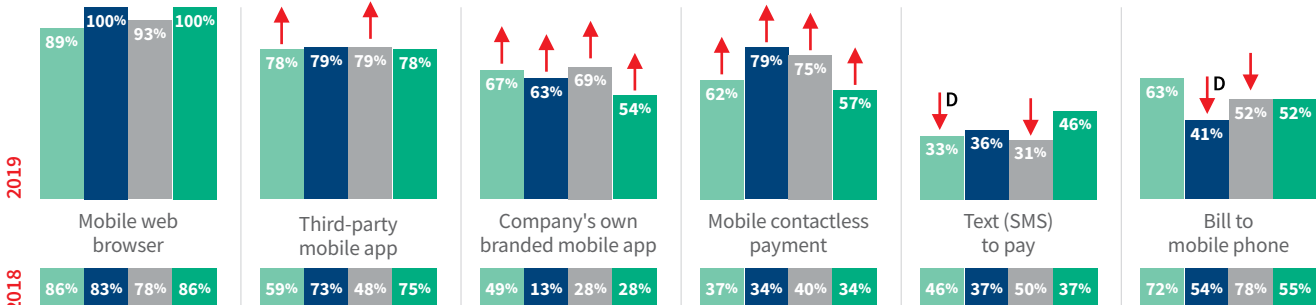
card-less ATM transactions or where consumers add their banking credit card to their mobile device to make purchases directly through this method. That said, some firms have dropped Text-to-Pay and Bill-to-Mobile-Phone as options, presumably based on concerns about risk.



% Mobile Channels are USED BY  
**Mid/Large Financial Services  
Firms Allowing M-commerce**  
(\$10M+ Revenues)



% Mobile Channels are USED BY  
**Small Financial Services  
Firms Allowing M-commerce\*\***  
(<\$10M Revenues)



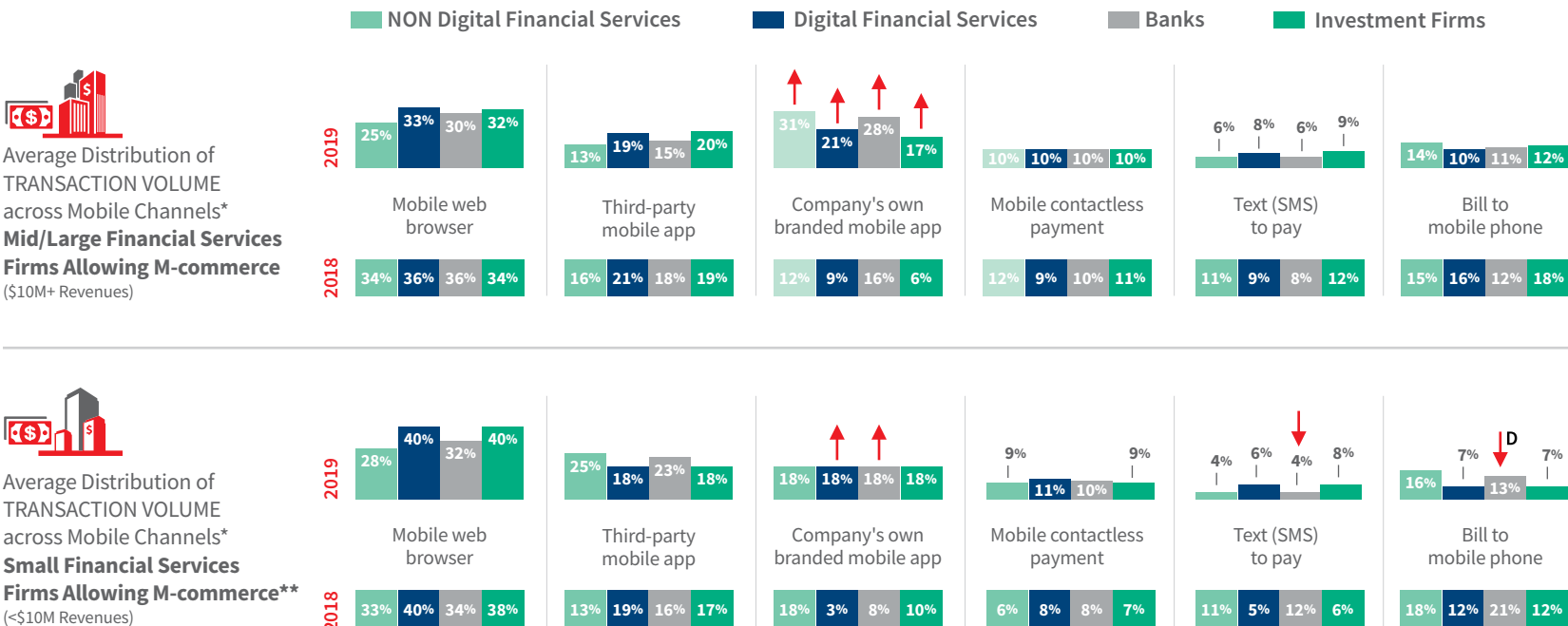
\*\* CAUTION: Low base sizes for 2018; Incidence of m-commerce among small financial services low in 2018

**Survey Question:**  
**Q4:** what is the distribution of transactions  
through each of the mobile channels your  
company uses/accepts?

# The change in consumer demand is seen most with a significant increase in the average percent of mobile apps transactions.

This average represents a sizeable portion for both small and mid/ large firms when combining third-party and branded mobile apps; more financial institutions have offered this option and consumers have accepted the offer.

While a number of financial services firms offer Text-to-Pay and Bill-to-Mobile-Phone options, few consumers tend to use these methods.

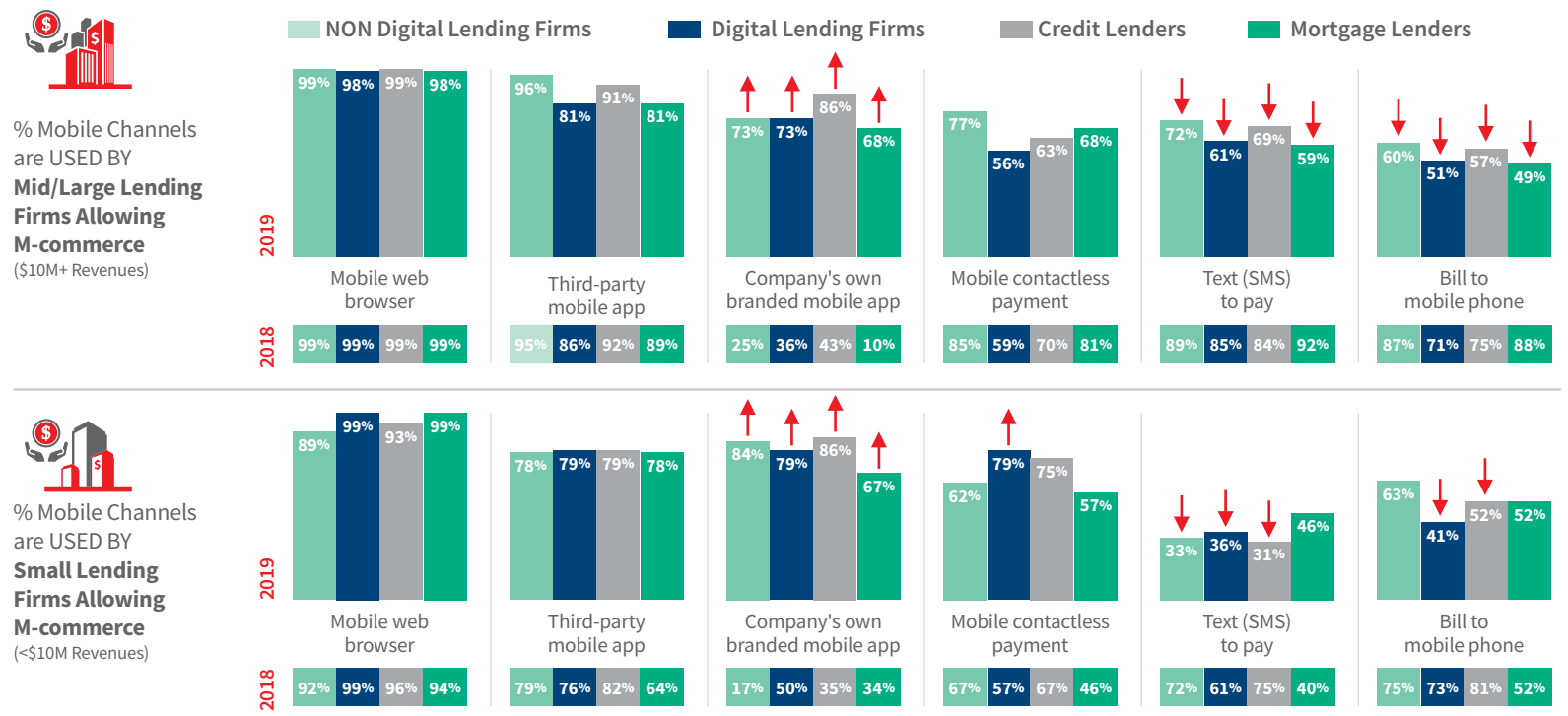


**Survey Question:**  
Q4: what is the distribution of transactions through each of the mobile channels your company uses/accepts?

## There are also significantly more lending firms that have implemented use of their own company-branded mobile app.

But while a majority of mid/large firms continue to offer Text-to-Pay and Bill-to-Mobile-Phone, there are some who have dropped these; this coincides with a significant number of smaller lenders which have

stopped offering these methods. This could be related to perceived risk, but also to more limited consumer use as shown on the next slide.

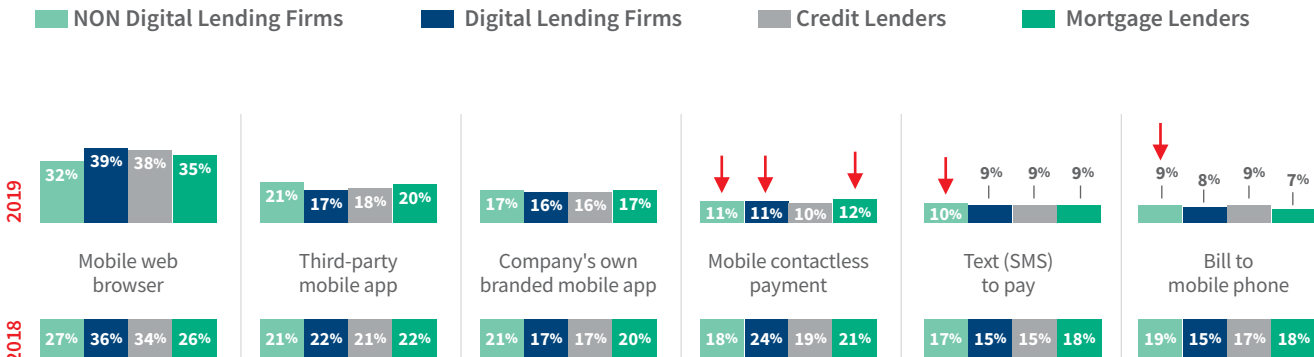


# Mobile web browsers continue to be used by consumers more than other channels for lending, even though more firms have begun offering the use of mobile apps.

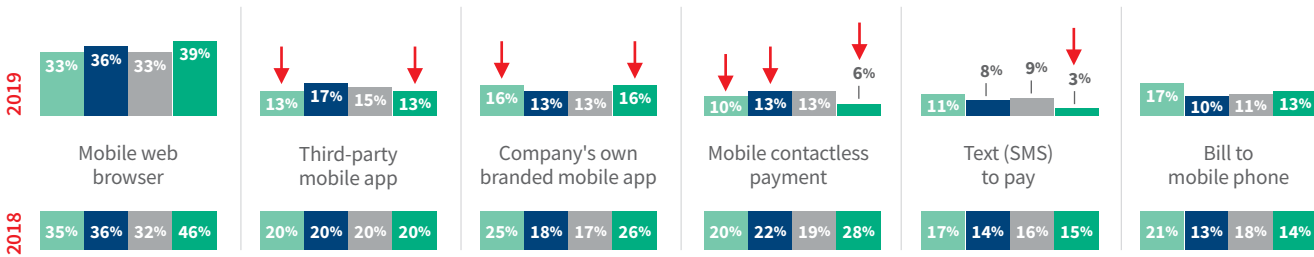
Even fewer transactions are reported through mobile contactless than in 2018, with a directional decline in the volume going through Text-to-Pay and Bill-to-Mobile-Phone.



Average Distribution of TRANSACTION VOLUME across Mobile Channels\*  
**Mid/Large Lending Firms Allowing M-commerce**  
(\$10M+ Revenues)



Average Distribution of TRANSACTION VOLUME across Mobile Channels\*  
**Small Lending Firms Allowing M-commerce**  
(<\$10M Revenues)



**Survey Question:**  
Q4: what is the distribution of transactions through each of the mobile channels your company uses/accepts?

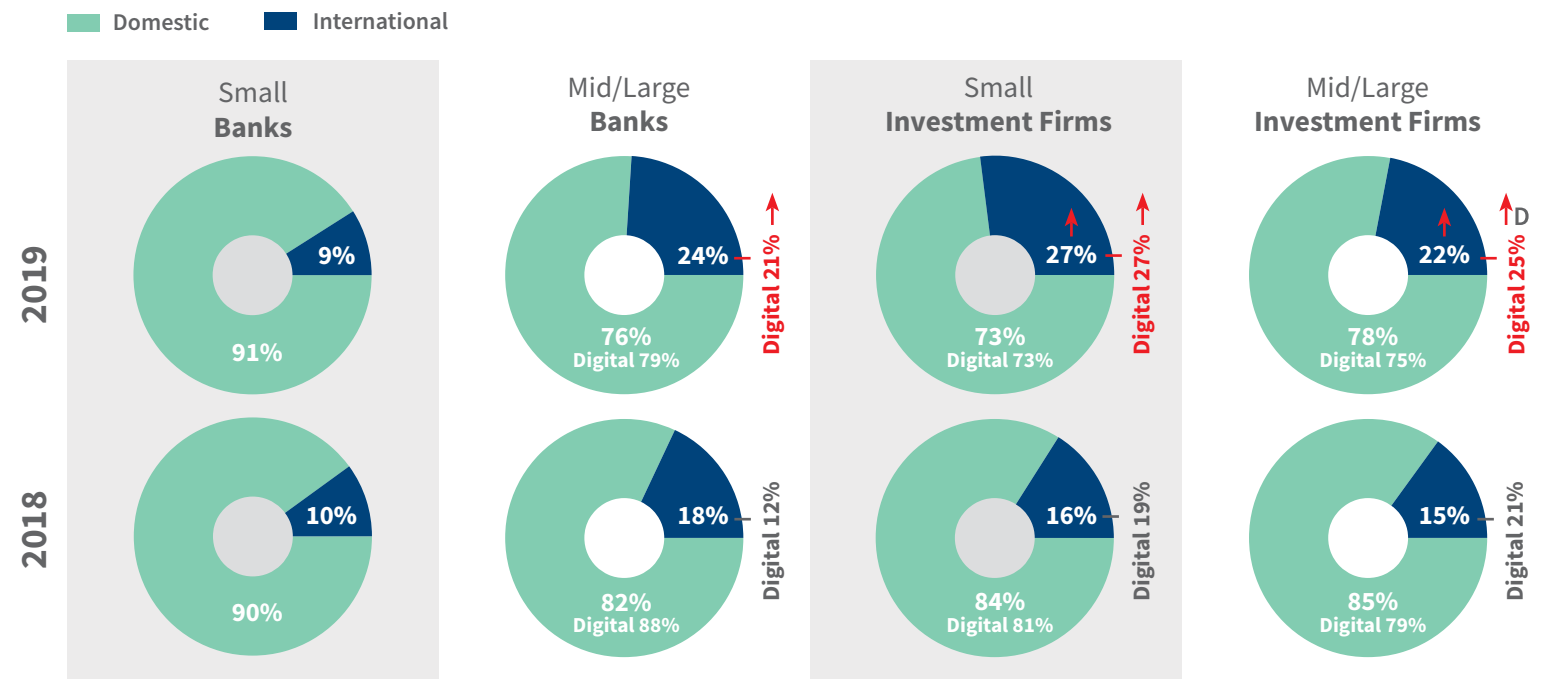
\* % can add to more than 100% since answers based on using a channel, in which case the base size changes per channel

## Trend #2: More Cross-Border Transactions – There has been an increase in the volume of international transactions among mid/large digital banks and small/mid/large digital lenders.

