Fighting Fraud in the e-Commerce Channel: A Merchant Study

June 2018

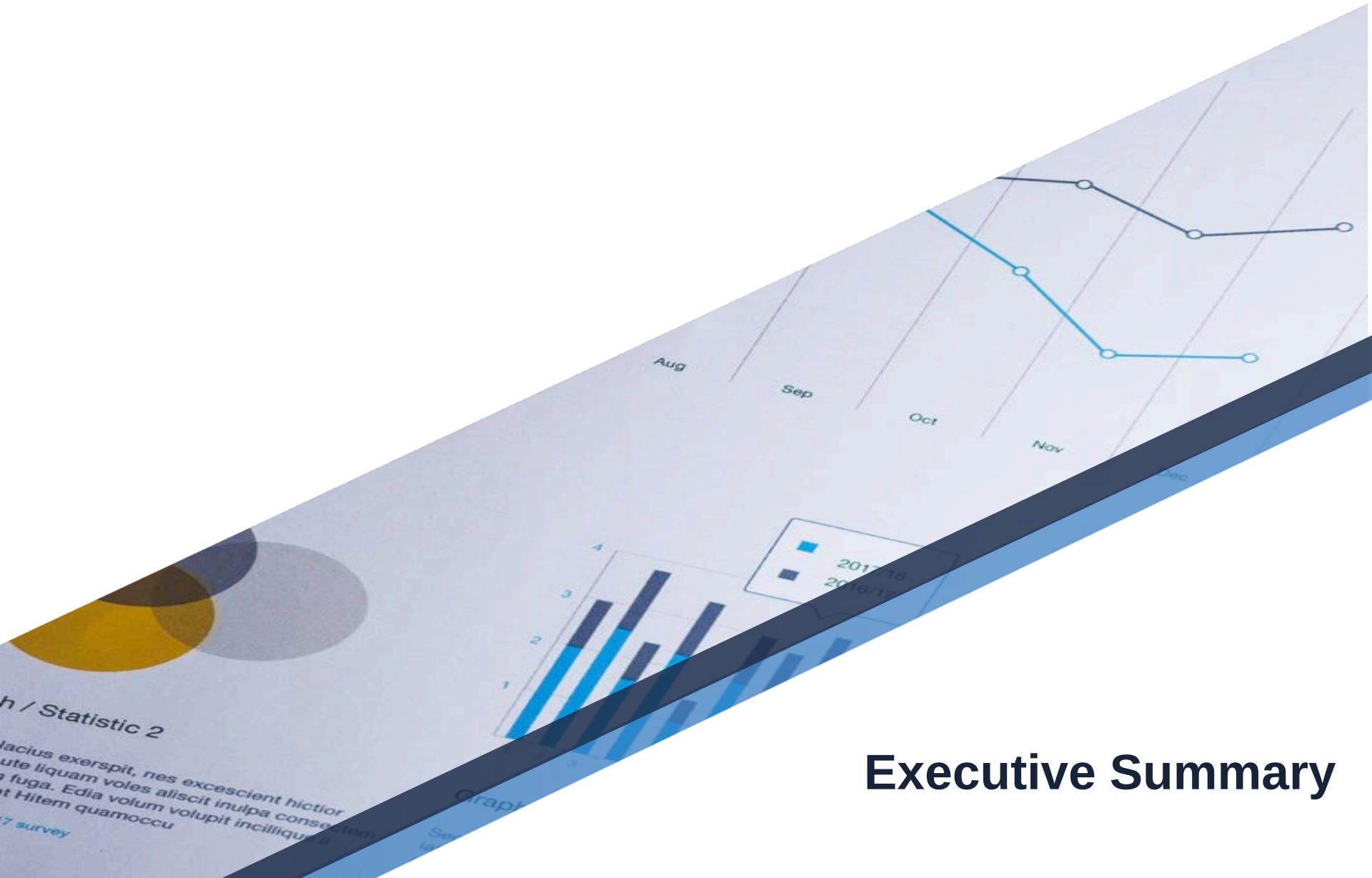
FEDERAL RESERVE BANK *of* MINNEAPOLIS

Contents

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Research Topics Covered

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.



Executive Summary

Methodology Recap

This report presents findings from an online survey of 166 U.S. retailers with an e-commerce presence. The sample was drawn from the largest 12,500 retailers with $25M or more in annual sales. Data collection occurred from December 2017 to March 2018 by Phoenix Marketing International.

Annual sales size segments represented include:

- $1.5B+
- $400M - <$1.5B
- $100M - $399M
- <$100M

This merchant study complements the financial institution fraud mitigation tool effectiveness study published by the Federal Reserve Bank of Minneapolis in Q1 2018.

Executive Summary

1 **Merchants say card-not-present (CNP) fraud is their #1 fraud threat**

- Survey respondents overall and those in the largest and smallest segments view CNP fraud as their greatest fraud problem
- Overall #2 fraud problem: in-person card fraud at the point of sale

2 **Nearly half of all retailers (including two-thirds of the largest segment) worry about their systems' abilities to handle increased e-commerce fraud as a result of data breaches**

- More than three-quarters of retailers expect e-commerce fraud attacks to climb in next 6 to 12 months

3 **Top three drivers of e-commerce fraud attacks are:**

- **Data breaches**
- **Growth in e-commerce**
- **Targeted attacks**

4 **No single fraud tool was used by more than 76% of respondents, which suggests high fragmentation**

5 **The most used fraud mitigation tools in the e-commerce channel are security code and shipping address verification**

- Retailers continue to rely on older mitigation techniques while exploring newer emerging solutions

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Executive Summary, continued

Study Objectives

Seek input from merchants on:

1. Types of fraud that pose the greatest risk
2. Approaches, tools and techniques that effectively mitigate fraud threats in the e-commerce/online sales channel
3. Merchant participation in industry fraud mitigation partnerships and the effectiveness of those efforts

6 **Fraud mitigation tools the largest retailers (annual sales $1.5B+) find <u>most effective</u> are:**

- **Out of band authentication using one time password sent to mobile device, email, text message or phone call**
- **Enhanced cardholder verification at registration/ enrollment for a new card on file account**
- **Customized proprietary fraud models**
- **Purchase velocity checks**

7 **The top three fraud mitigation tools that retailers plan to adopt in the next 6 to 12 months are:**

- **3D Secure, Verified by Visa or similar systems**
- **Purchase velocity checks**
- **Geolocation to identify anomalous transactions**

8 **Although usage of emerging fraud mitigation technologies is low, confidence is high among users of artificial intelligence systems, facial recognition and voice recognition**

- Large retailers who use behavioral biometrics rate it high in effectiveness

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Executive Summary, continued

2017 U.S. Retail Sales
Total sales from the nearly 3.8 million retail establishments in the U.S. were $3.5 trillion in 2017. E-commerce or online channel sales were $453 billion, accounting for about 13% of total retail sales.
U.S. Department of Commerce

