The research provides a snapshot of current fraud trends in the United States and spotlights key pain points that...

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

How do I grow my business, navigate and manage the cost of fraud while strengthening customer trust and loyalty?
The study included a comprehensive survey of 1,264 risk and fraud executives during March & April 2018, broken out as follows:

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

Surveys were conducted online. LexisNexis® Risk Solutions was not identified as the sponsor of the study.

### Fraud Definitions

- Fraud is defined as the following:
  - Fraudulent and/or unauthorized transactions *for retail and online/mobile merchants*
  - Fraudulent transactions due to identity fraud, which is the misuse of stolen payments methods (such as credit cards) or personal information *for financial services companies and lenders*
  - Fraudulent requests for refund/return; bounced checks
  - Lost or stolen merchandise, as well as redistribution costs associated with redelivering purchased items
  - *This research covers consumer-facing fraud methods*
  - Does not include insider fraud or employee fraud
  - The LexisNexis Fraud Multiplier℠ cost
    - Estimates the total amount of loss a merchant occurs based on the actual dollar value of a fraudulent transaction
## Segments by Industry Definitions

<table>
<thead>
<tr>
<th>Industry</th>
<th>Mid/Large Physical Goods only</th>
<th>E-Commerce</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail</td>
<td>Ears $10 million in annual revenues; sells physical goods only.</td>
<td>Ears $10 million in annual revenues; sells physical goods only.</td>
</tr>
<tr>
<td></td>
<td><strong>Mid/Large Digital and Physical Goods</strong></td>
<td><strong>Mid/Large Digital and Physical Goods</strong></td>
</tr>
<tr>
<td></td>
<td>Ears $10 million in annual revenues; sells digital goods only, or</td>
<td>Ears $10 million in annual revenues; sells digital goods only, or</td>
</tr>
<tr>
<td></td>
<td>digital and physical goods.</td>
<td>digital and physical goods.</td>
</tr>
<tr>
<td></td>
<td><strong>Financial Services</strong></td>
<td><strong>Lending</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Mid/Large Some or No Digital Transactions</strong></td>
<td><strong>Large Some or No Digital Transactions</strong></td>
</tr>
<tr>
<td></td>
<td>Ears $10 million in annual revenues; less than 50% through the</td>
<td>Less than 50% of revenue through the online and/or mobile channels.</td>
</tr>
<tr>
<td></td>
<td>online and/or mobile channels.</td>
<td><strong>Mid/Large Primarily Digital Transactions</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Mid/Large Primarily Digital Transactions</strong></td>
<td>Ears $10 million in annual revenues; 50% or more through the online and/or</td>
</tr>
<tr>
<td></td>
<td>Ears $10 million in annual revenues; 50% or more through the online and/or mobile channels.</td>
<td>mobile channels.</td>
</tr>
<tr>
<td></td>
<td><strong>Lending</strong></td>
<td><strong>Large Primarily Digital Transactions</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Large Some or No Digital Transactions</strong></td>
<td>More than 50% of revenue through the online and/or mobile channels.</td>
</tr>
<tr>
<td></td>
<td>Ears $10 million in annual revenues; less than 50% through the</td>
<td><strong>Large Primarily Digital Transactions</strong></td>
</tr>
<tr>
<td></td>
<td>online and/or mobile channels.</td>
<td>More than 50% of revenue through the online and/or mobile channels.</td>
</tr>
</tbody>
</table>

**m-Commerce**

Allows transactions through mobile web browser, mobile apps, or bill-to-mobile phone.
Company Types by Industry

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

- Apparel
- Home Improvement
- Housewares
- Electronics
- Retail
- Books
- Computers
- Food and Beverage
- Sporting Goods
- Clothing
- Gifts
- e/m-Commerce

Financial Services Companies Include:
- Retail/Commercial Banks
- Credit Unions
- Investments
- Trusts
- Wealth Management

Lending Institutions Include:
- Auto Lenders
- Finance Companies
- Mortgage Companies
- Non-Bank Credit Card Issuer
- Non-Bank Personal Loan Issuer
Executive Summary: Key Findings
Key Findings

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

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

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

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

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

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

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

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

- Survey findings show that those who layer solutions by identity authentication and transaction/identity verification experience fewer fraud costs.
Sizeable fraud continues to occur across industries, though it has grown somewhat more for Financial Services and Lending.
The cost of fraud continues to be high across study industries, but has grown somewhat more since last year for Financial Services and Lending firms.