While domestic transactions account for the bulk of annual revenues, the percent attributed to international transactions has increased substantially for larger banking.



### Domestic vs. International Transaction Volumes: Financial Services Firms



**Survey Question:**  
Q9: Please indicate the percent of annual revenue generated through domestic compared to international transactions in the last 12 months.

# Mortgage lenders report a significant drop in foreign transactions, which aligns reports from the National Association of Realtors®.

In a recently published survey by this association, findings show a marked drop in foreign transactions during the past year, which

coincides with a decline in global growth and housing inventory.<sup>2</sup> International transaction volume for credit lenders tends to be less than that reported by most financial services firms.



## Domestic vs. International Transaction Volumes: Lending Firms

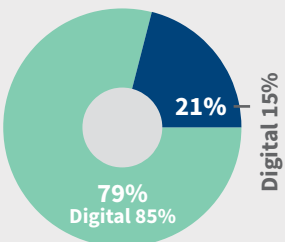
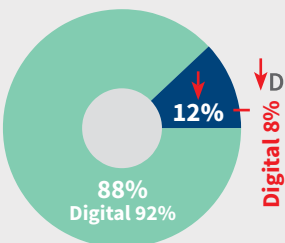
Domestic

International

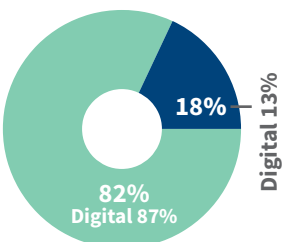
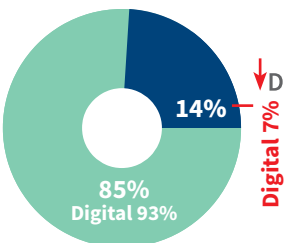
2019

2018

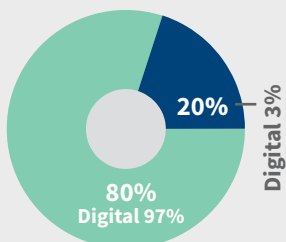
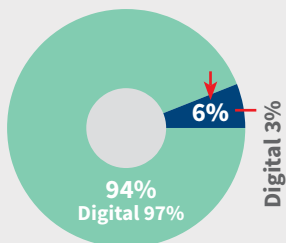
### Small Credit Lenders



### Mid/Large Credit Lenders



### Mortgage Lenders



**Survey Question:**  
Q9: Please indicate the percent of annual revenue generated through domestic compared to international transactions in the last 12 months.

<sup>2</sup> <https://www.nar.realtor/newsroom/realtor-survey-shows-decline-in-foreign-investment-in-u-s-residential-real-estate>

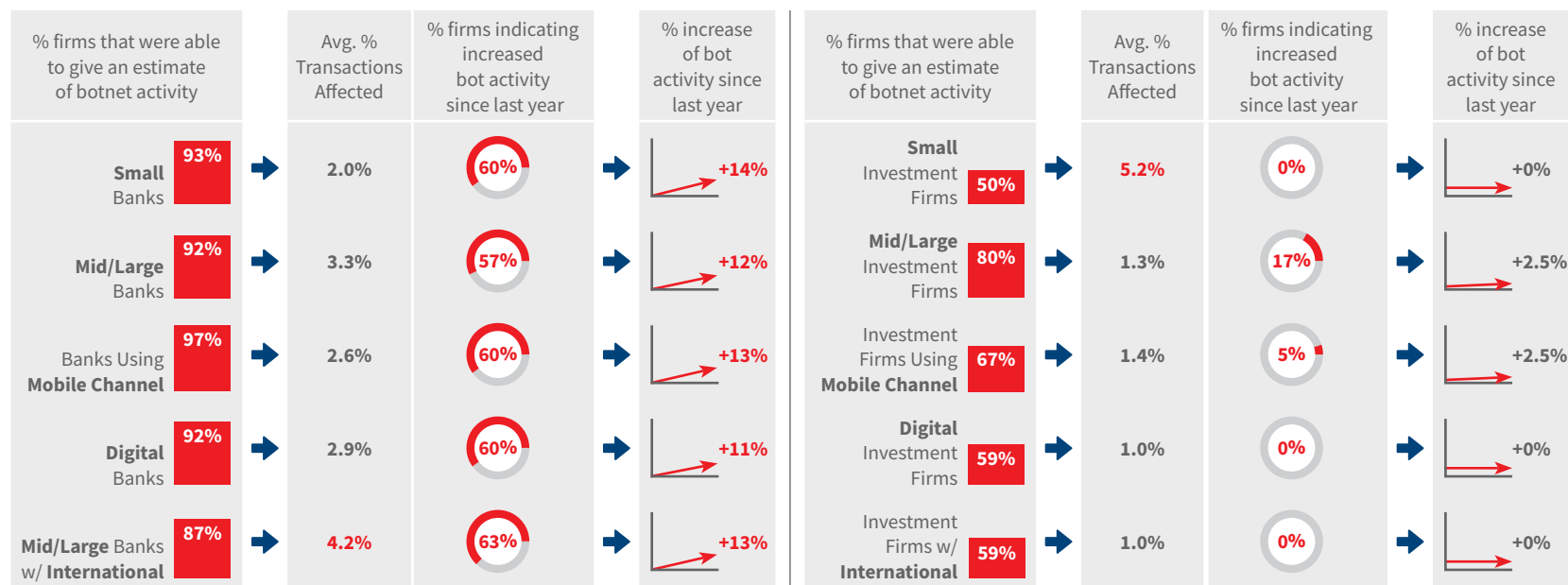
## Trend #3: More Botnets – A majority of banks reported double-digit year-over-year growth in these malicious activities; this involves more transactions, on average, for banks with international business.

Among the few investment firms that could provide an estimate, few mentioned seeing an increase since last year. This seems low, given that botnets target account takeover / new creation which is a sizeable

portion of identity-related fraud among lending firms; as a result, these firms may have more limited tools to detect bots and, therefore, be at higher risk as a result.



### Botnet Activity as % of Transactions Per Month: Financial Services Firms



**Survey Questions:**  
**B1a:** In a typical month, what percent of your transactions are determined to be malicious automated bot attacks?  
**B1b:** How does this compare to the same time last year? Would you say the percent of monthly automated malicious bot attacks has:

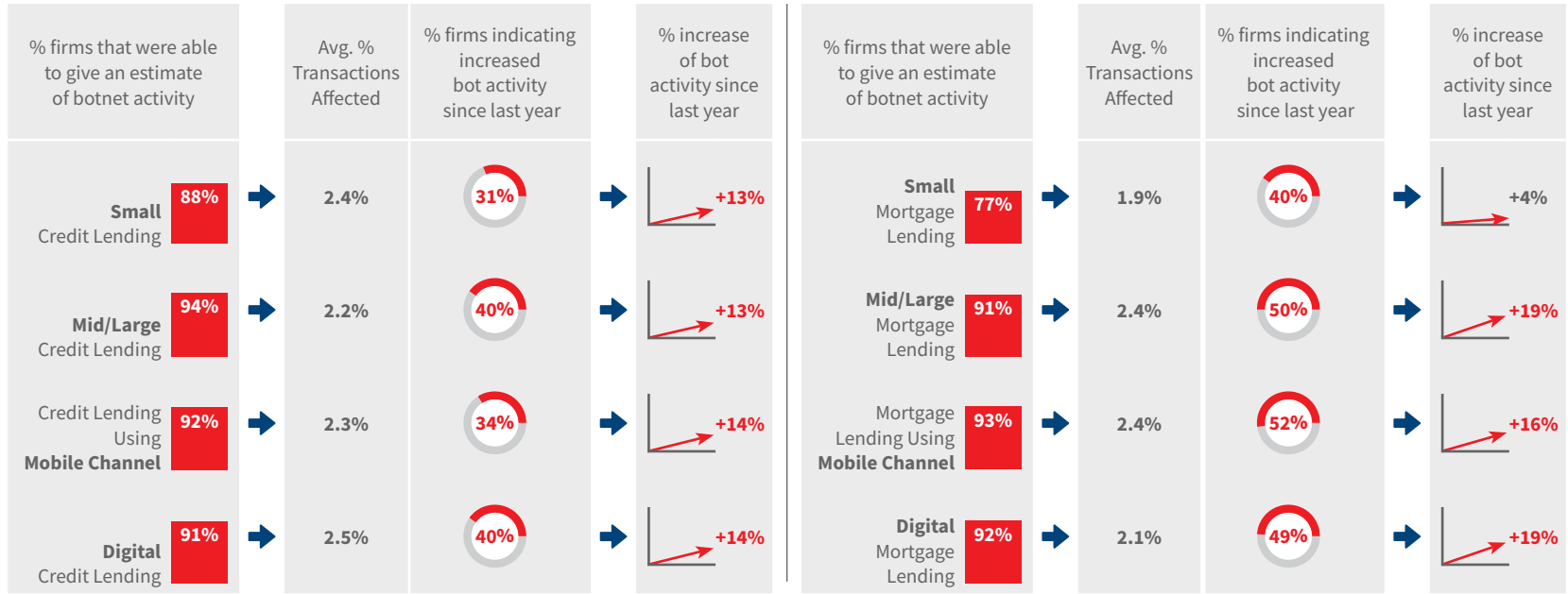
**Survey Questions:**  
**B1a:** In a typical month, what percent of your transactions are determined to be malicious automated bot attacks?  
**B1b:** How does this compare to the same time last year? Would you say the percent of monthly automated malicious bot attacks has:

# Both credit and mortgage lenders indicated awareness of botnet activity, with around half of mortgage lenders reporting significant year-over-year growth in these malicious activities.

Across financial services and lending firms, more banks have indicated an increase in YOY botnet activity than lenders, followed by mortgage lenders.



## Botnet Activity as % of Transactions Per Month: Lending Firms





Overview



Key Findings



Attacks &amp; Costs



Trends



Challenges



Impacts


Tracking &  
Solution Usage


Strategic Approaches



Recommendations

## So, why is mobile, digital and international more risky?



### Mobile

- **Rise of mobile botnet attacks**; malware infects devices without consumer knowledge; steals identity, hacks accounts, makes fraudulent purchases.<sup>3</sup>
- **Consumer risk behaviors**; using open WiFi networks increases risk of smishing (SMS-based phishing) and man-in-the-middle interception of passcodes used for multi-factor authentication<sup>4</sup>; “keep me logged in” habits become an unlocked entry point to accounts.
- **Increasing pool for fraudster opportunity** as more people conduct mobile transactions.



### Cross Border

- **Uncertainties, blind spots and new payment methods**; it becomes difficult to determine transaction origination; lack of verifiable data on consumers in other markets (particularly with GDPR).



### Digital

- **More exposure**; by conducting the majority of business through the anonymous remote online and/or mobile channels, digital financial services and lending firms have more risk exposure by definition; there is the need for more digital identity and behavior data and analysis based to detect unique risks (botnet attacks; account hacking; mobile malware); traditional risk detection solutions that rely on more of the physical identity attributes will not be as effective in this environment – and fraudsters know it.
- **Easy targets**; synthetic identities and stolen data make it difficult to distinguish between malicious attacks and legitimate customers in the anonymous channel.

## Synthetic identities are a serious threat. Their very nature makes it extremely difficult to detect before damage is incurred.



Synthetic identities are comprised of real and/or fake personal information. They are created by using information from either:



**Multiple real persons** into a single fake identity, with a valid shipping address, Social Security Number (SSN), date of birth, name, etc. – none of which matches any one person. This type may be used for shorter-term fraud gains, such as bigger ticket items.



**One real person** by using some of his / her information combined with fake data. In this case, the fraudster is likely to be nurturing this identity, using it to establish a good credit history before ultimately “going bad”.



**No known persons** in which the personally identifiable information doesn’t belong to any consumer. It is entirely fabricated based on a new SSN, using the same range as the Social Security Administration for randomly-issued numbers. This may also be nurtured for longer-term gain and is useful when posing as an underbanked consumer with a less established purchasing footprint (e.g., younger Millennials).

### Risks and Challenges

#### Extremely Hard to Distinguish from Legitimate Customers

Focus on nurturing the identity to mimic a good customer; establishes good credit, pays on-time, etc. before “breaking bad.”

#### Difficult to detect with traditional identity verification / authentication solutions

These are professional fraudsters; they often know the types of information required to gain approval and pass certain checkpoints. Use of real identity data helps them do this.

#### Real customers don’t help; behaviors make it difficult to spot anomalies with current ID solutions.

Consumers access accounts from different locations anywhere and anytime. They might share passwords and use different devices at different times. It is harder to make physical and digital connections that distinguish fraudulent from legitimate patterns.



## Key Finding #3: Challenges



3

These trends are increasing the challenges with identity verification and customer friction.

- The mobile channel and international transactions are recognized as making it more difficult to conduct identity proofing.
- Key identity-related challenges across channels involve determining the source of transaction origination, limited ability to determine geolocation and balancing speed of verification with customer friction.
- The rise of malicious botnets and synthetic identities are contributing to the above.
- There is a need for more third-party, real-time data and transaction tracking tools.

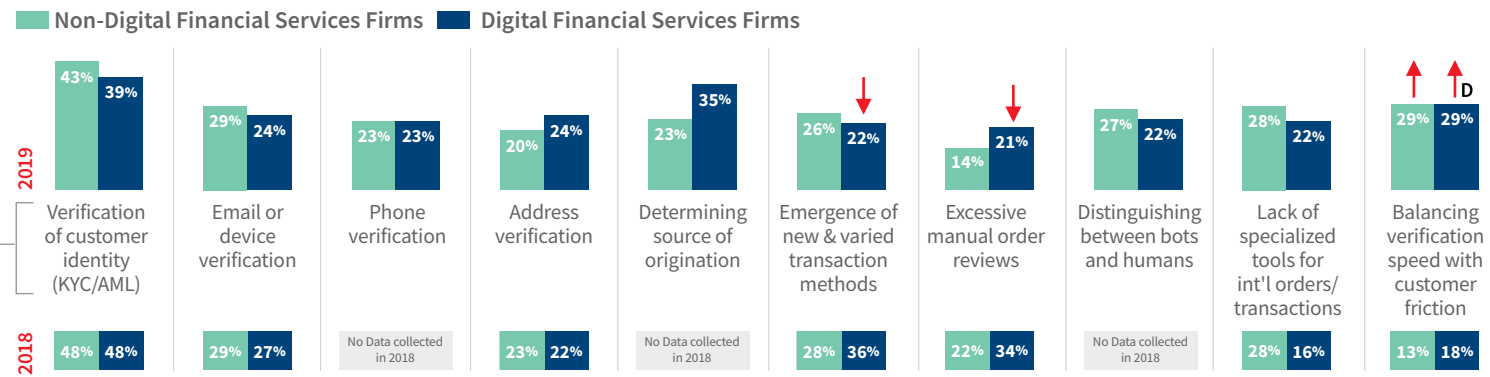
# Not surprisingly, identity verification remains the top challenge when conducting financial transactions online.