9 **When asked to rank six fraud areas in terms of corporate resources (dollars and labor) devoted to countering or mitigating each fraud type, *card-not-present fraud in the online shopping channel* was ranked #1 overall and #1 by the two smallest segments**

- The two largest segments selected *in-person card at the point of sale* as #1

10 **Over half of retailers rely on processing systems from third parties to fight e-commerce fraud**

11 **About four in ten retailers analyze and adjust fraud rules in real time based on changing conditions**

- An additional one-third make adjustments at least weekly

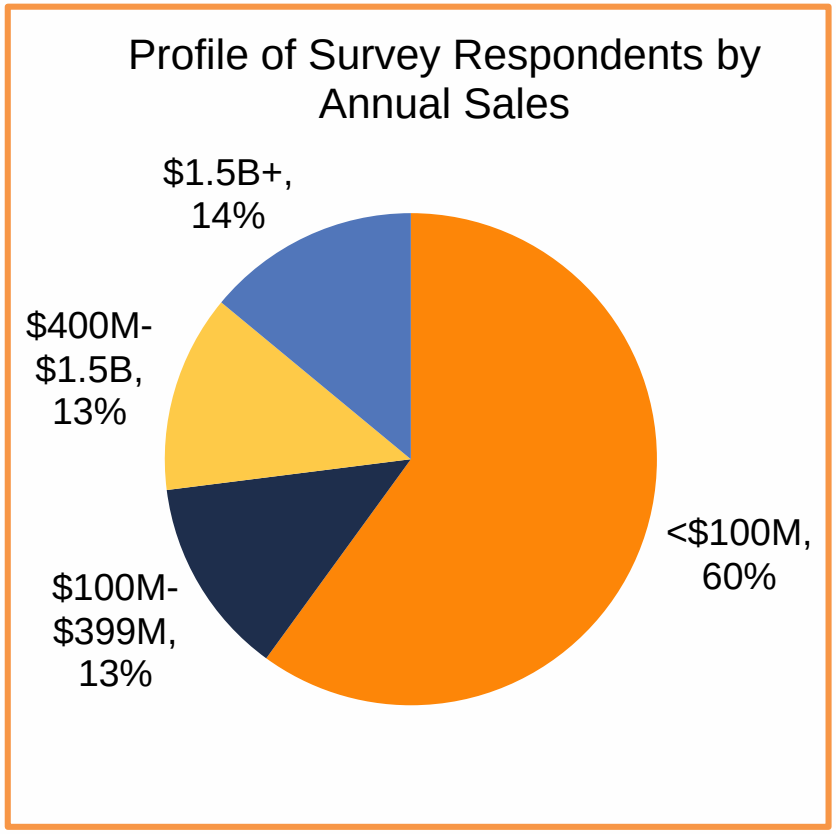
12 **Only about one-third of retailers participate in an information sharing partnership to identify current fraud attacks and exchange threat information**

- Overall, partnerships with payment card networks and third party processors have the greatest participation
- Over half of the largest retailers (annual sales of $1.5B+) participate in one or more information sharing partnerships
- The Financial Services Information Sharing and Analysis Center (FS-ISAC) is top-rated in effectiveness, although several partnerships received high marks

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Fighting Fraud in the e-Commerce Channel 2018

Survey respondents are U.S. retailers with an e-commerce presence.



Comparison of Survey Sample Annual Sales versus U.S. Retail Industry

Survey Respondents			All U.S. Retailers Based on data obtained from Phoenix Marketing International		
Annual sales size	Percent %	Count #	Annual sales size	Percent %	Count #
$1.5B+	14.5%	24	$1.5B+	5.4%	675
$400M-$1.5B	12.7%	21	$400M-$1.5B	5.6%	695
$100M-$399M	13.3%	22	$100M-$399M	13.7%	1,589
<$100M	59.6%	99	<$100M	76.3%	9,550
TOTALS	*100%	166	TOTALS	*100.0%	12,509

*Totals exceed 100% due to rounding.

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Section I:

Identifying Threats

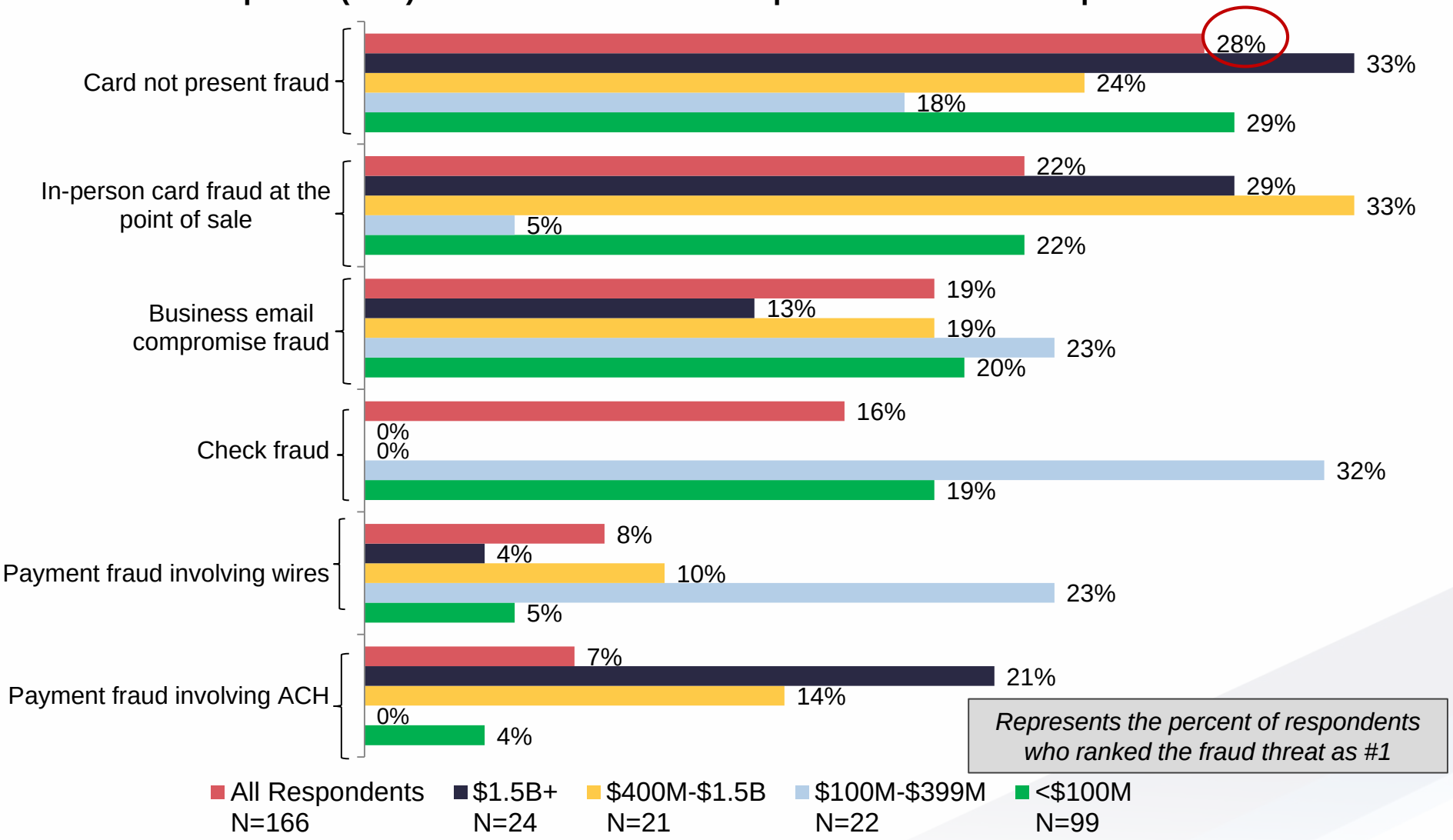
Card-not-present fraud in the online shopping channel **is ranked as the #1 fraud threat by retailers overall and by two of the segments.**