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

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

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

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

Additionally, the level of fraud as a percentage of revenues has increased, particularly for Financial Services firms, which are starting to feel the effects of “fast fraud” and its associated costs (as shown in next section).
And fraud consistently impacts digital, either whether it is the channel or type of good sold.
The cost of fraud is even higher for organizations that are digital – Retail and e-Commerce merchants selling digital goods or Financial Services and Lending firms conducting digital transactions.

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

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

That said, fraud still has a sizeable impact on Retail and Financial Services firms dealing with digital goods or transactions.
For Mid/Large e-Commerce merchants selling digital goods in particular, there is a relationship between fraud and continued botnet activity and usage of non-traditional payment methods.

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

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

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

Digital Products Sold – Most Mentioned

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

Transaction Methods/Fraud

- % of Method Used to Fund Transaction
- % of Fraud Cost by Transaction Method (as % of total annual fraud losses)*/**

Credit transaction
Debit transaction
Alternative transaction methods (PayPal, BillMeLater, eCheck)
Other transaction methods***

39% 32%
12% 16%
11% 16%

*CAUTION: Small sample size; use directionally, asked only of those who track fraud and then further split into size segments
** % can add to more than 100% since answers based on using a channel, in which case the base size changes per channel
D1b: What type of digital goods are sold by your company?
Q3: Please indicate the percentage for each method used (over the past 12 months) to fund transactions or disburse funds.
Q18: Please indicate the percentage distribution of the payment methods used to commit fraud against your company.

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

73% agree that combatting automated botnet fraud activity is overwhelming
86% agree that selling digital goods increases risk of fraud

***Company-branded mobile app, gift cards, virtual currency, mobile wallets, checkout by Amazon, social media payments
The mobile channel has grown for some industries and contributes to increased fraud risks.
As predicted in previous waves of this study, m-Commerce growth continues to be driven by larger firms selling digital goods or transacting digitally.

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

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

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

### % Currently Allowing & Considering m-Commerce

<table>
<thead>
<tr>
<th>% Currently Allowing &amp; Considering m-Commerce</th>
<th>Currently Allow m-Commerce</th>
<th>Considering m-Commerce</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail Overall</td>
<td>65%</td>
<td>74%</td>
</tr>
<tr>
<td>M/L Selling Physical Goods Only</td>
<td>37%</td>
<td>41%</td>
</tr>
<tr>
<td>M/L Selling Digital Goods</td>
<td>28%</td>
<td>33%</td>
</tr>
<tr>
<td>e-Commerce Overall</td>
<td>94%</td>
<td>93%</td>
</tr>
<tr>
<td>M/L Selling Physical Goods Only</td>
<td>46%</td>
<td>47%</td>
</tr>
<tr>
<td>M/L Selling Digital Goods</td>
<td>17%</td>
<td>15%</td>
</tr>
<tr>
<td>Financial Services Overall</td>
<td>63%</td>
<td>82%</td>
</tr>
<tr>
<td>M/L Selling Physical Goods Only</td>
<td>46%</td>
<td>78%</td>
</tr>
<tr>
<td>M/L Selling Digital Goods</td>
<td>17%</td>
<td>47%</td>
</tr>
<tr>
<td>Financial Services M/L Some or No Digital Trans</td>
<td>61%</td>
<td>64%</td>
</tr>
<tr>
<td>M/L Mostly Digital Trans</td>
<td>17%</td>
<td>17%</td>
</tr>
<tr>
<td>Lending Overall</td>
<td>85%</td>
<td>84%</td>
</tr>
<tr>
<td>Large Some or No Digital Trans</td>
<td>68%</td>
<td>66%</td>
</tr>
<tr>
<td>Large Mostly Digital Trans</td>
<td>67%</td>
<td>67%</td>
</tr>
<tr>
<td>Large Mostly Digital Trans</td>
<td>95%</td>
<td>100%</td>
</tr>
</tbody>
</table>