Those conducting a majority of business online (digital) are also directionally more likely to mention online challenges with determining the source of a transaction origination; this is an underlying reason for making identity verification challenging (61% of those ranking this as a challenge point to limited ability to identify geolocation). Additional factors contributing to identity verification challenges among digital firms include rise of synthetic identities and botnet attacks.

Balancing speed of verification against speed for minimal customer friction has increased as a challenge for not only digital financial services firms, but also for “bricks and mortar” organizations that allow online transactions. Since they also cite the need for more real-time data and transaction tracking, this suggests that these non-digital firms are relying more on traditional risk detection solutions.



## Top Ranked ONLINE FRAUD Challenges Among Top 3 Ranked: Financial Services Firms



### Top Identity Verification Challenges

**NON-DIGITAL FINANCIAL SERVICES FIRMS**  
Need for real-time third-party data (68%)  
Need for real-time transaction tracking (59%)

**DIGITAL FINANCIAL SERVICES FIRMS**  
Rise of synthetic identities (65%)  
Volume of malicious botnet attacks (50%)  
Limited ability to identify geolocation (40%)

Noted decreases from 2018 for *excessive manual reviews* and *new/ varied transaction methods* do not necessarily indicate that these are less critical issues; since this is a ranking question (top 3), a decrease more often means that other challenges are either rising to the top or that there is a broadening of issues faced by firms such that there is less consensus around any one specific challenge.

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

# Key online challenges vary by firm size and type. Smaller banks directionally struggle most with digital identity verification which leads to increased manual reviews.

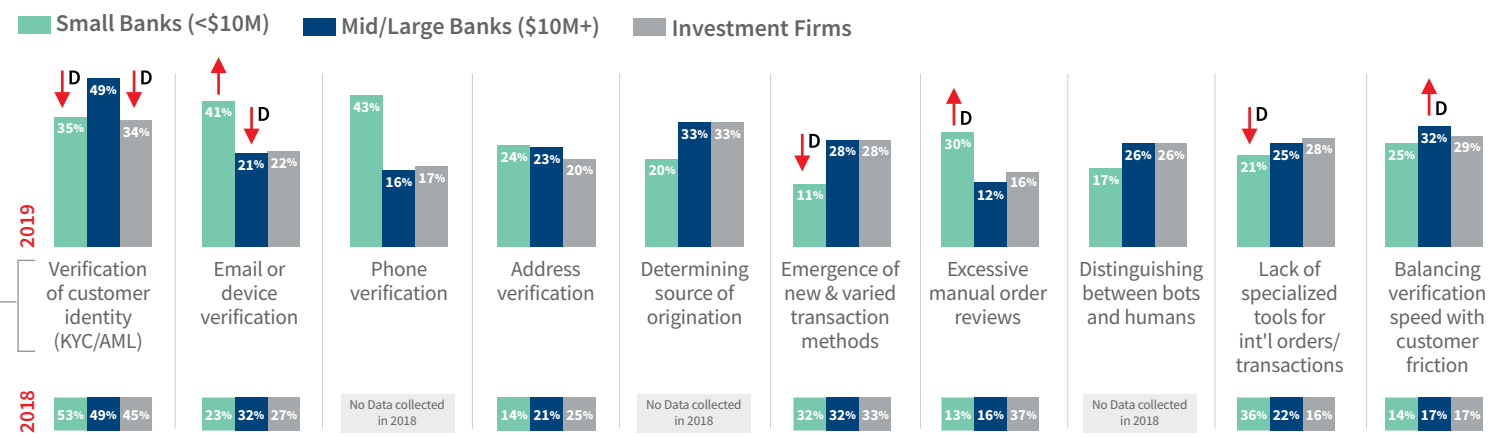
Mid/Large banks also struggle most with identity verification as it relates to determining the source of origination.

The rise of synthetic identities, volume of malicious botnet attacks and need for real-time third-party data are top underlying factors contributing to the above issues.

Balancing identity verification with speed and minimal customer friction is a challenge across financial services organizations.



## Top Ranked ONLINE FRAUD Challenges Among Top 3 Ranked: Financial Services Firms



**Top Identity Verification Challenges\***

- Rise of synthetic identities (55%)
- Volume of malicious botnet attacks (49%)
- Need for real-time third-party data (48%)

\* Base sizes for reporting individual segments selecting verification of customer identity too low; need to report in aggregate across the above segments

Noted directional decreases from 2018 for verification of customer identity and email device verification do not necessarily indicate that these are less critical issues; since this is a ranking question (top 3), a decrease more often means that other challenges are either rising to the top or that there is a broadening of issues faced by firms such that there is less consensus around any one specific challenge.

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

# Determining source origination, distinguishing between botnets and legitimate transactions and need for real-time third-party data contribute to identity verification issues among digital lenders.

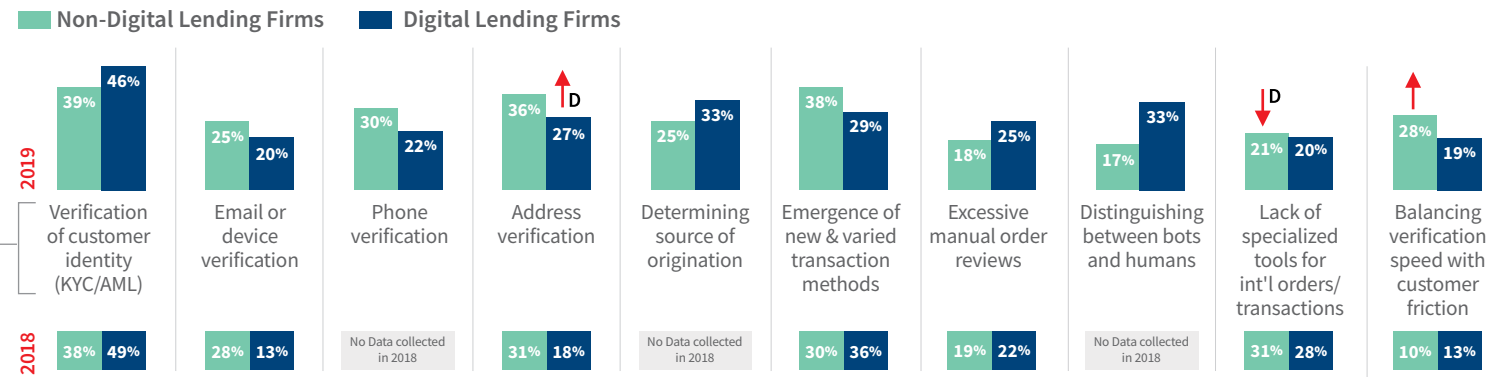
The rise of synthetic identities is a particular underlying cause of identity verification challenges cited by digital lenders.

Balancing verification speed with customer friction has increased as a challenge among non-digital firms, which are more multi-channel

focused rather than digital firms that conduct a majority of business remotely. As shown later, fewer non-digital lending firms invest in solutions that support newer risks in the digital channels; rather, they continue to rely on traditional types of identity proofing solutions and data across different channels.



## Top Ranked ONLINE FRAUD Challenges Among Top 3 Ranked: Lending Firms



### Top Identity Verification Challenges

#### NON-DIGITAL LENDING FIRMS

- Balancing speed of fraud detection with customer friction (61%)
- Need for real-time third-party data (49%)
- Limited ability to identify geolocation (45%)

#### NON-DIGITAL LENDING FIRMS

- Rise of synthetic identities (64%)
- Limited ability to identify geolocation (57%)
- Need for real-time third-party data (46%)

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

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

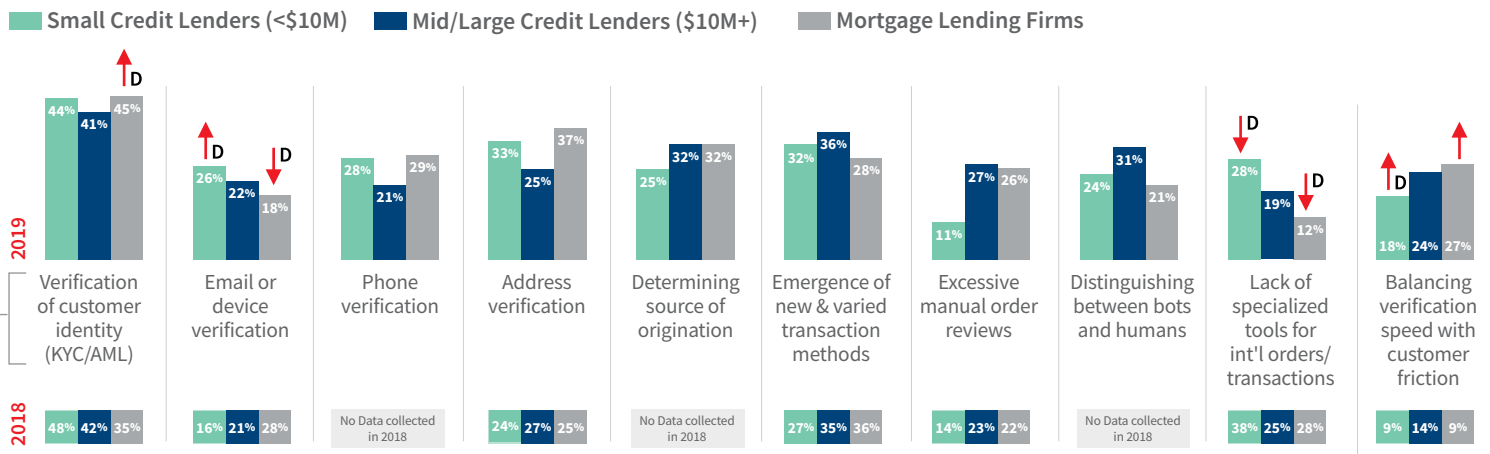
# Identity verification also remains a key online challenge for lenders and had directionally increased as an issue among mortgage lenders.

A limited ability to identify geolocation, the rise of synthetic identities and the need for more real-time third-party data are key underlying reasons for identity verification issues.

As with other segments, there continues to be an increasing focus on increasing the speed of this verification in order to minimize customer friction.



## Top Ranked ONLINE FRAUD Challenges Among Top 3 Ranked: Lending Firms



**Top Identity Verification Challenges LENDERS\***  
 Limited ability to identify geolocation (52%)  
 Rise of synthetic identities (51%)  
 Need for real-time third-party data (47%)

\* Base sizes for reporting individual segments selecting verification of customer identity too low; need to report in aggregate across the above segments

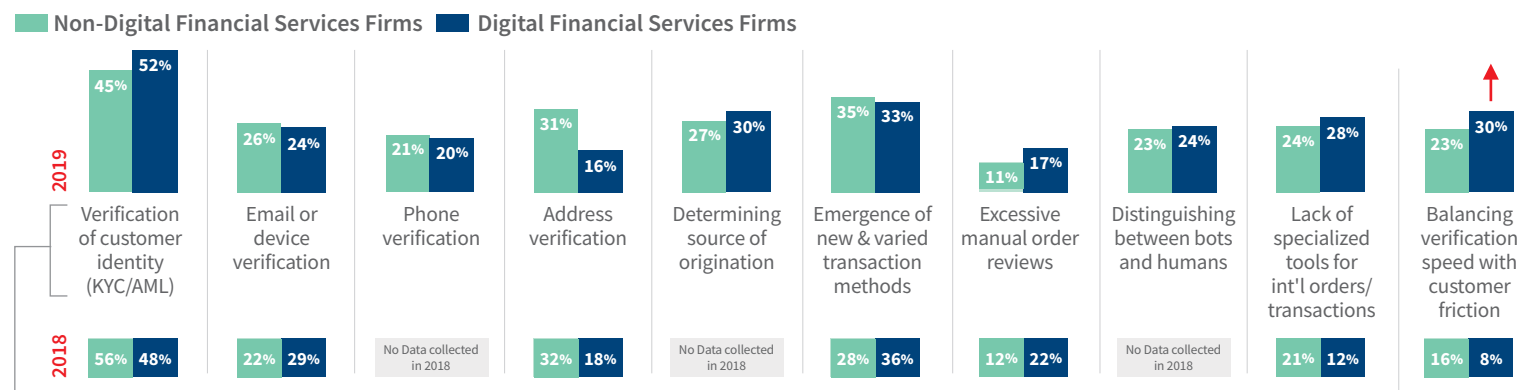
# Key mobile channel challenges have remained fairly constant for digital and non-digital financial services firms, though with a rise in the challenge of balancing verification speed against friction.

The emergence of new / varied transaction methods also remains a challenge, as is determining the source of transaction origination. Both digital and non-digital financial services firms point to the underlying nature of the mobile channel and a limited ability to identify geolocation as key reasons for identity verification issues.

Digital firms are also likely to mention the volume of malicious botnet attacks, with significantly more ranking customer friction and transaction speed as challenge compared to 2018.



## Top Ranked MOBILE FRAUD Challenges Among Top 3 Ranked: Financial Services Firms



### Top Identity Verification Challenges

**NON-DIGITAL FS FIRMS\***  
 Limited ability to identify geolocation (81%)  
 Need for real-time third-party data (66%)  
 Use of the mobile channel (56%)  
 Rise of synthetic identities (47%)

**DIGITAL FS FIRMS**  
 Balancing speed of fraud detection with customer friction (58%)  
 Limited ability to identify geolocation (49%)  
 Use of the mobile channel (43%)  
 Volume of malicious botnet attacks (42%)

\* CAUTION: Low base size of non-digital firms using the mobile channel and ranking identity verification as a top mobile challenge

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

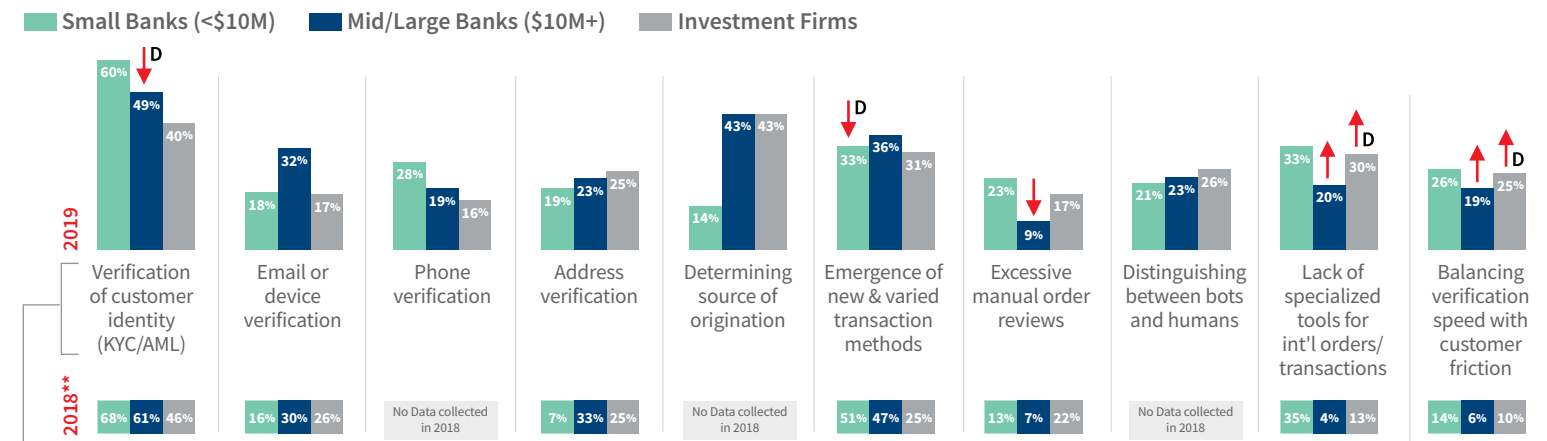
# Investment firms and mid/large banks are particularly more challenged with determining transaction origination compared to small banks. This relates to their higher volume of cross-border business.