Ranking of Top Fraud Threats	All Respondents N=166	$1.5B+ N=24	$400M-$1.5B N=21	$100M-$399M N=22	<$100M N=99
Card-not-present fraud in the online shopping channel	#1	#1	#2	#4	#1
In-person card fraud at the point of sale	#2	#2	#1	#5	#2
Business email compromise fraud perpetrated through social engineering attacks	#3	#4	#3	#3	#3
Check fraud	#4	#6	#6	#1	#4
Payment fraud involving wires	#5	#5	#5	#2	#5
Payment fraud involving ACH	#6	#3	#4	#6	#6

Q1. Please rank the following fraud areas from 1 to 6 in terms of how much of a threat you believe they are to your organization, where 1 means "Highest threat" and 6 means "Lowest threat".

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Over one-quarter (28%) of retailers view card-not-present fraud as the top threat.



Q1. Please rank the following fraud areas from 1 to 6 in terms of how much of a threat you believe they are to your organization, where 1 means "Highest threat" and 6 means "Lowest threat".

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

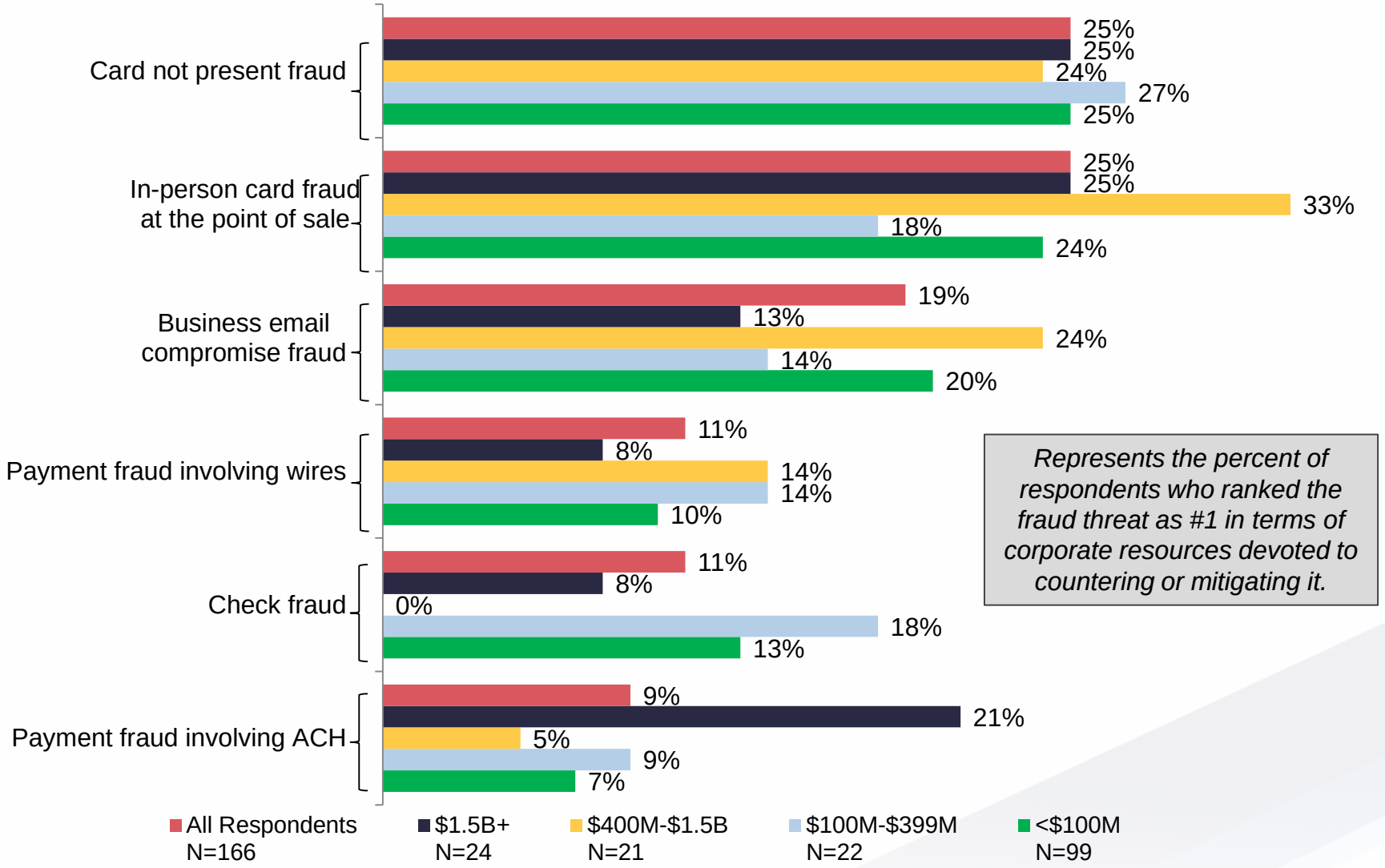
When asked to rank six fraud areas in terms of corporate resources (dollars and labor) devoted to countering or mitigating each fraud type, *card-not-present fraud in the online shopping channel* was ranked #1 overall and #1 by the two smallest segments. The two largest segments selected *in-person card at the point of sale* as #1.

Ranking of Corporate Resources Directed to Fighting Fraud Threats	All Respondents N=166	$1.5B+ N=24	$400M-$1.5B N=21	$100M-$399M N=22	<$100M N=99
Card-not-present fraud in the online shopping channel	#1	#2	#2	#1	#1
In-person card fraud at the point of sale	#2	#1	#1	#2	#2
Business email compromise fraud perpetrated through social engineering attacks	#3	#4	#3	#5	#3
Check fraud	#4	#6	#6	#3	#4
Payment fraud involving wires	#5	#5	#4	#4	#6
Payment fraud involving ACH	#6	#3	#5	#6	#5

Q1A. Now rank those same six areas in terms of corporate resources (dollars and labor) devoted to countering or mitigating those types of fraud. (Enter a number from 1 to 6 for each item below, in which 1 receives the most resources and 6 the least.)