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

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

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

---

### 2018 LexisNexis Fraud Multiplier℠

<table>
<thead>
<tr>
<th>Sector</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Retail</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M/L Selling Digital Goods</td>
<td>$2.94</td>
<td>$3.13</td>
</tr>
<tr>
<td>M/L w/ m-Comm &amp; Selling Digital Goods</td>
<td>$2.65</td>
<td>$3.29</td>
</tr>
<tr>
<td><strong>e-Commerce</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M/L Selling Digital Goods</td>
<td>$3.08</td>
<td>$3.27</td>
</tr>
<tr>
<td>M/L w/ m-Comm</td>
<td></td>
<td>$3.18</td>
</tr>
<tr>
<td><strong>Financial Services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M/L Mostly Digital Trans</td>
<td>$3.04</td>
<td>$3.18</td>
</tr>
<tr>
<td>M/L w/ m-Comm &amp; Mostly Digital Trans</td>
<td>$3.04</td>
<td>$3.26</td>
</tr>
<tr>
<td><strong>Lending</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Large Mostly Digital Trans</td>
<td>$3.07</td>
<td>$3.37</td>
</tr>
<tr>
<td>Large w/ m-Comm &amp; Mostly Digital Trans</td>
<td>$3.16</td>
<td>$3.39</td>
</tr>
</tbody>
</table>

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

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

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

☐ Significantly different from 2017 within segment at the 95% Confidence Interval
Mid/Large e-Commerce merchants are being hit hard by fraud, not only through the less secure mobile web browser, but through 3rd party mobile apps as well.

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

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


64% agree the evolution of mobile payment & channel adds significant fraud risk
63% agree that security of mobile transactions still unknown

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

*CAUTION: Small sample size; use directionally, asked only of those who track fraud and then further split into size segments. ** % can add to more than 100% since answers based on using a channel, in which case the base size changes per channel
The mobile web browser is also a significant issue for Mid/Large Financial Services firms. They experience nearly half of their fraud losses through this channel.

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

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

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

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

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

Q17: Please indicate the distribution of fraud across the various mobile channels you use/accept.
So why risk offering the mobile channel as a transaction option? It optimizes the customer experience, which can lead to customer acquisition/retention and revenue growth.

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

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

**Mobile Channel Drivers**

- RETAIL – Mid/Large ($10M+) w/ m-Commerce & Selling Digital Goods
- FINANCIAL SERVICES – Mid/Large ($10M+) Digital
- E-COMMERCE – Mid/Large ($10M+) w/ m-Commerce
- LENDING – Large Digital ($50M+) Credit

**Customer experience**
- Customer convenience: 69% RETAIL, 67% MID/LARGE, 65% E-COMMERCE, 42% FINANCIAL SERVICES
- Meets customer expectations of providing more engagement: 52% RETAIL, 60% MID/LARGE, 54% E-COMMERCE, 58% FINANCIAL SERVICES
- Easier, faster customer experience: 67% RETAIL, 58% MID/LARGE, 41% E-COMMERCE, 14% FINANCIAL SERVICES

**Business health**
- Helps grow my business: 60% RETAIL, 56% MID/LARGE, 66% E-COMMERCE, 32% FINANCIAL SERVICES
- Need to remain competitive: 68% RETAIL, 62% MID/LARGE, 52% E-COMMERCE, 45% FINANCIAL SERVICES
- Helps efficient processing of applications and transactions: 52% RETAIL, 42% MID/LARGE, 41% E-COMMERCE, 55% FINANCIAL SERVICES
- Less expensive to interact with customers: 27% RETAIL, 26% MID/LARGE, 14% E-COMMERCE, 17% FINANCIAL SERVICES

Q5: What were the reasons your company decided to start accepting mobile account origination or transactions?
Adding international transactions, within the online and/or mobile channels, further increases fraud risks and costs for some.
Fraud costs are even higher for Mid/Large Financial Services firms that use m-Commerce and transact internationally -- $3.38 for $1 of fraud.

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

While the mobile web browser continues to experience the largest share of fraud, and fraud is sizeable among mobile apps, bill-to-mobile phone fraud becomes much more of a factor in international fraud (than compared to domestic).
Fraud costs jump to $3.59 for every $1 of fraud for Large Digital Lenders that transact internationally.