Verifying email or device also remains a mobile channel challenge for mid/large banks. That isn't surprising since – as shown later – few are using solutions to support this (i.e., device ID, email risk and verification).

Lack of specialized tools for international transactions has risen as a challenge, which aligns with limited ability to identify geolocation as an underlying cause of identity verification issues (along with the rise of synthetic identities).



## Top Ranked MOBILE FRAUD Challenges Among Top 3 Ranked: Financial Services Firms



**Top Identity Verification Challenges\***  
 Limited ability to identify geolocation (58%)  
 Use of the mobile channel (47%)  
 Balancing speed of fraud detection with customer friction (47%)  
 Rise of synthetic identities (41%)

\* Base sizes for reporting individual segments selecting verification of customer identity too low; need to report in aggregate across the above segments  
 \*\* CAUTION: Low base size of small banks using the mobile channel in 2018

Noted directional decrease among mid/large banks from 2018 for verification of customer identity does not necessarily indicate that this is a less critical issue; since this is a ranking question (top 3), a decrease more often means that other challenges are either rising to the top or that there is a broadening of issues faced by firms such that there is less consensus around any one specific challenge.

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

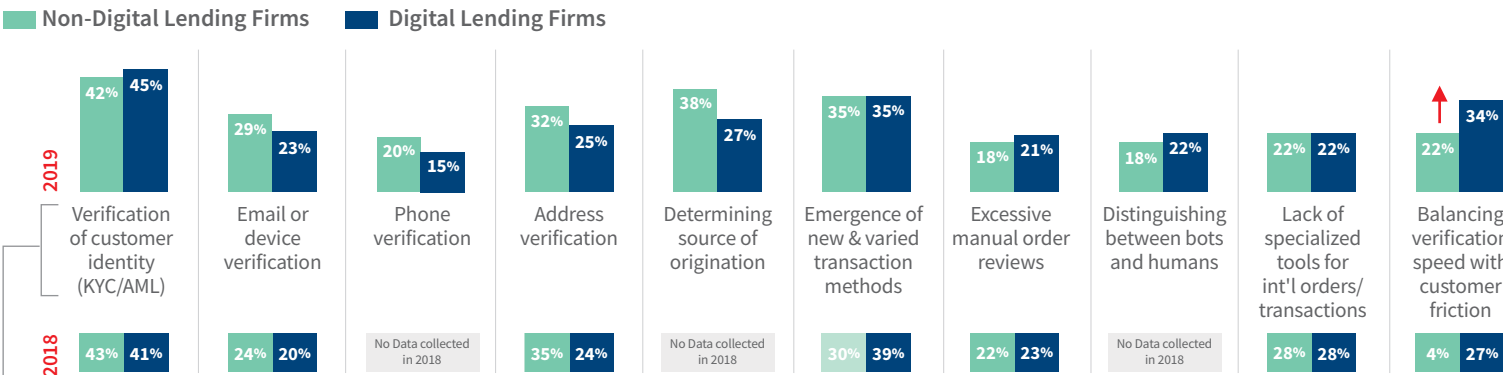
# Key mobile channel challenges for digital and non-digital lenders have remained fairly constant since 2018.

Where this differs, it is with a significant increase for balancing verification speed with customer friction among non-digital lenders. This was also seen with online channel challenges and the need for investing in solutions that will more effectively support identity verification in the digital environment.

Both digital and non-digital lending firms blame the underlying nature of the mobile channel as a key challenge for identity verification.. They also point to the rise of synthetic identities, need for real-time, third-party data and limited ability to identify geolocation.



## Top Ranked MOBILE FRAUD Challenges Among Top 3 Ranked: Lending Firms



### Top Identity Verification Challenges

**NON-DIGITAL LENDING FIRMS**  
 Use of the mobile channel (67%)  
 Rise of synthetic identities (63%)  
 Need for real-time third-party data (42%)  
 Limited ability to identify geolocation (41%)

**DIGITAL LENDING FIRMS**  
 Rise of synthetic identities (61%)  
 Use of the mobile channel (58%)  
 Need for real-time third-party data (55%)  
 Limited ability to identify geolocation (45%)

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

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

# Identity verification has particularly increased as a mobile channel challenge for mortgage lenders.

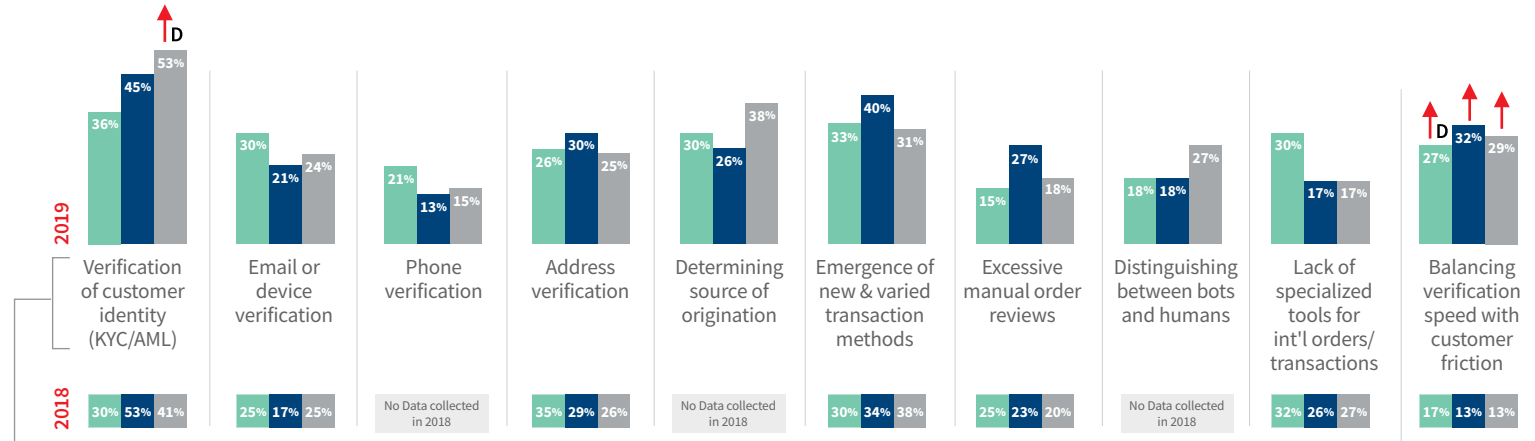
The rise of synthetic identities and need for more real-time, third-party data contribute to this, as well as (directionally) the inability to determine location origination and distinguish between malicious bots and legitimate human transactions.

Balancing verification speed with customer friction has increased across lenders as a mobile channel issue.



## Top Ranked MOBILE FRAUD Challenges Among Top 3 Ranked: Lending Firms

Small Credit Lenders (<\$10M)    Mid/Large Credit Lenders (\$10M+)    Mortgage Lending Firms



**Top Identity Verification Challenges LENDERS\***  
Use of the mobile channel (61%)  
Rise of synthetic identities (61%)  
Need for real-time third-party data (50%)

\* Base sizes for reporting individual segments selecting verification of customer identity too low; need to report in aggregate across the above segments

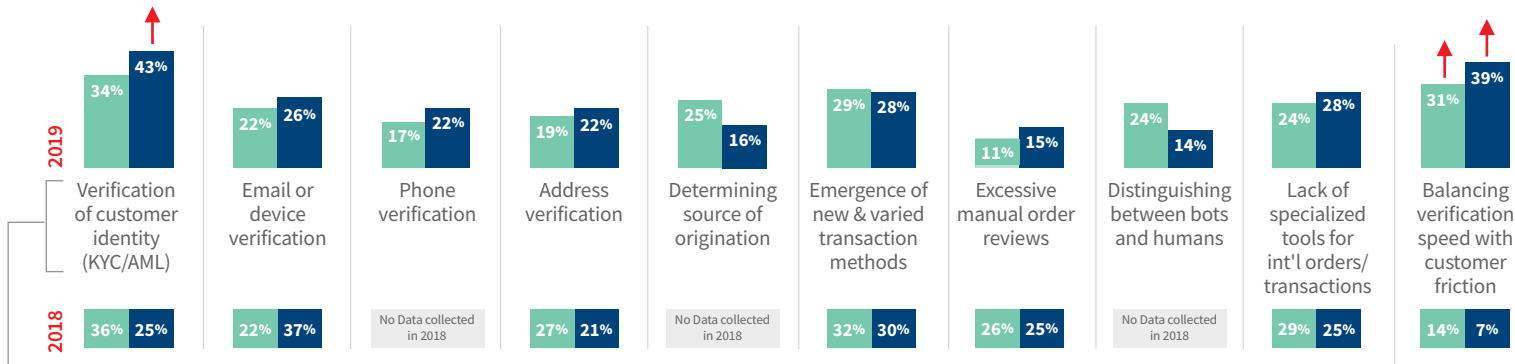
# Identity verification has increased significantly as a top ranked challenge with financial services firms using the mobile channel for international transactions.

A limited ability to identify geolocation and deal with malicious botnet attacks while also providing quick verification and minimal customer friction are related to this.



## Top Ranked ONLINE & MOBILE FRAUD Challenges Among Top 3 Ranked: Mid/Large Financial Services Firms with International

Online Channel Challenges    Mobile Channel Challenges



### Top Identity Verification Challenges

#### INTERNATIONAL MOBILE CHANNEL TRANSACTIONS

Limited ability to identify geolocation (64%)  
Balancing speed of fraud detection with customer friction (52%)  
Volume of malicious botnet attacks (48%)

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

# Key Finding #4: Impacts

- Overview
- Key Findings
  - #1 Attacks & Costs
  - #2 Trends
  - #3 Challenges
  - #4 **Impacts**
  - #5 Tracking & Solution Usage
  - #6 Strategic Approaches
- Recommendations



- 4** All of this is increasing fraud volume and costs for digital financial services and lending firms that conduct mobile and/or international transactions.
- There has been a significantly sharp rise in fraud attacks on digital financial services and lending firms, particularly those that use the mobile channel.
  - Identity-related fraud represents a significant portion of all fraud losses, particularly among mid/large banks with mobile channel and international transactions.
  - Account takeover fraud represents a majority of identity-related fraud activities, particularly for smaller digital banks and mortgage lenders using the mobile channel and which have not invested in digital risk mitigation solutions.
  - Therefore, the cost of fraud is higher for digital firms using the mobile channel and conducting international transactions.

**Survey Questions:**  
Q22: In a typical month, approximately how many fraudulent transactions are prevented by your company?  
Q24: In a typical month, approximately how many fraudulent transactions are successfully completed at your company?

# There has been a significantly sharp rise in fraud attacks on digital financial services firms, particularly banks.

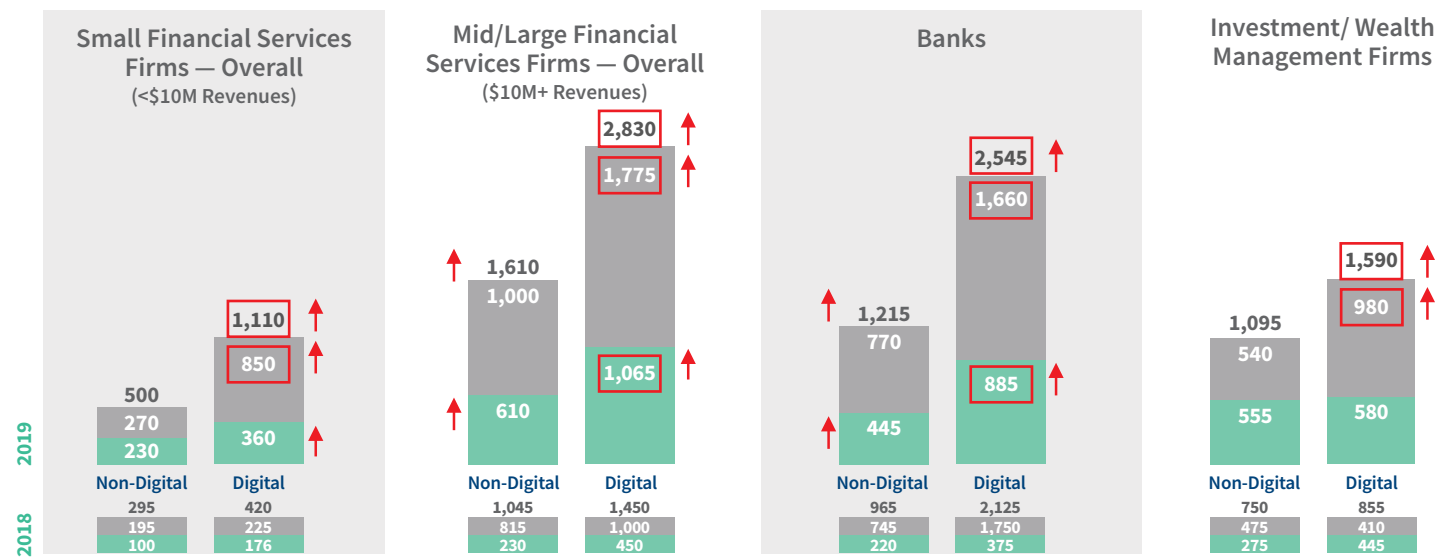
The trend continues where digital firms experience a higher volume of fraud attacks than non-digital ones. However, fraudsters have also been attacking bricks and mortar (non-digital) firms as shown by significant jumps in their successful fraud attempts. It's important to keep in mind that while non-digital firms (according to our definition) do not conduct a majority of business through remote channels, they

nonetheless have broadened their multi-channel business model to these channels as a means of remaining competitive and meeting consumer demand. Therefore, they can also be faced with significant risk of fraud – especially those which limit investments in next generation digital identity solutions.



## Average Number of Total Fraud Attempts Per Month: Digital Financial Services Firms

■ Average Number of Attempts Prevented per Month ■ Average Number of Attempts that Succeed per Month



**Survey Questions:**  
**Q22:** In a typical month, approximately how many fraudulent transactions are prevented by your company?  
**Q24:** In a typical month, approximately how many fraudulent transactions are successfully completed at your company?