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

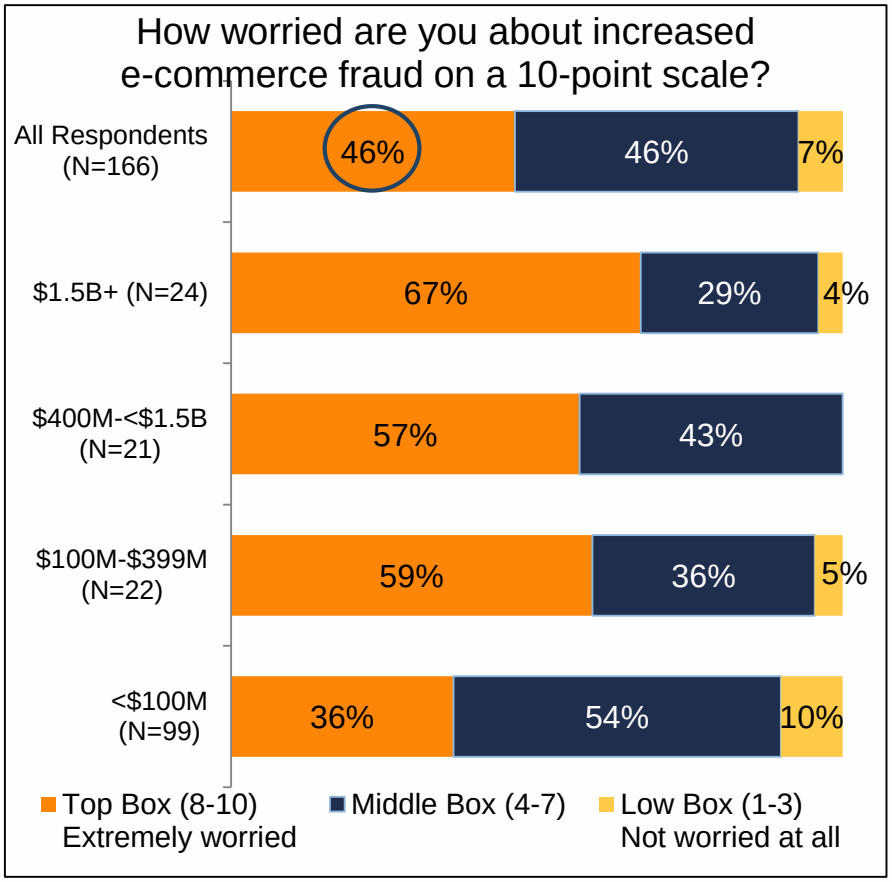
The most corporate fraud fighting resources are devoted to fighting CNP and POS card fraud.



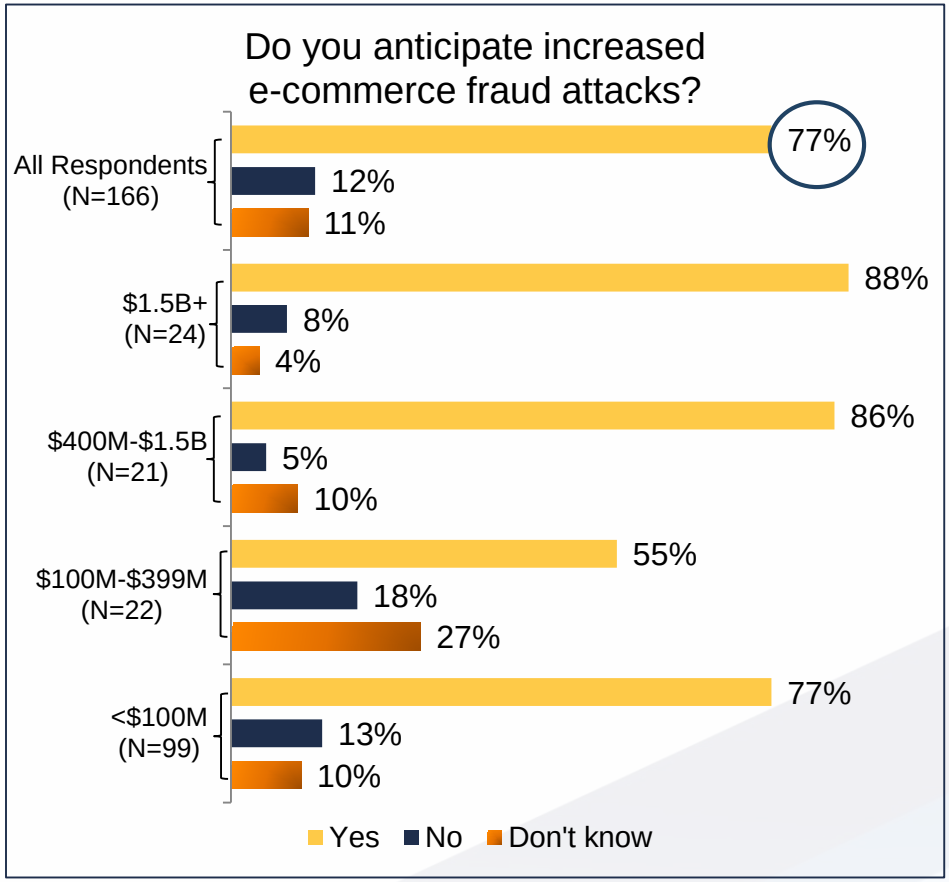
Q1A. Now rank those same six areas in terms of corporate resources (dollars and labor) devoted to countering or mitigating those types of fraud. (Enter a number from 1 to 6 for each item below, in which 1 receives the most resources and 6 the least.)

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Nearly half (46%) of all retailers express high levels of concern with increased e-commerce fraud as a result of data breaches. More than three-quarters (77%) anticipate increased incidents of e-commerce fraud in the next 6 – 12 months.