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

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

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

Q13: Please indicate the percent of fraud costs generated through domestic transactions compared to international transactions in the last 12 months.

Q14c: Please allocate 100 points across the following to indicate the distribution that each region represents of your total international fraud costs.

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

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

**Company-branded mobile app, gift cards, virtual currency, mobile wallets, checkout by Amazon, social media payments**
Identity fraud and verification remain key issues for firms selling digital goods or transacting digitally.
Identity and synthetic identity fraud continue to account for a significant degree of fraud losses for firms selling digital goods or transacting digitally.

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

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

Q12: Please indicate the percentage distribution of the following fraud methods as attributed to your total annual fraud loss over the past 12 months.
Not surprisingly, Mid/Large Retailers selling digital goods and using m-Commerce are challenged by minimizing customer friction while verifying identities in the US, particularly with the use of newer payment methods.

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

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

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

- **Verification of customer identity**
- **Email or device verification**
- **Emergence of new and varied payment methods**
- **Balancing speed of risk verification with customer friction**
- **Address verification**
- **Delay in payment confirmation**
- **Fraud assessment by country**
- **Lack of specialized tools for international fraud mitigation**
- **Excessive manual order reviews**

**Key Reasons for Identity Verification Challenges**

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

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

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

* Significantly different from other segment within category at the 95% Confidence Interval
Mid/Large e-Commerce merchants selling digital goods are similarly challenged by minimizing customer friction while verifying identities, particularly with the use of newer payment methods.

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

---

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

**Top Ranked Challenges, By Type of Goods**

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Mid/Large ($10M+) Selling Physical Goods Only</th>
<th>Mid/Large ($10M+) with Digital Goods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Balancing speed of risk verification with customer friction</td>
<td>49%</td>
<td>57%</td>
</tr>
<tr>
<td>Address verification</td>
<td>42%</td>
<td>64%</td>
</tr>
<tr>
<td>Verification of customer identity</td>
<td>6%</td>
<td>41%</td>
</tr>
<tr>
<td>Emergence of new and varied payment methods</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email or device verification</td>
<td>44%</td>
<td>44%</td>
</tr>
<tr>
<td>Delay in payment confirmation</td>
<td>21%</td>
<td>29%</td>
</tr>
<tr>
<td>Challenges in acceptance of int’l based transaction methods</td>
<td>31%</td>
<td>29%</td>
</tr>
<tr>
<td>Excessive manual order reviews</td>
<td>12%</td>
<td>3%</td>
</tr>
<tr>
<td>Confirmation of package delivery</td>
<td>23%</td>
<td></td>
</tr>
</tbody>
</table>

**Key Reasons for Identity Verification Challenges**

- **89%** Rise of synthetic identities
- **64%** Volume of botnet orders being placed at once
- **47%** Lack real-time tracking/velocity solutions

---

Q19a: Please rank the top 3 challenges related to fraud faced by your company when selling physical goods . . . when selling digital goods.

Q19a/b:2: Please rank the top 3 factors that make customer identity verification a challenge when selling digital goods inside/ outside the US.
And identity verification remains the top challenge for Mid/Large Financial Services firms when transacting online and has grown since 2017 as a mobile channel challenge.

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

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

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

**Top Ranked Fraud Challenges, By Channel**

- **Online Channel**
  - Verification of customer identity: 57%
  - Emergence of new and varied payment methods: 46%
  - Delay in transaction confirmation: 44%
  - Excessive manual order reviews: 29%
  - Email or device verification: 29%
  - Lack of specialized tools for int’l transactions: 27%
  - Address verification: 22%
  - Assessment of fraud risk by country/region: 15%
  - Challenges in acceptance of int’l based transaction methods: 13%
  - Balancing speed of risk verification with customer friction: 13%

- **Mobile Channel**
  - Verification of customer identity: 39%
  - Emergence of new and varied payment methods: 36%
  - Delay in transaction confirmation: 30%
  - Excessive manual order reviews: 24%
  - Email or device verification: 19%
  - Lack of specialized tools for int’l transactions: 21%
  - Address verification: 18%
  - Assessment of fraud risk by country/region: 22%
  - Challenges in acceptance of int’l based transaction methods: 16%
  - Balancing speed of risk verification with customer friction: 8%

Q20: Please rank the top 3 challenges related to fraud faced by your company when serving customers in the Online/Mobile Channel. Significantly different than 2017 within Segment
For Large Digital Lenders, identity verification remains a top challenge when conducting mobile transactions and has actually grown since last year as an issue for the online channel.