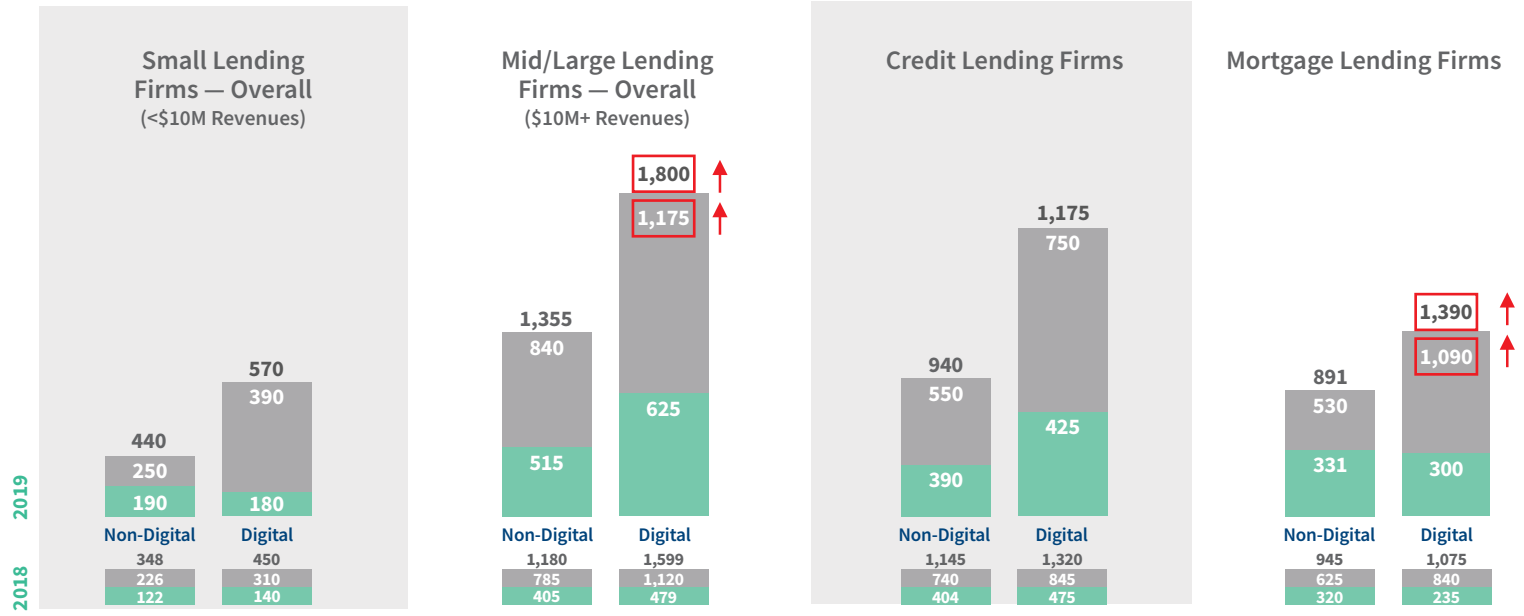
# There has also been an increase in fraud attacks among mid/large digital lenders, particularly mortgage lenders.

Again, being a digital lending firm carries more risk and fraud volume. That said, there has been a significantly greater year-over-year fraud emphasis and impact on digital banks in comparison to lending firms.



## Average Number of Total Fraud Attempts Per Month: Digital Lending Firms

■ Average Number of Attempts Prevented per Month ■ Average Number of Attempts that Succeed per Month



**Survey Questions:**  
Q22: In a typical month, approximately how many fraudulent transactions are prevented by your company?  
Q24: In a typical month, approximately how many fraudulent transactions are successfully completed at your company?

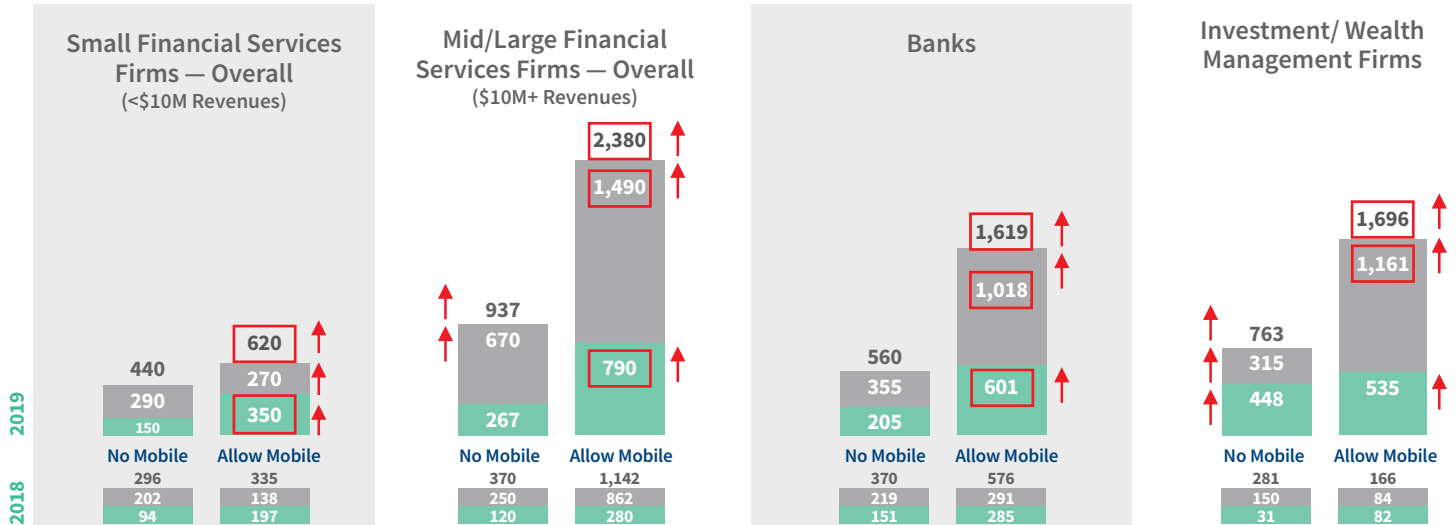
# Adding mobile to one's channel strategy continues to invite fraud attacks, which have increased significantly for mid/large financial services firms.

But there has also been an increase among smaller firms. More financial services firms in this size segment are new to the mobile channel within the past year, particularly smaller banks which have not invested in solutions to address unique risks from mobile transactions (e.g., Device ID, Geolocation, Authentication Using Biometrics, Email Risk & Verification).



## Average Number of Total Fraud Attempts Per Month: Financial Services Firms Using Mobile Channels

■ Average Number of Attempts Prevented per Month   ■ Average Number of Attempts that Succeed per Month

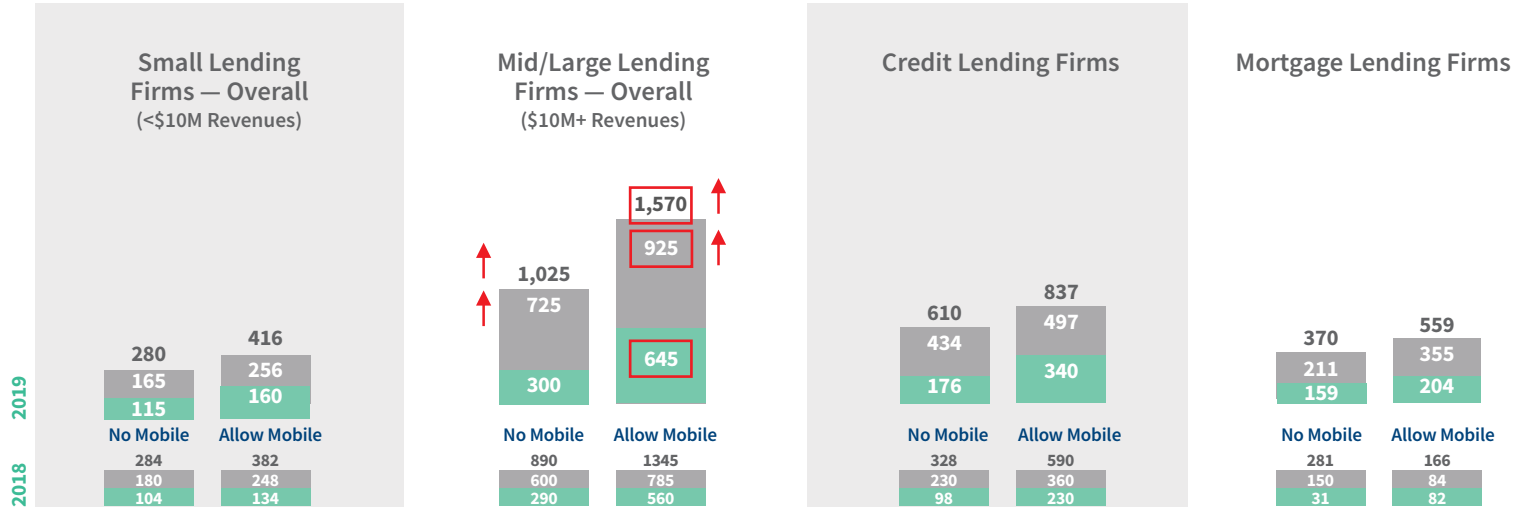


There has been a moderate increase in fraud attacks for mid/large lending firms using the mobile channel, but not as significant as found for mobile channel financial services firms.



### Average Number of Total Fraud Attempts Per Month: Lending Firms Using Mobile Channels

■ Average Number of Attempts Prevented per Month ■ Average Number of Attempts that Succeed per Month



**Survey Questions:**  
**Q22:** In a typical month, approximately how many fraudulent transactions are prevented by your company?  
**Q24:** In a typical month, approximately how many fraudulent transactions are successfully completed at your company?

# Financial services firms report a high proportion of identity-related fraud, with mid/large digital banks that allow mobile and international transactions experiencing the highest.

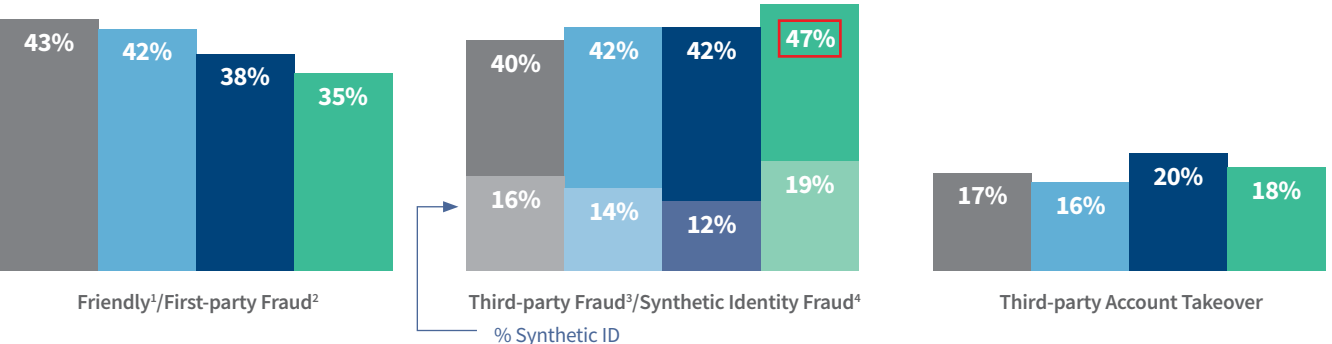
They also report a higher distribution of these losses attributed to synthetic identities than others. Overall, the higher level of identity-related losses among this segment relates to a larger degree and increased level of botnet attacks, limitations with determining

transaction origination / location and limited use of specific risk mitigation solutions that could address these unique issues (e.g., Geolocation, Authentication Using Biometrics, Email Risk / Verification).



## Distribution of Fraud Losses by Type: Financial Services

Financial Services Firms Overall    Digital Financial Services Firms  
Small Digital Banks w/Mobile Channel    Mid/Large Digital Banks w/Mobile & International



**Survey Question:**  
Q12: Please indicate, to the best of your knowledge, the percentage distribution of the following fraud methods below, as they are attributed to your total annual fraud loss over the past 12 months.

1. Friendly fraud (an individual associated with/having access to an account conducts transaction without the primary account owner's knowledge or permission)
2. 1st party fraud (owner to authorized user of the account commits the fraud)
3. third-party identity fraud (unauthorized transaction using other people's existing/real information)
4. Synthetic identity fraud (creation of a new identity using a combination of real and fabricated information, sometimes entirely fictitious)

# Identity fraud activity primarily involves account login/takeover among financial services firms.

Small digital banks using the mobile channel attribute a somewhat higher distribution of identity-related to account login/takeover than others.

Mid/Large digital banks with both mobile and international channel transactions are also likely to indicate a majority related to account takeover, but they are likely to mention fraudulent account creation more so than others.

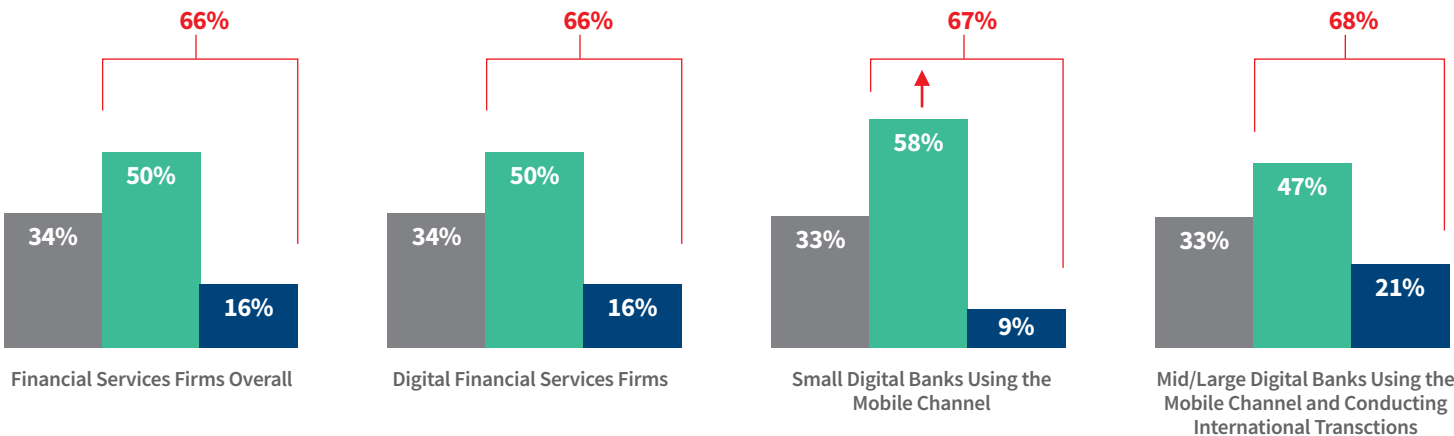


## Identity-related Fraud Distribution by Activity: Financial Services

Fraudulent Distribution of Funds

Account Login<sup>1</sup>/Takeover

Fraudulent Account Creation<sup>2</sup>



**Survey Question:**  
Q12b: For identity-related fraud, what is the distribution of these by the following types of activities?

- Account login (to hack, access or take over an account)
- Account creation (fraudulently establish an account using other people's identity/personal information)

**Survey Question:**  
**Q16a:** In thinking about the total fraud losses suffered by your company, please indicate the distribution of various direct fraud costs over the past 12 months.

# Mortgage lending firms also report a high proportion of identity-related fraud. Adding the mobile channel increases this; adding international increases account takeover risk.

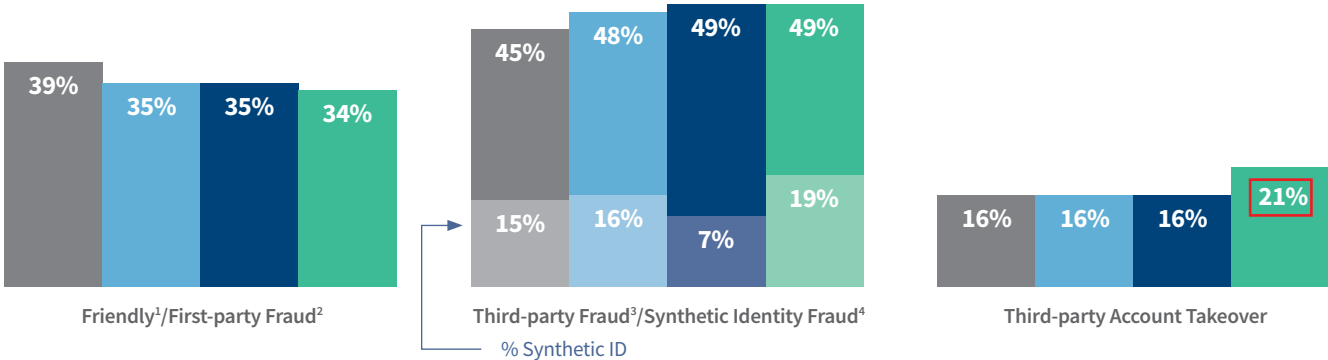
Small mortgage lending firms that use the mobile channel report nearly 50% of their fraud losses as involving identity fraud. This could actually be higher since they attribute a very small percent of these to synthetic identities which are very difficult to detect. Given more limited use of digital identity solutions to detect these, it's likely that some portion of synthetic identity-related fraud is going unreported / unnoticed.