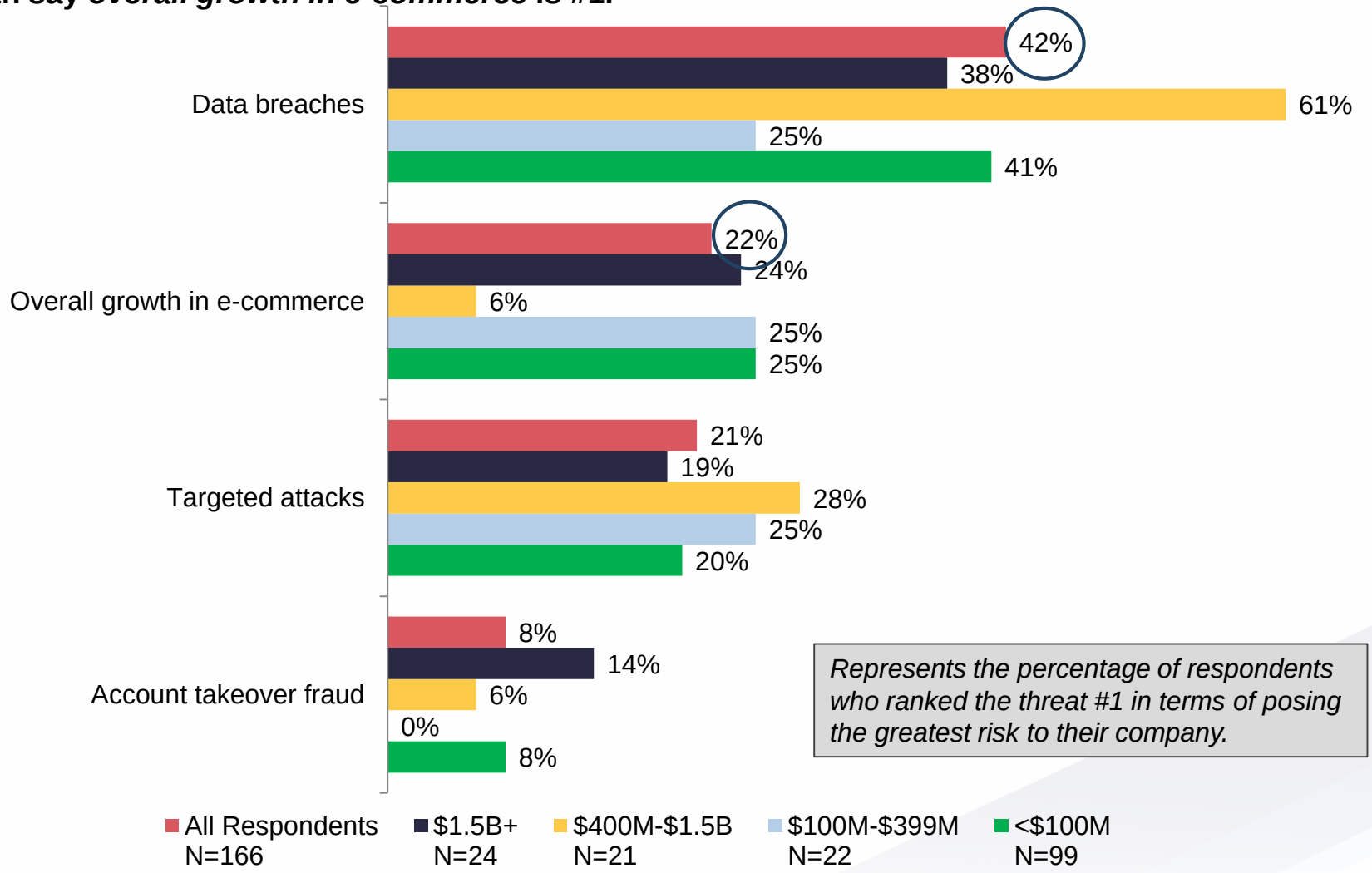
Q2A. Thinking specifically about your company's systems and processes, how worried are you about increased fraud in the e-commerce channel as a result of ongoing data breaches, where 1 means "Not worried at all" and 10 means "Extremely worried?"



Q2B. Do you anticipate e-commerce fraud attacks will increase in the next 6-12 months?

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Overall 42% rank *data breaches* first as the greatest risk to their companies, while about one-fifth say *overall growth in e-commerce* is #1.

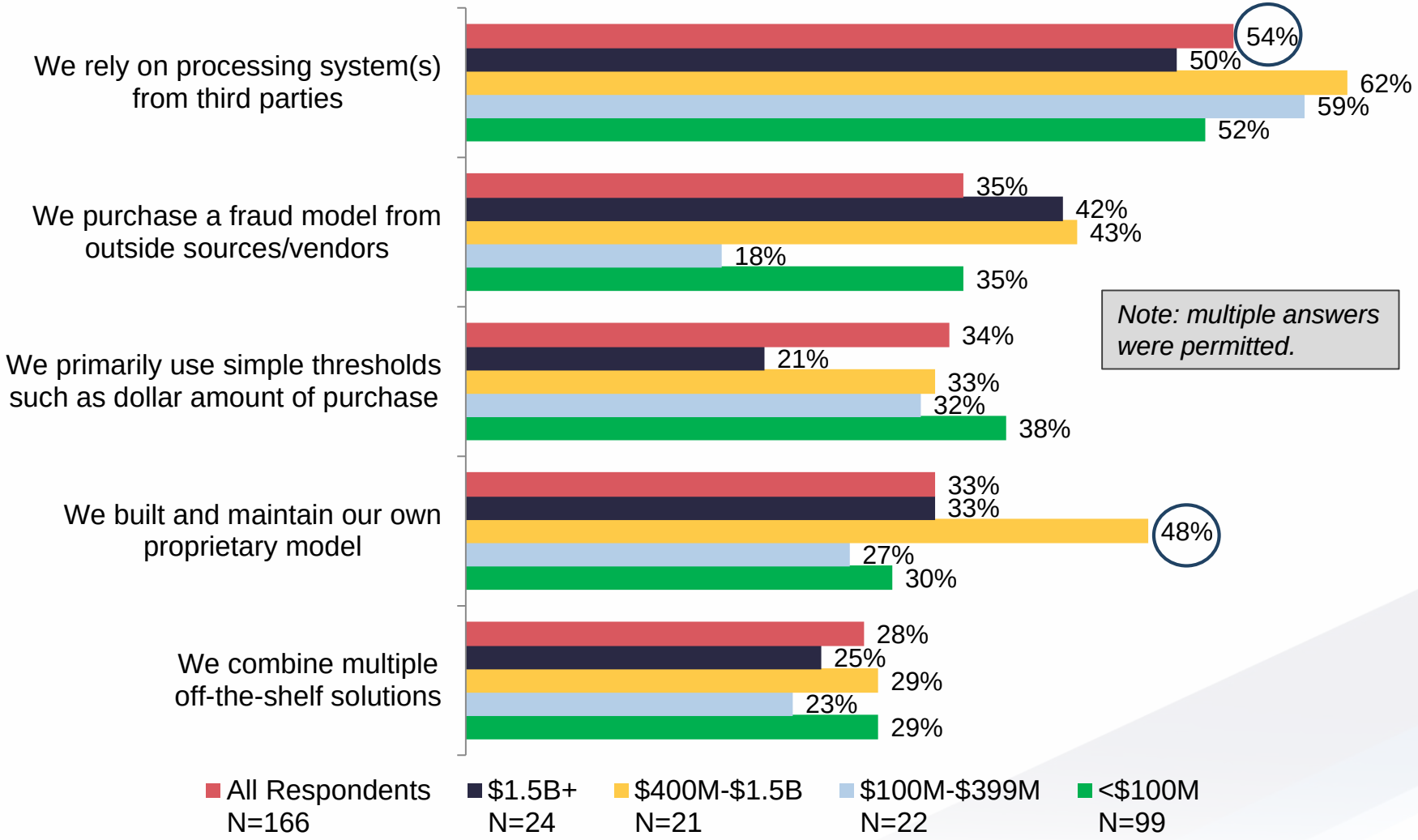


Represents the percentage of respondents who ranked the threat #1 in terms of posing the greatest risk to their company.