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

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

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

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

Significantly different than 2017 within Segment
Tracking of fraud has increased, but for those hit harder by fraud, it still isn’t optimal.
Segments with the highest fraud costs, to a large degree, track fraud costs by both channel and payment/transaction method.

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

That said, these segments – Mid/Large Retailers selling digital goods and using m-Commerce, Mid/Large e-Commerce merchants using m-Commerce, Mid/Large Financial Services transacting internationally and using m-Commerce, and Large Digital Creditors – have high fraud costs nonetheless.
That said, these harder hit segments are more likely to be tracking where fraud has been successful rather than also tracking where they’ve been able to prevent it.

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

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

**% Tracking SUCCESSFUL Fraud Transaction By Channel & Payment Method**

<table>
<thead>
<tr>
<th>Segment</th>
<th>By Channel</th>
<th>By Payment Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M/L Selling Digital Goods</td>
<td>63%</td>
<td>54%</td>
</tr>
<tr>
<td>M/L w/ m-Comm &amp; Selling Digital Goods</td>
<td>71%</td>
<td>66%</td>
</tr>
<tr>
<td>e-Commerce</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M/L Selling Digital Goods</td>
<td>65%</td>
<td>50%</td>
</tr>
<tr>
<td>M/L w/ m-Comm</td>
<td>84%</td>
<td>52%</td>
</tr>
<tr>
<td>Financial Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M/L Mostly Digital Trans</td>
<td>56%</td>
<td>51%</td>
</tr>
<tr>
<td>M/L w/ m-Comm &amp; International</td>
<td>70%</td>
<td>42%</td>
</tr>
<tr>
<td>Lending</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Large Mostly Digital Trans</td>
<td>80%</td>
<td>81%</td>
</tr>
<tr>
<td>Large Digital Credit</td>
<td>83%</td>
<td>76%</td>
</tr>
</tbody>
</table>

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

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

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

33
And combined fraud solution and automated alert system usage remains high or has increased among these at risk segments.

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

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

- **Retail**
  - M/L Selling Digital Goods: 2017 61%, 2018 87%
  - M/L w/ m-Comm & Selling Digital Goods: 2017 45%, 2018 76%

- **e-Commerce**
  - M/L Selling Digital Goods: 2017 86%, 2018 81%
  - M/L w/ m-Comm: 2017 **, **%

- **Financial Services**
  - M/L Mostly Digital Trans: 2017 29%, 2018 87%
  - M/L w/ m-Comm & International: 2017 76%, 2018 76%

- **Lending**
  - Large Mostly Digital Trans: 2017 66%, 2018 92%
  - Large Digital Credit: 2017 76%, 2018 90%

**Q35:** Does your company use an automated system to flag potentially fraudulent transactions?

**Q35b:** Does your company use an electronic service that alerts you when a TC-40/chargeback claim has been filed based on one of your transactions?

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

- Significantly different from other segment within industry category at the 95% Confidence Interval
- Significantly different from 2017 within segment at the 95% Confidence Interval

*LexisNexis RISK SOLUTIONS*
But this doesn’t seem to improve the accuracy or efficiency of the fraud identification process.

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


<table>
<thead>
<tr>
<th>Segment</th>
<th>% Flagged</th>
<th>% Sent</th>
<th>% False</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M/L Selling Digital Goods</td>
<td>56%</td>
<td>46%</td>
<td>25%</td>
</tr>
<tr>
<td>M/L w/ m-Comm &amp; Selling Digital Goods</td>
<td>52%</td>
<td>43%</td>
<td>24%</td>
</tr>
<tr>
<td>e-Commerce</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M/L Selling Digital Goods</td>
<td>63%</td>
<td>57%</td>
<td>22%</td>
</tr>
<tr>
<td>M/L w/ M-Comm</td>
<td>50%</td>
<td>45%</td>
<td>20%</td>
</tr>
<tr>
<td>Financial Services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M/L Mostly Digital Trans</td>
<td>67%</td>
<td>39%</td>
<td>21%</td>
</tr>
<tr>
<td>M/L w/ m-Comm &amp; International</td>
<td>60%</td>
<td>38%</td>
<td>21%</td>
</tr>
<tr>
<td>Lending</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Large Mostly Digital Trans</td>
<td>66%</td>
<td>33%</td>
<td>13%</td>
</tr>
<tr>
<td>Large Digital Credit</td>
<td>64%</td>
<td>35%</td>
<td>13%</td>
</tr>
</tbody>
</table>