For mid/large digital credit lending firms, the addition the mobile channel and international transactions increases the level of reported losses related to both synthetic identities and third-party account takeovers.



## Distribution of Fraud Losses by Type: Lending Firms

Lending Firms Overall
  Digital Lending with Mobile
  Small Mortgage Lending with Mobile
  Mid/Large Credit Lending w/Mobile & International



1. Friendly fraud (an individual associated with/having access to an account conducts transaction without the primary account owner's knowledge or permission)  
 2. 1st party fraud (owner to authorized user of the account commits the fraud)  
 3. Third-party identity fraud (unauthorized transaction using other people's existing/real information)  
 4. Synthetic identity fraud (creation of a new identity using a combination of real and fabricated information, sometimes entirely fictitious)

## Identity fraud activity also primarily involves account login/takeover among lending firms.

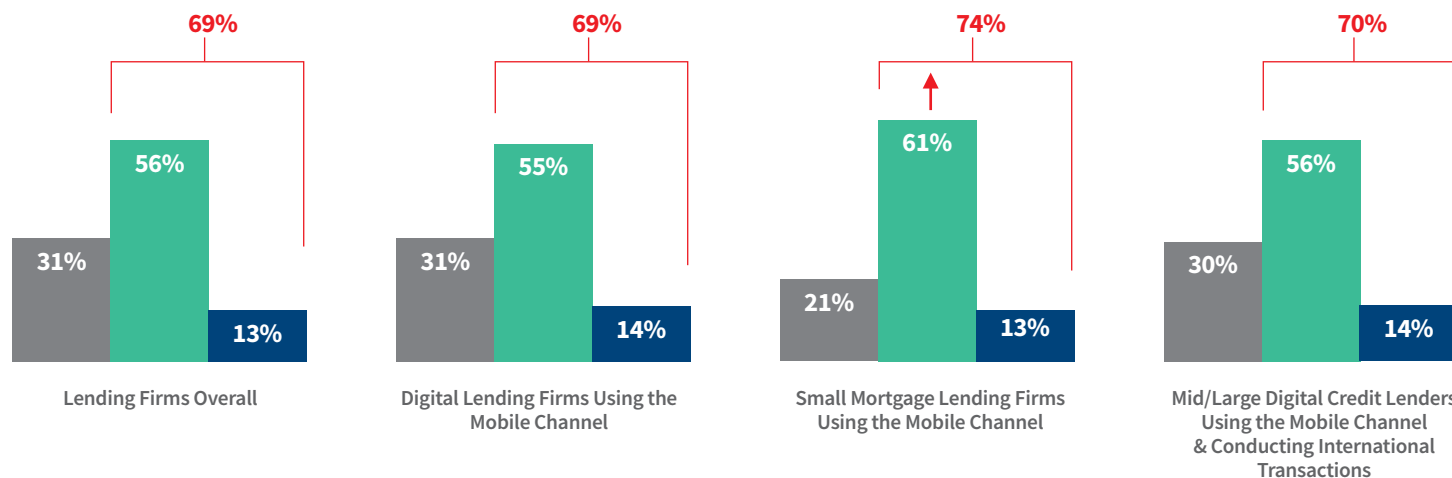
Small mortgage firms using the mobile channel attribute a somewhat higher distribution of identity-related to account login/takeover than others.



### Identity-related Fraud Distribution by Activity: Lending Firms

Fraudulent Distribution of Funds

Account Login<sup>1</sup>/Takeover

Fraudulent Account Creation<sup>2</sup>


#### Survey Question:

**Q12b:** For identity-related fraud, what is the distribution of these by the following types of activities?

- Account login (to hack, access or take over an account)
- Account creation (fraudulently establish an account using other people's identity/personal information)

1. Account login (to hack, access or take over an account)

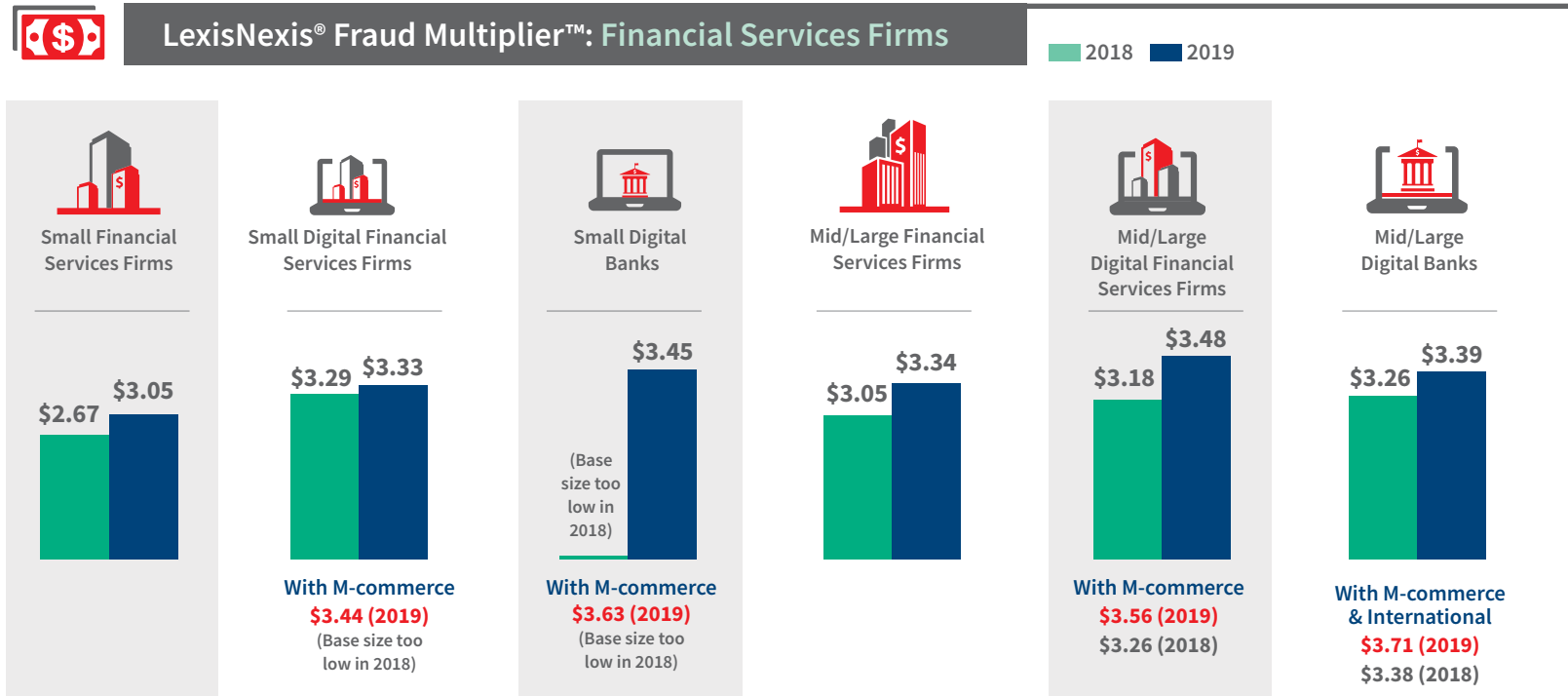
2. Account creation (fraudulently establish an account using other people's identity/personal information)

**Survey Question:**  
Q16a: In thinking about the total fraud losses suffered by your company, please indicate the distribution of various direct fraud costs over the past 12 months.

# The impact of these fraud trends is that the cost of fraud is higher for financial services firms that are digital, use the mobile channel and conduct international transactions.

Each additional layer (e.g., adding the mobile channel, adding more international) tends to increase the cost of fraud to these firms because, as demonstrated earlier, these factors add further layers of risk. Further, a number of firms in these higher risk segments

are applying the same traditional risk detection solutions across channels and types of transactions, even though each channel / transaction has a different / unique set of risks and challenges.



**The cost of fraud has grown significantly for mid/large digital lending firms, particularly credit lenders with mobile and cross-border transactions.**

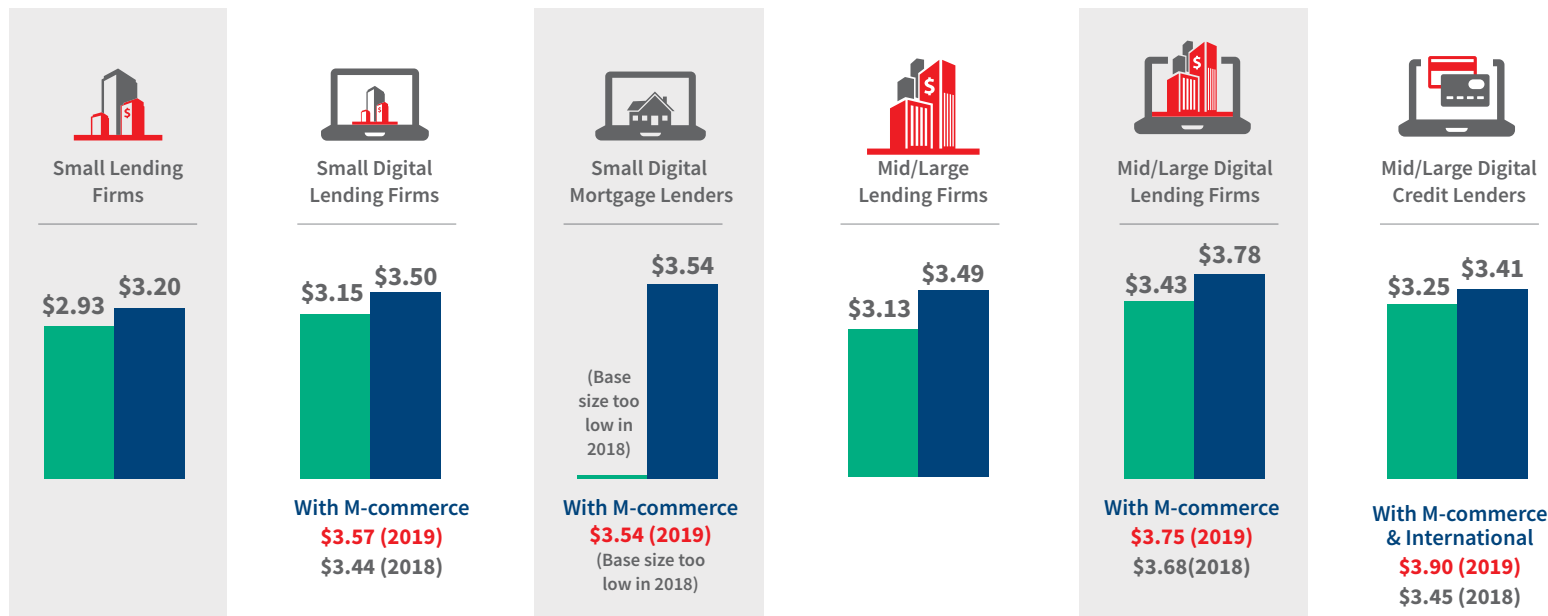
Each additional layer (e.g., adding the mobile channel, adding more international) tends to increase the cost of fraud to these firms because, as demonstrated earlier, these factors add further layers of risk. Further, a number of firms in these higher risk segments are

applying the same traditional risk detection solutions across channels and types of transactions, even though each channel / transaction has a different / unique set of risks and challenges.



## LexisNexis® Fraud Multiplier™: Lending Firms

■ 2018 ■ 2019



**Survey Question:**

**Q16a:** In thinking about the total fraud losses suffered by your company, please indicate the distribution of various direct fraud costs over the past 12 months.



Overview



Key Findings



Attacks &amp; Costs



Trends



Challenges



Impacts

Tracking &  
Solution Usage

Strategic Approaches



Recommendations

## Key Finding #5: Tracking & Solution Usage



5

Financial services and lending firms most at-risk for attack may not be optimizing solutions and approaches to fight newer and more complex types of fraud.

- As fraud continues to become more sophisticated, the use of more sophisticated solutions remains limited.
- There is limited use of passive / digital identity-based solutions that will detect more complex forms of identity fraud, including synthetic identities and botnet attacks.
- Further, firms are not tracking fraud from a holistic perspective involving successful and prevented attacks through different channels and transaction methods.

**Survey Question:**  
Q26: Does your company track the cost of fraudulent transactions by payment channels or methods? Track successful fraud by payment channels or methods?

# Tracking all of the ways that fraud impacts the business is essential — both successful and prevented by channel and payment methods.

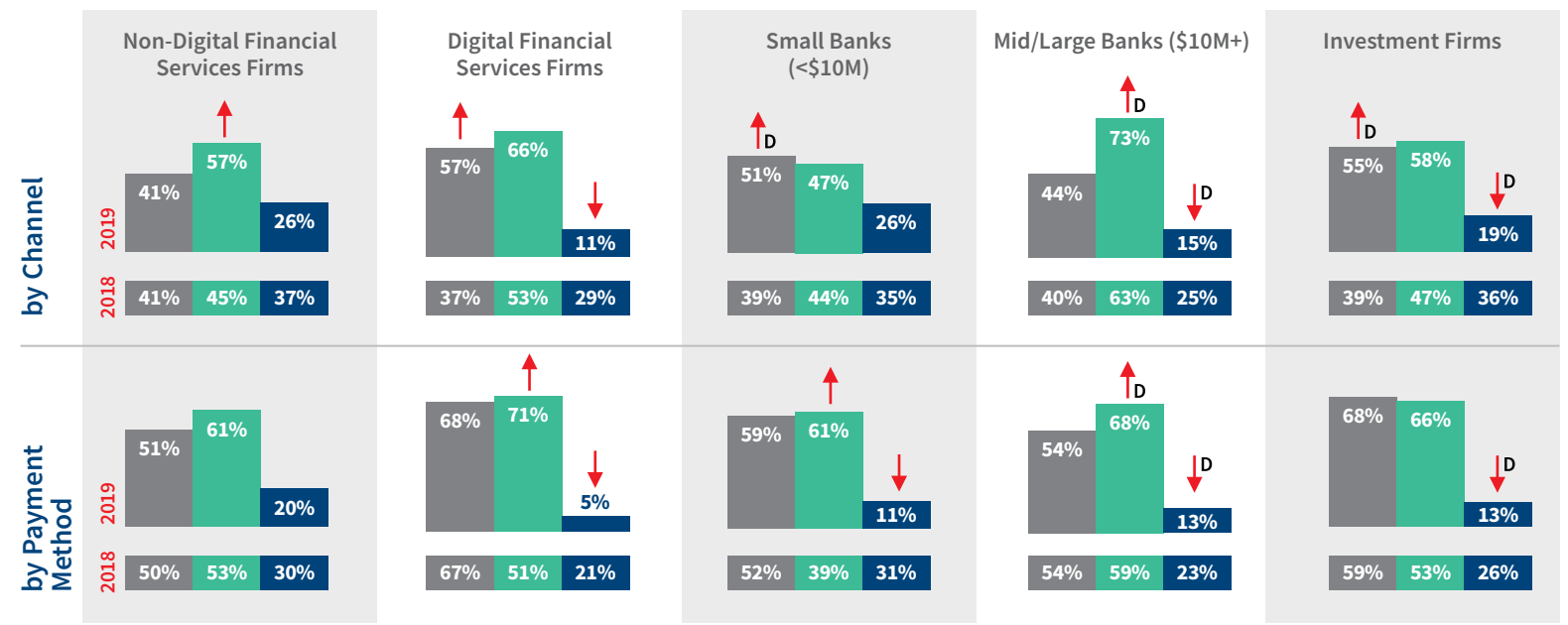
More firms have begun to track both successful and prevented fraud by transaction channel and payment method, though there's a sizeable minority of firms across this industry which do not. For the latter,

this weakens efforts to fully detect and mitigate fraud as criminals constantly probe for the weakest links.