Q2B2. Please rank the Top 3 factors to show which ones are posing the greatest risk to your company.

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Half or more of retailers of all sizes rely on processing systems from third parties to fight e-commerce fraud. Note that almost half (48%) of the second largest tier retailers surveyed ($400M - $15.B) rely on their own proprietary model.



Q2C. How would you describe your organization's approach to fighting e-commerce fraud? Check as many as apply.

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Additional Fraud Threats Specifically Mentioned

Merchants continue to deal with a variety of threats from high tech, like Bots and Phishing attacks, to medium tech such as upgraded card skimmers, to pervasive legacy threats like counterfeiting and check scams.

"An uptick in skimmers used by holders of our fuel cards …" ($1.5B+)

"Payroll checks are deposited remotely…and cashed" ($1.5B+)

"Marked increase in chargebacks…from stolen cards" ($400M-$1.5B+)

"…Bots with changing behaviors" ($400M-$1.5B)

Multiple mentions of various card fraud ($100M-$399M)

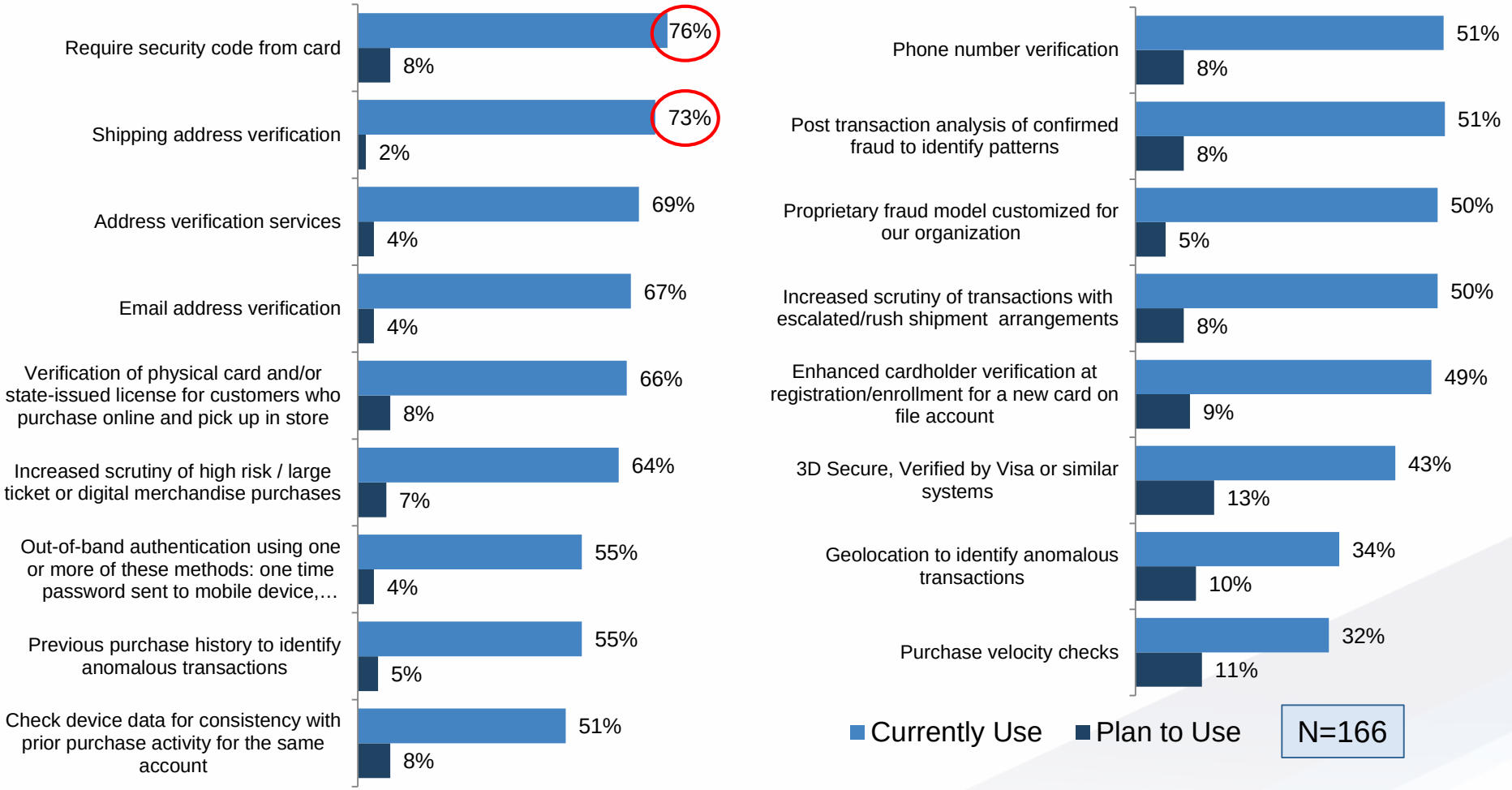
"Phishing that is harder to distinguish…" ($<100M)

Q9. Have you identified any additional fraud threats that you are starting to see?

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Section II:
Fraud Mitigation Tools