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

Q36: Of all the transactions your company flagged as potentially fraudulent in the past 12 months, what percentage was flagged by your auto system?
Q37: Of this (…), what proportion are sent for manual review?
Q39: What percentage of declined transactions turned out to be false positives?
A number of higher risk firms are using fraud prevention solutions, but not necessarily the right combination to successfully prevent fraud.
The average number of reported solutions used has increased or is on par with 2017 for segments hit hardest by fraud.

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

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

**Average Number of Fraud Mitigation Solutions Currently Used**

<table>
<thead>
<tr>
<th>Segment</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>M/L Selling Digital Goods</td>
<td>4.9</td>
<td>7.8</td>
</tr>
<tr>
<td>M/L w/ m-Comm &amp; Selling Digital Goods</td>
<td>4.7</td>
<td>7.8</td>
</tr>
<tr>
<td>M/L Selling Digital Goods</td>
<td>7.0</td>
<td>8.2</td>
</tr>
<tr>
<td>M/L w/ m-Comm</td>
<td>6.3</td>
<td>6.6</td>
</tr>
<tr>
<td>M/L Mostly Digital Trans</td>
<td>3.8</td>
<td>5.8</td>
</tr>
<tr>
<td>M/L w/ m-Comm &amp; International</td>
<td>7.3</td>
<td>6.3</td>
</tr>
<tr>
<td>Large Mostly Digital Trans</td>
<td>6.8</td>
<td>6.4</td>
</tr>
<tr>
<td>Large Digital Credit</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

Significantly different from 2017 within segment at the 95% Confidence Interval.
But while solutions continue to be the major component of fraud mitigation spend for these segments, a sizeable portion is still budgeted for manual reviews. This is the case regardless of sector.

Distribution of Fraud Mitigation Costs by Percent of Spend

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

** Incidence too low for Mid/Large m-Commerce in 2017; base size too small to show comparison findings.
Harder-hit Retailers might not be fully optimizing the use of risk mitigation solutions, even though they use more of them than others.

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

Also, an increase in some solutions/services, such as check verification and PIN/signature authentication, reminds us that these merchants are using multiple channels – and may be trying to use the same types of solutions in different channels that present different types of risks.
There is also only marginally directional growth with reported use of some solutions among Mid/Large e-Commerce selling digital goods and those using m-Commerce.

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

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

<table>
<thead>
<tr>
<th>E-COMMERCE – Fraud Mitigation Solutions Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>M/L Selling Digital Goods</td>
</tr>
<tr>
<td>M/L w/ m-Comm</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Basic Verification &amp; Transaction Solutions</th>
<th>Advanced Identity Authentication Solutions</th>
<th>Advanced Identity &amp; Transaction Verification Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Verification</td>
<td>Authenticate by Quiz/Knowledge</td>
<td>Identity Verification Services</td>
</tr>
<tr>
<td>51%</td>
<td>52%</td>
<td>67%</td>
</tr>
<tr>
<td>20%</td>
<td>38%</td>
<td>58%</td>
</tr>
<tr>
<td>44%</td>
<td>45%</td>
<td>58%</td>
</tr>
<tr>
<td>35%</td>
<td>41%</td>
<td>45%</td>
</tr>
<tr>
<td>53%</td>
<td>46%</td>
<td>41%</td>
</tr>
<tr>
<td>55%</td>
<td>65%</td>
<td>31%</td>
</tr>
<tr>
<td>44%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address Verification</td>
<td>Authenticate by Challenge Questions/Secure Tools/Shared Secrets</td>
<td>Rules-based Filters</td>
</tr>
<tr>
<td>58%</td>
<td>54%</td>
<td>55%</td>
</tr>
<tr>
<td>55%</td>
<td>58%</td>
<td>54%</td>
</tr>
<tr>
<td>53%</td>
<td>46%</td>
<td>41%</td>
</tr>
<tr>
<td>60%</td>
<td>65%</td>
<td>45%</td>
</tr>
<tr>
<td>59%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIN/Sig Authentica</td>
<td>Customer Profile Databases</td>
<td>Automated Transaction Scoring</td>
</tr>
<tr>
<td>44%</td>
<td>58%</td>
<td>49%</td>
</tr>
<tr>
<td>44%</td>
<td>46%</td>
<td>41%</td>
</tr>
<tr>
<td>CVV</td>
<td>45%</td>
<td>41%</td>
</tr>
<tr>
<td></td>
<td>45%</td>
<td>41%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