## Tracking Successful & Prevented Fraud Transactions: Financial Services Firms

■ Track Prevented ■ Track Successful ■ Does Not Track



# Lending firms have the same level of fraud tracking as found with financial services firms.

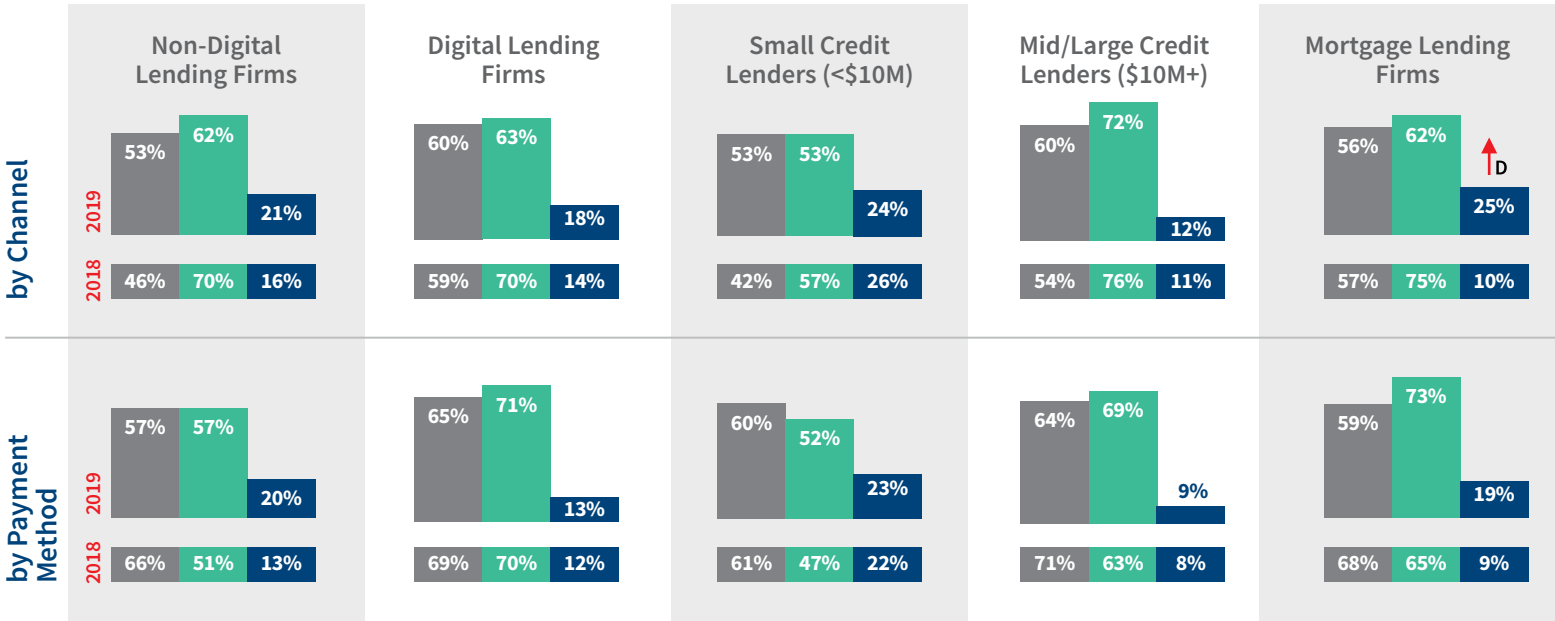
There is a directional relationship between tracking successful fraud transactions by both channel and payment methods and lower fraud costs. The harder hit large digital lenders and large digital creditors are somewhat less likely to track both.

- Overview
- Key Findings
- #1 Attacks & Costs
- #2 Trends
- #3 Challenges
- #4 Impacts
- #5 Tracking & Solution Usage
- #6 Strategic Approaches
- Recommendations



## Tracking Successful & Prevented Fraud Transactions: Lending Firms

Track Prevented Track Successful Does Not Track



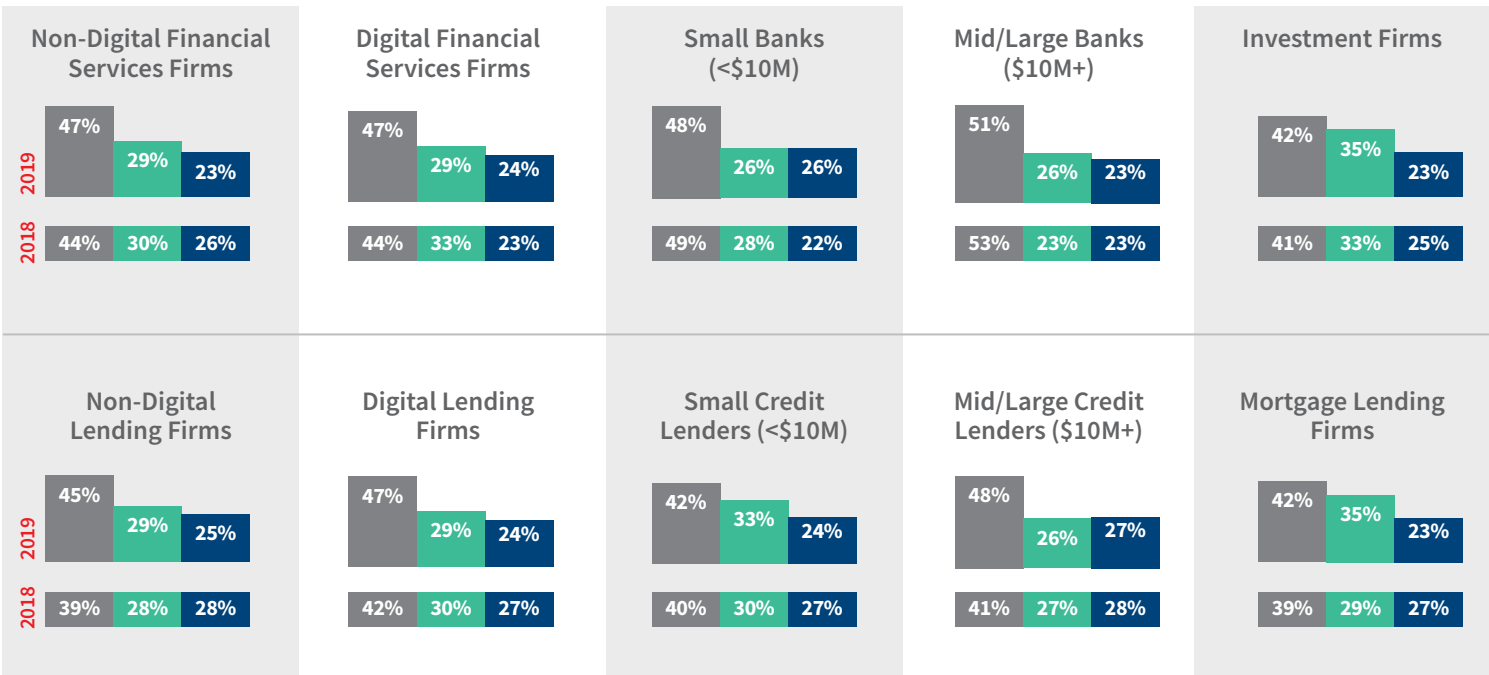
**Survey Question:**  
Q26: Does your company track the cost of fraudulent transactions by payment channels or methods? Track successful fraud by payment channels or methods?

# Risk mitigation solutions remain a significant portion of financial services and lending firms' fraud mitigation budgets. However, manual reviews also continue to be sizeable as well.



## Distribution of Fraud Mitigation Costs by Percent of Spend: Financial Services Firms and Lending Firms

■ Cost of Fraud Solutions ■ Cost of Manual Reviews ■ Cost of Physical Security



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

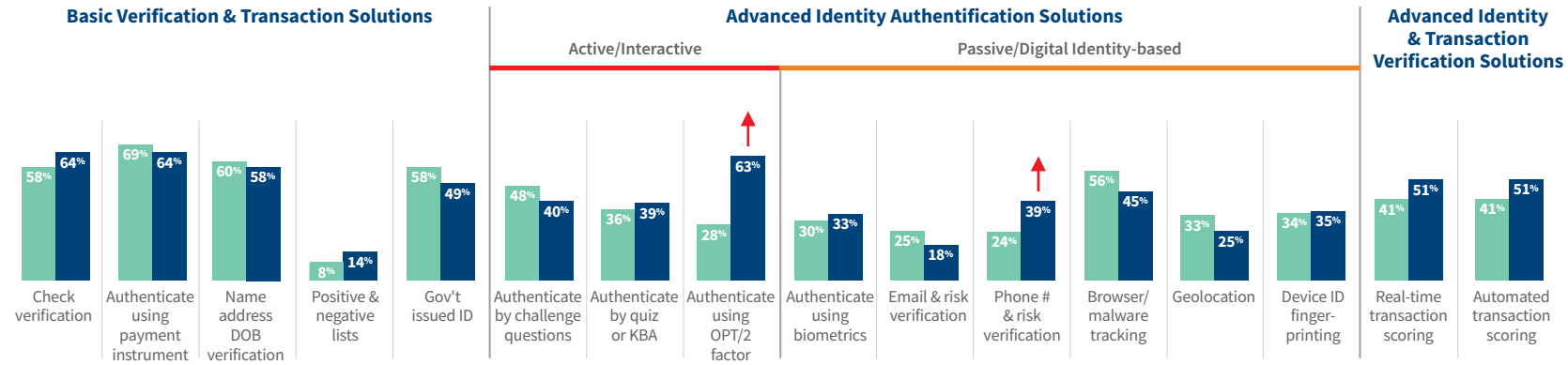
# While more digital financial services firms report using authentication using OTP/2 factor, the use of other identity solutions designed to address unique digital identity threats is limited.

In fact, digital firms are more likely to use solutions to test the physical identity attributes, such as name/DOB, check verification and government-issued ID, than solutions to assess the threats unique to the digital channel – as described on the previous page. This is a significant contributor to higher fraud volume and costs among these types of firms.



## Fraud Mitigation Solutions Usage\*: Financial Services Firms

Non-Digital Financial Services Firms Digital Financial Services Firms



Survey Question:  
Q27: Which of the following fraud solutions does your company currently use?

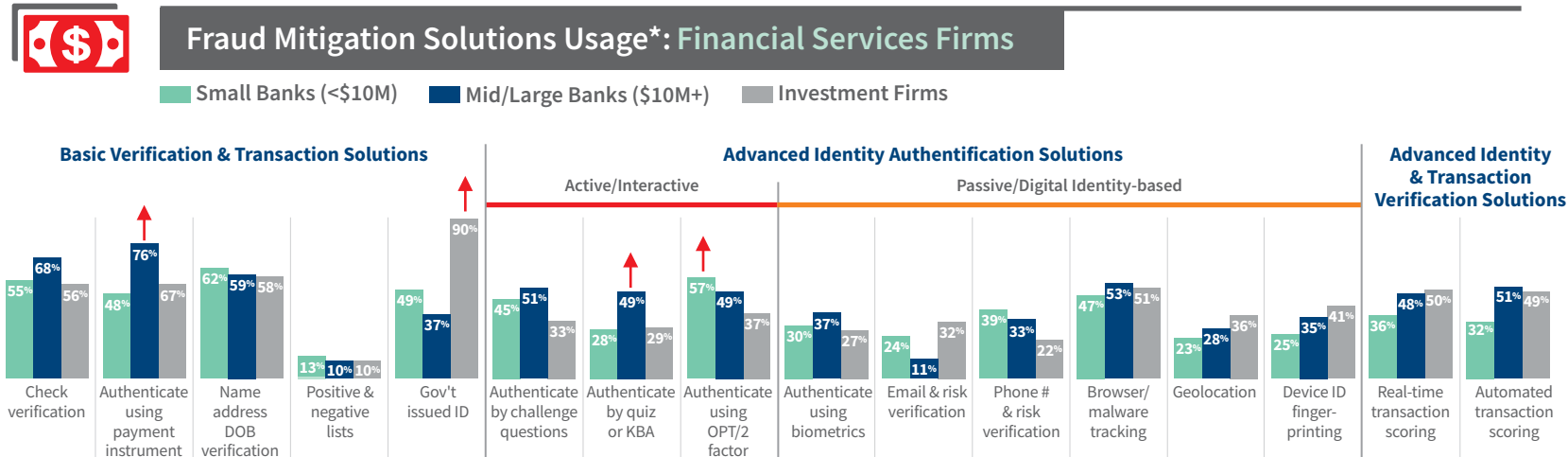
\*Solutions list was modified in 2019, making it difficult to trends from previous waves

**Survey Question:**  
Q27: Which of the following fraud solutions  
does your company currently use?

# The limited use of solutions to identify digital behavior threats are found across types of financial services firms, including for those which face unique challenges from the mobile channel.

As more smaller banks have adopted the mobile channel, few appear to have invested in solutions designed to address the challenges specific to this channel as identified earlier. This includes a low incidence with authentication using biometrics, email risk and verification, geolocation and device ID. This can also be said for mid/ large banks that not only allow mobile transactions, but also cross-border ones as well.

The exception is with mid/large digital investment / wealth management firms, which have been more likely to invest in a number of passive / digital identity and transaction-based solutions as noted below. It is important to understand that these types of digital identity solutions are more effective for remote channels and international transactions, not only to more successfully stop fraud, but address the key challenge of doing so quickly while minimizing customer friction.



More mid/large digital investment firms have adopted Email Risk & Verification (50%), Geolocation (63%), Device ID (77%), Real-time Transaction Scoring (65%), and Automated Transaction Scoring (68%)

\*Solutions list was modified in 2019, making it difficult to trends from previous waves

**Survey Question:**  
Q27: Which of the following fraud solutions  
does your company currently use?

# There is also significantly limited use of solutions among digital lender to effectively detect complex fraud, including synthetic identities and botnets, that are unique to the digital channels.