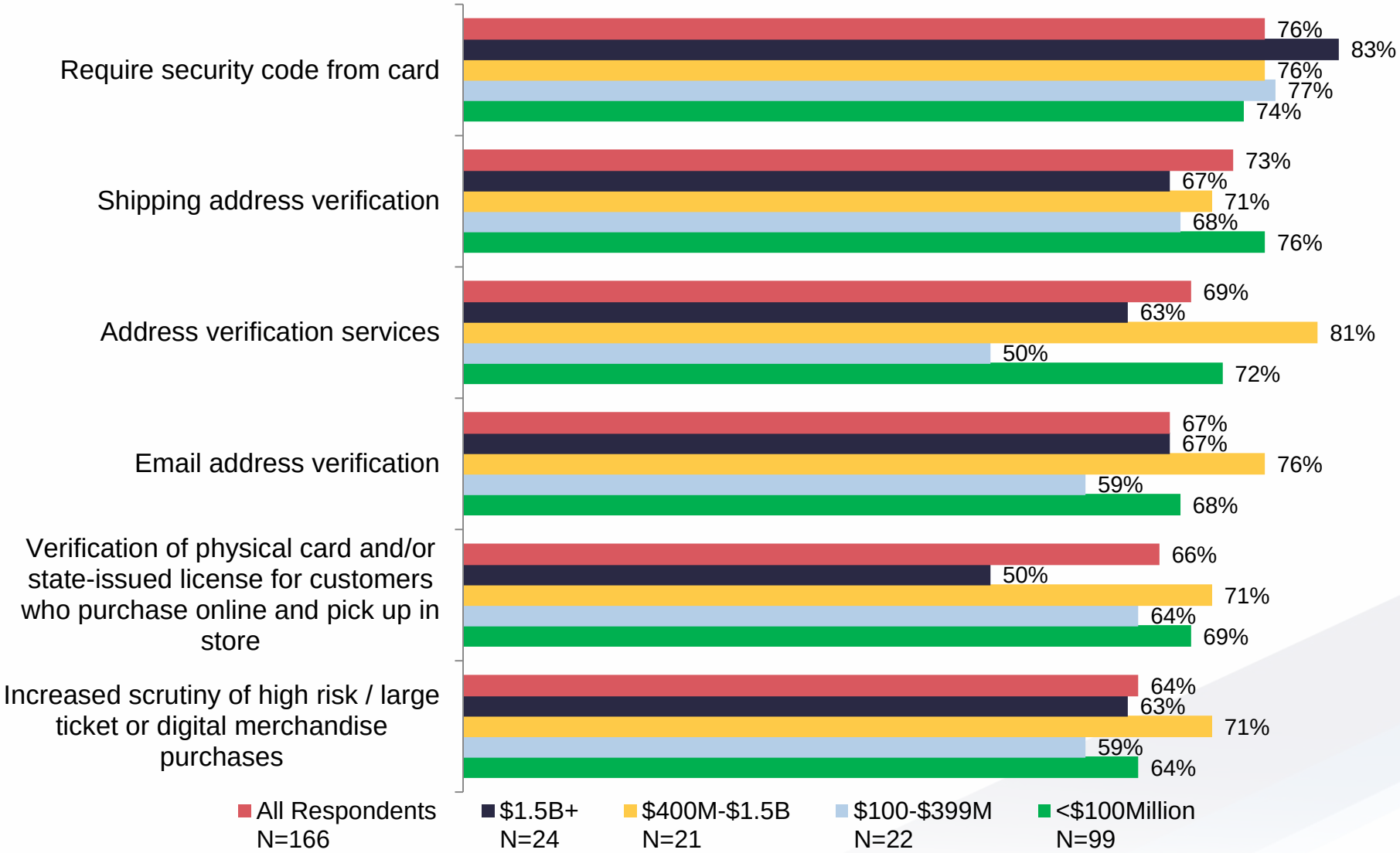
The most commonly used fraud mitigation tool in the e-commerce channel is *requiring the security code from card* (76%), while *shipping address verification* is a close second at 73%.



Q3A. Which of the following fraud mitigation tools/techniques does your organization currently use in the e-commerce sales channel?
3C. [If not using] Which of these do you plan to use in the next 6 to 12 months?

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

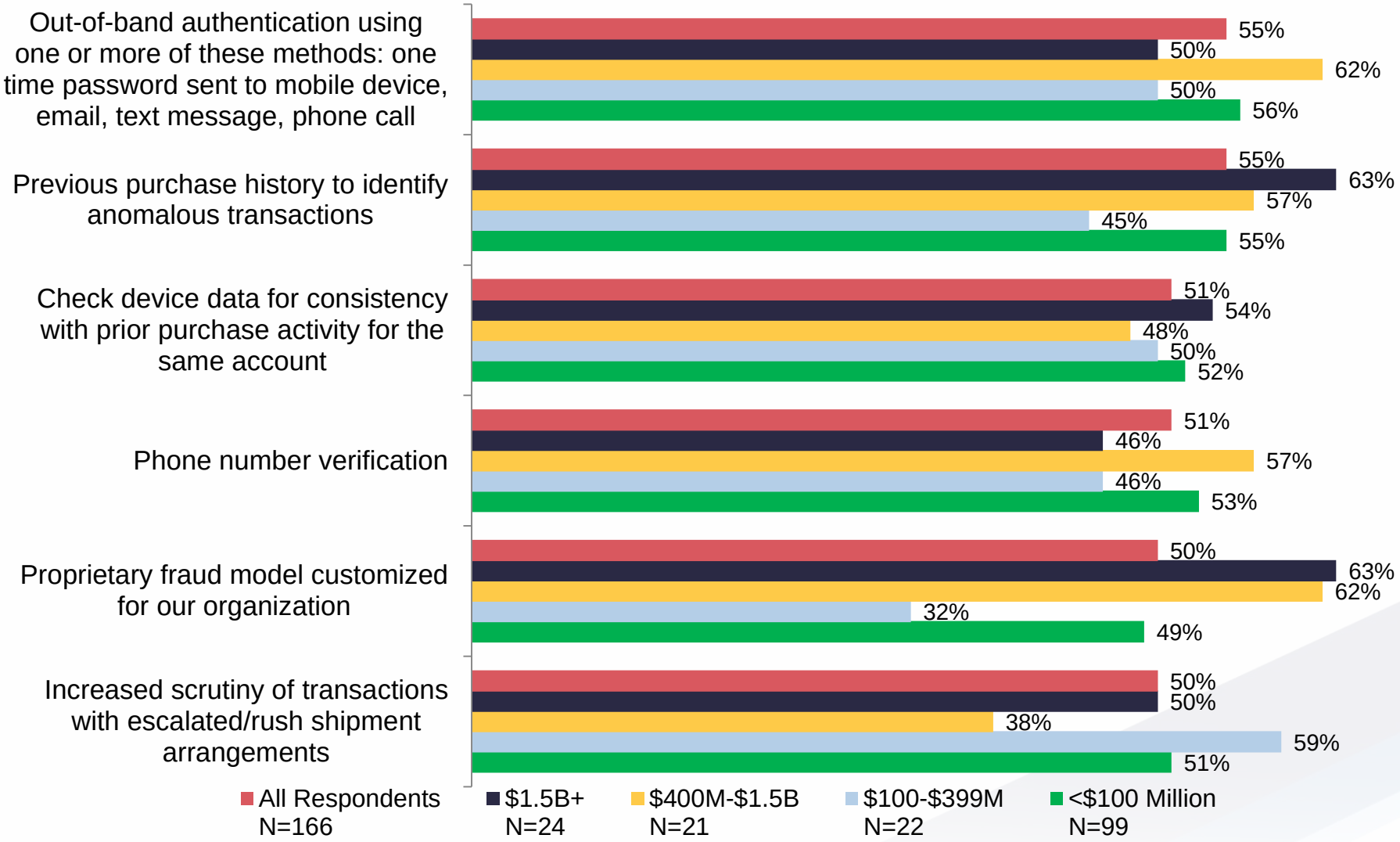
Usage by Segment Sizes of Current Fraud Mitigation Tools: slide 1 of 3



Q3A. Which of the following fraud mitigation tools/techniques does your organization currently use in the e-commerce sales channel?