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

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

FINANCIAL SERVICES – Fraud Mitigation Solutions Use

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

Q27: Which of the following best describes your awareness and use of the fraud solutions listed?
While a good share of Large Digital Lenders, particularly Large Digital Creditors, report using authentication by 3-D secure tools and customer profile databases, the use of other advanced identity authentication solutions remains somewhat limited.

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

**LENDING – Fraud Mitigation Solutions Use**

<table>
<thead>
<tr>
<th>Basic Verification &amp; Transaction Solutions</th>
<th>Advanced Identity Authentication Solutions</th>
<th>Advanced Identity &amp; Transaction Verification Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Verification</td>
<td>Authenticate by Quiz/Knowledge</td>
<td>Identity Verification Services</td>
</tr>
<tr>
<td>Browser/Malware Tracking</td>
<td>Authenticate by Challenge Questions/Shared Secrets</td>
<td>Rules-based Filters</td>
</tr>
<tr>
<td>Address Verification Services</td>
<td>Authenticate 3-D Secure Tools</td>
<td>Automated Transaction Scoring</td>
</tr>
<tr>
<td></td>
<td>Customer Profile Databases</td>
<td>Real-time Transaction Tracking</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Year</th>
<th>M/L Digital</th>
<th>Large Digital Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td><strong>49%</strong></td>
<td><strong>42%</strong></td>
</tr>
</tbody>
</table>

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

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

- Significantly different from other segments within category at the 95% Confidence Interval
- Significantly different than 2017 within Segment
Findings show that using the right combination of tools is crucial to combatting fraud risks and cost.
Firms that use a multi-layered solution approach experience a lower cost of fraud.

Survey findings show that those who layer core + advanced identity authentication + advanced transaction/identity verification solutions have lower fraud costs than others per fraud event ($2.63 - $2.76 for every $1 of fraud versus $3.47 - $3.71) and as a percent of annual revenues.
Recommendations
It is critical for firms to address both identity and transaction-related fraud. These are two different perspectives.

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

Transaction-related fraud is about keeping the “bad guys out”.

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

A layered approach can reduce costs associated with manual reviews, successful fraud attempts and fewer false positives.
Recommendation #2

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

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

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

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

Recommendation #3

A multi-layered solution approach is particularly essential for mid/larger firms selling digital goods and/or transacting via the mobile channel in order to fight fraud generated by botnets and synthetic identities.
Identity fraud can be complicated, with various layers of masks and connections in the background. Investing in a layered solution approach will be much more effective if from a solutions partner that provides unique linking capabilities which identify and match hidden relationships, shed light on suspicious activities or transactions and identify collusion. These patterns are not easily uncovered by a number of risk solutions on the market today.

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

Recommendation #4

Firms should seek external providers with deep data and analytics resources to most effectively address identity-based fraud challenges. This in particular includes those conducting international transactions.
Recommendation #5

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

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

That said, the rise of synthetic identities makes it easier for fraud to go undetected. Without the aid of risk mitigation solutions designed to identify fraudulent identity characteristics, tracking approaches will miss certain clues; this will weaken tracking efforts.
LexisNexis® Risk Solutions can help
LexisNexis® Risk Solutions provides powerful identity verification, identity authentication and transaction scoring tools to combat fraud.

LexisNexis® Risk Solutions:

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

**Customer-Focused Solutions**

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

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

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

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

For more information: visit [http://risk.lexisnexis.com](http://risk.lexisnexis.com) or call 800.869.0751