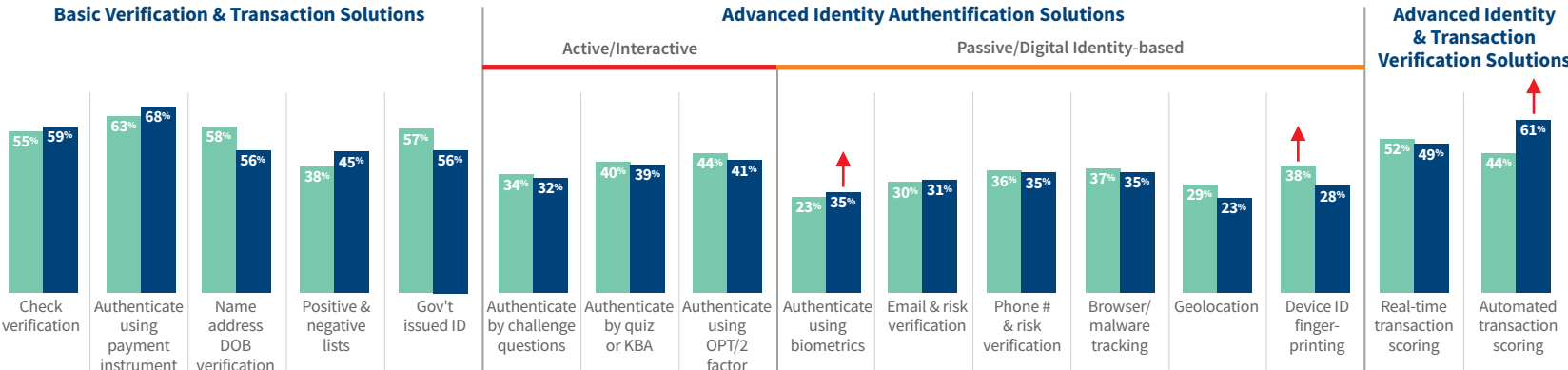
As with financial services, digital lending firms are more likely to use solutions to test the physical identity attributes, such as name/DOB, check verification and government-issued ID. Therefore, they experience more successful fraud attacks and cost than non-digital firms.

Having said that, there are a slight majority of digital lenders which do use automated transaction scoring, keeping in mind the importance of assessing both the identity and the transaction.



## Fraud Mitigation Solutions Usage\*: Lending Firms

Non-Digital Lending Firms Digital Lending Firms



\*Solutions list was modified in 2019, making it difficult to trends from previous waves

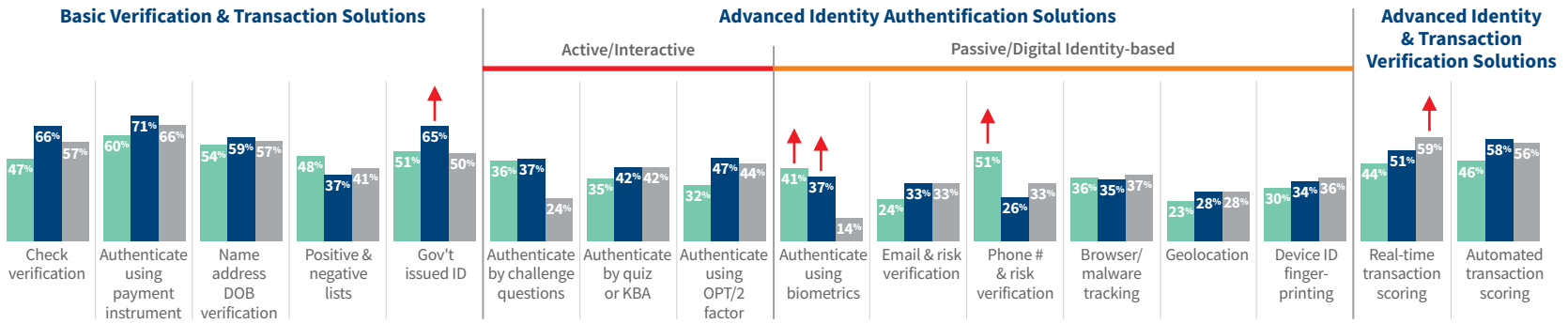
# The limited use of solutions to identify digital behavior threats are also found across types of lending firms, including for those which face unique challenges from the mobile channel.

That said, there is a sizeable minority of credit lenders who have invested in biometrics authentication.



## Fraud Mitigation Solutions Usage\*: Lending Firms

Small Credit Lenders (<\$10M)    Mid/Large Credit Lenders (\$10M+)    Mortgage Lending Firms



**Survey Question:**  
Q27: Which of the following fraud solutions does your company currently use?

\*Solutions list was modified in 2019, making it difficult to trends from previous waves

- Overview
- Key Findings
- #1 Attacks & Costs
- #2 Trends
- #3 Challenges
- #4 Impacts
- #5 Tracking & Solution Usage
- #6 Strategic Approaches
- Recommendations

# Fraud has become more complex; various risks can occur at the same time with no single solution. Fraud tools need to authenticate both digital and physical criteria, as well as both identity and transaction risk.

FRAUD ISSUES



**Digital services**  
fast transactions, easy synthetic identity and botnet targets; **need velocity checking to determine transaction risk along with data and analytics to authenticate the individual**



**Account-related fraud**  
breached data **requires more levels of security, as well as authenticating the person from a bot or synthetic ID**



**Synthetic identities**  
**need to authenticate the whole individual** behind the transaction in order to distinguish from, fake identity based on partial real data



**Botnet attacks**  
mass human or automated attacks often to test cards, passwords/credentials or infect devices



**Mobile channel**  
source origination and infected devices add risk; mobile bots and malicious malware makes authentication difficult; **need to assess the device and the individual**

SOLUTION OPTIONS

ASSESSING THE TRANSACTION RISK

**Velocity checks/transaction scoring:** monitors historical trans-action patterns of an individual against their current transactions to detect if volume by the cardholder match up or if there appears to be an irregularity. **Solution examples:** real-time transaction scoring; automated transaction scoring

▶ AUTHENTICATING THE PHYSICAL PERSON ▶

**Basic Verification:** verifying name, address, DOB or providing a CVV code associated with a card. **Solution examples:** check verification services; payment instrument authentication; name/ address/DOB verification

**Active ID Authentication:** use of personal data known to the customer for authentication; or where user provides two different authentication factors to verify themselves. **Solution examples:** authentication by challenge or quiz; authentication using OTP/ 2 factor

▶ AUTHENTICATING THE DIGITAL PERSON

**Digital identity/behavioral biometrics:** analyzes human-device interactions and behavioral patterns such as mouse clicks and keystrokes, to discern between a real user and an impostor by recognizing normal user and fraudster behavior. **Solution examples:** authentication by biometrics; email/phone risk assessment; browser/malware tracking; device ID / fingerprinting

**Device assessment:** uniquely identify a remote computing device or user. **Solution examples:** device ID/ fingerprint; geolocation



Overview



Key Findings



Attacks &amp; Costs



Trends



Challenges



Impacts

Tracking &  
Solution Usage

Strategic Approaches



Recommendations

## Key Finding #6: Strategic Approaches



6

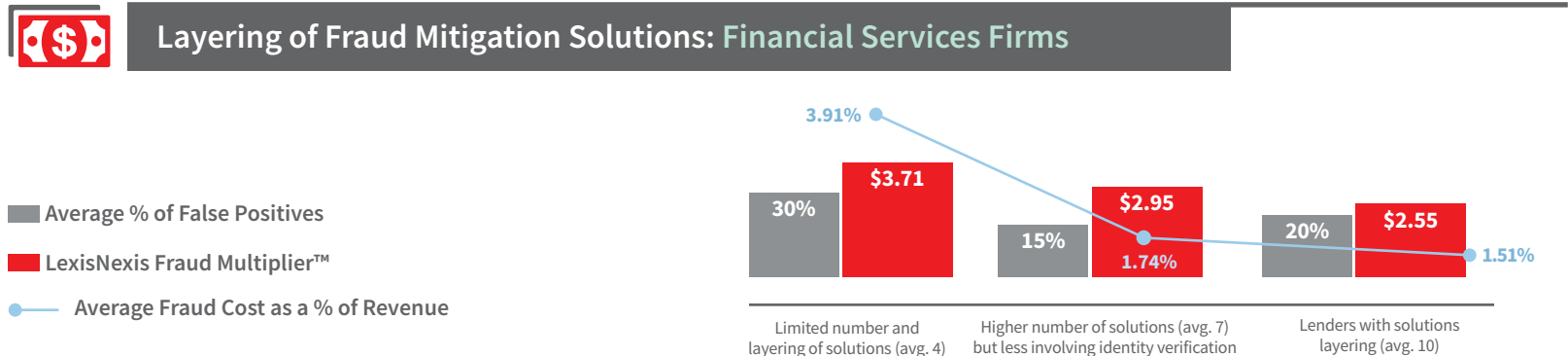
Study findings show that those financial services and lending firms which use a layered solution approach involving identity authentication and transaction verification, including digital identity / behavior biometric tools, experience a lower cost of fraud.

- Fraud is not a one-size fits all. The risks posed by the remote channels, particularly mobile, are different than those from the online or in-person environments. The ability to distinguish between a legitimate customer and a fraudster is very difficult when the criminal is using a synthetic identity with real personally identifiable information.
- Different solutions need to be applied for different channels and types of transactions. These should assess fraud for both the identity and the transaction, using physical and digital identifying information.

# Financial services firms which use a multi-layered solution approach experience fewer false positives and 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 (\$2.55 for every \$1

of fraud versus up to \$3.71) and as a percent of annual revenue. They also tend to have a lower volume of false positives.



Layers of Protection		Limited	Limited	Multi-Layered
Common Core Solutions Used Most Often	Check Verification, Authentication by Payment Instrument (CVV), Name/Address/DOB Verification, Positive/Negative Lists	Mostly	Many	✓
Layering of Advanced Identity Solutions	Authentication by Challenge Questions / Quiz, Authentication by OTP / 2-Factor, Authentications Using Biometrics, Email Risk & Verification, Phone # Risk & Verification, Browser / Malware Tracking, Geolocation, Device ID	Minimal	Minimal	✓
Layering of Fraud Transaction Risk Assessment Solutions	Automated Transaction Scoring, Real Time Transaction Tracking,	Minimal	Many	✓

## This is also found with lending 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 for every \$1

of fraud versus up to \$3.47) and as a percent of annual revenues. They also tend to have a lower volume of false positives.

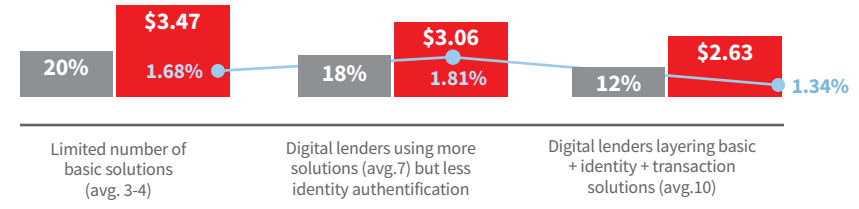


### Layering of Fraud Mitigation Solutions: Lending Firms

■ Average % of False Positives

■ LexisNexis Fraud Multiplier™

● Average Fraud Cost as a % of Revenue



Layers of Protection		Limited	Limited	Multi-Layered
Common Core Solutions Used Most Often	Check Verification, Authenticate Using Payment Instrument, Name / Address / DOB Verification, Positive & Negative Lists, Government-issued ID	Mostly	Many	✓
Layering of Advanced Identity Solutions	Authentication by Challenge Questions / Quiz, Authentication by OTP / 2-Factor, Authentications Using Biometrics, Email Risk & Verification, Phone # Risk & Verification, Browser / Malware Tracking, Geolocation, Device ID	Minimal to None	Minimal to None	✓
Layering of Fraud Transaction Risk Assessment Solutions	Automated Transaction Scoring, Real Time Transaction Tracking,	Minimal to None	Many	✓



Overview



Key Findings



Attacks &amp; Costs



Trends



Challenges



Impacts

Tracking &  
Solution Usage

Strategic Approaches



Recommendations

## Recommendation #1

Mid/Large firms which conduct significant remote channel transactions should prioritize a multi-layered risk solution approach.



The mobile channel is growing; more consumers are expecting this option, particularly younger demographics that are becoming mainstream customers. At the same time, fraudsters are professionals who continue to mutate; that means fraud will continue to increase. Left unaddressed, these digital firms will not only continue to see fraud costs take a bite out of bottom line profits, but also increase the potential for customer friction and churn.



A multi-layered solution approach is critical for both identity and transaction-related fraud detection.

Identity verification and authentication is important for “letting your customers in” with the least amount of friction.

Transaction verification is important for keeping fraudsters out.





Overview



Key Findings



Attacks &amp; Costs



Trends



Challenges



Impacts

Tracking &  
Solution Usage

Strategic Approaches



Recommendations

## Recommendation #2

Financial services and lending firms should seek external providers with deep data and analytics resources to most effectively address identity-based fraud challenges. This particularly 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 that 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.



With international transactions, 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 data on consumers and businesses.





## Recommendation #3

When seeking a layered solution approach, it is essential that digital financial services and lending firms implement solutions for unique channel issues and fraud. There is no one-size-fits-all.



As study findings have shown, there are differences between the online and mobile channels in terms of the key challenges and fraud costs.

Using the same solution to address both may not be as effective, particularly given the transient nature of mobile transactions.



And, where one tries to force a one-size-fits-all approach, particularly by using traditional onsite with remote channel transactions, there is likelihood of increasing false positives which leads to customer friction and lost current/future business.





## Recommendation #4

Digital financial services and lending firms, particularly multi-channel ones, need to remain vigilant by holistically tracking fraud by both payment and channel type – including that which has been successful and prevented.



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.



The rise of synthetic identities makes it easier for fraud via different payment methods in remote channels. This includes when using third-party apps for transaction payments.



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

- Overview
- Key Findings
- #1 Attacks & Costs
- #2 Trends
- #3 Challenges
- #4 Impacts
- #5 Tracking & Solution Usage
- #6 Strategic Approaches
- Recommendations




## Customer-Focused Solutions

- |  |  |  |  |
|--|--|--|--|
| <b>Identity Verification</b> <ul style="list-style-type: none"> <li>• Validate name, address and phone information</li> <li>• Reconcile name variations, duplicates, multiple addresses, and myriad other inconsistencies and linkages</li> <li>• Perform global identity checks with seamless integration and reporting capabilities</li> </ul> | <b>Transaction Risk Scoring</b> <ul style="list-style-type: none"> <li>• Identify risks associated with bill-to and ship-to identities with a single numeric risk score</li> <li>• Quickly detect fraud patterns and isolate high-risk transactions</li> <li>• Resolve false-positive and Address Verification Systems failures</li> </ul> | <b>Manual Research Support</b> <ul style="list-style-type: none"> <li>• Access billions of data records on consumers and businesses</li> <li>• Discover linkages between people, businesses and assets</li> <li>• Leverage specialized tools for due diligence, account management and compliance</li> </ul> | <b>Identity Authentication</b> <ul style="list-style-type: none"> <li>• Authenticate identities on the spot using knowledge-based quizzes</li> <li>• Dynamically adjust security level to suit risk scenario</li> <li>• Receive real-time pass/fail results</li> </ul> |
|--|--|--|--|

## LexisNexis® Risk Solutions can help.

For more information:

 [risk.lexisnexis.com/FIM](https://risk.lexisnexis.com/FIM)

 +1 800 953 2877  
+408 200 5755





#### About LexisNexis Risk Solutions

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX Group (LSE: REL/NYSE: RELX), a global provider of information and analytics for professional and business customers across industries. RELX is a FTSE 100 company and is based in London. For more information, please visit [www.risk.lexisnexis.com](http://www.risk.lexisnexis.com), and [www.relx.com](http://www.relx.com)

This document is for educational purposes only and does not guarantee the functionality or features of LexisNexis products identified. LexisNexis does not warrant this document is complete or error-free. LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc., used under license. LexisNexis Fraud Multiplier is a trademark of RELX Inc. True Cost of Fraud is a trademark of LexisNexis Risk Solutions Inc. Copyright © 2019 LexisNexis. NXR14106-00-1019-EN-US