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

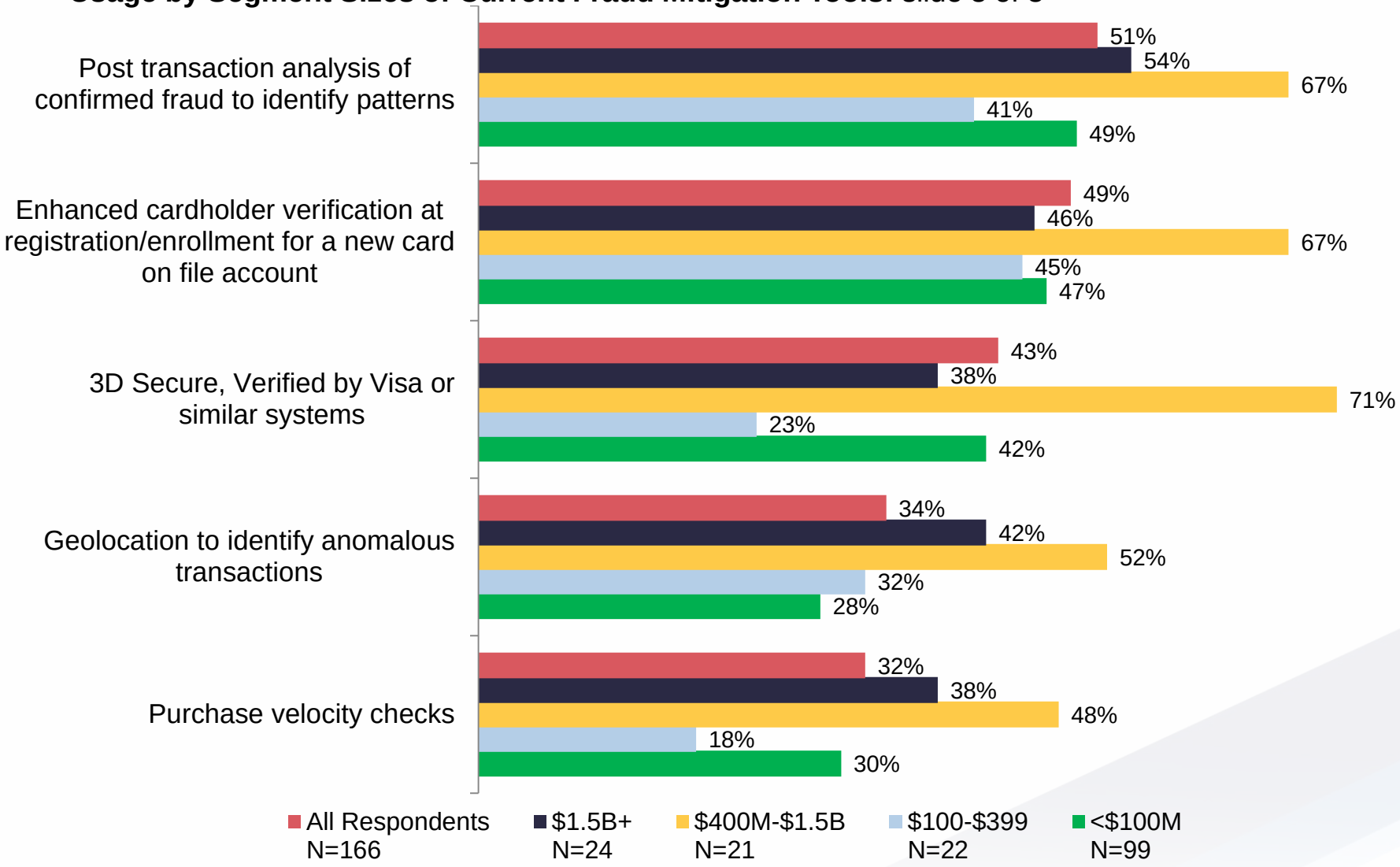
Usage by Segment Sizes of Current Fraud Mitigation Tools: slide 2 of 3



Q3A. Which of the following fraud mitigation tools/techniques does your organization currently use in the e-commerce sales channel?

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Usage by Segment Sizes of Current Fraud Mitigation Tools: slide 3 of 3



Q3A. Which of the following fraud mitigation tools/techniques does your organization currently use in the e-commerce sales channel?

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Largest retailers (with 1.5B+ annual sales) find out-of-band authentication, enhanced cardholder verification at registration/enrollment for a new card on file account, proprietary fraud models and purchase velocity checks to be particularly effective; 50%, 46%, 63%, and 38% of largest retailers respectively are using these tools.

	All Respondents N=166	$1.5B+ N=24	$400M-$1.5B N=21	$100M-$399M N=22	<$100M N=99
Enhanced cardholder verification at registration/enrollment for a new card on file account	8.0	8.0	8.6	7.3	8.0
Verification of physical card for customers who purchase online and pick up in store	7.9	7.8	8.3	7.6	7.9
3D Secure, Verified by Visa (or similar)	7.9	7.7	7.9	7.6	8.0
Require security code from card	7.9	7.7	8.6	7.4	7.9
Proprietary fraud model customized for our organization	7.8	7.9	7.6	7.3	7.9
Out-of-band authentication using one or more of these methods: one time password sent to mobile device, email, text message, phone call	7.8	8.1	8.5	7.6	7.6
Purchase velocity checks	7.8	7.9	8.1	8.0	7.6
Geolocation to identify anomalous transactions	7.8	7.4	7.7	7.9	7.9

Numbers on this and the next chart are mean or average values based on respondents rating each fraud tool on a 10-point scale, with 10 meaning "Extremely Effective".

3B. How effective is [Each] in helping Your Company combat current fraud threats and possible attacks? (On a 10-point scale where 1 means Not at all Effective and 10 means Extremely Effective.)

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Average Ratings of Fraud Tool Effectiveness, continued

	All Respondents N=166	$1.5B+ N=24	$400M-$1.5B N=21	$100M-$399M N=22	<$100M N=99
Increased scrutiny of high risk / large ticket or digital merchandise purchases	7.7	7.5	8.1	7.2	7.8
Shipping address verification	7.7	7.8	7.7	6.7	7.9
Check device data for consistency with prior purchase activity for the same account	7.7	7.3	8.2	7.6	7.8
Previous purchase history to identify anomalous transactions	7.6	7.3	7.7	7.0	7.8
Increased scrutiny of transactions with escalated / rush shipment arrangements	7.6	7.5	8.1	8.0	7.8
Address verification services	7.6	7.5	7.9	7.4	7.6
Post transaction analysis of confirmed fraud to identify patterns	7.5	7.3	7.3	7.6	7.6
Email address verification	7.3	6.8	8.1	6.8	7.3
Phone number verification	7.2	6.3	7.4	6.9	7.4

3B. How effective is [Each] in helping Your Company combat current fraud threats and possible attacks? (On a 10-point scale where 1 means Not at all Effective and 10 means Extremely Effective.)

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Observations about Current and Planned Usage of Fraud Mitigation Tools

1. No single tool is currently used by all or nearly all retailers surveyed.
   The tool with the highest usage score -- *requiring the security code from the card* -- is used by just three-quarters (76%) of respondents.

2. A multi-layered approach is the norm for the retailers' fraud fighting arsenal: findings indicate nine out of ten retailers employ two or more tools to fight fraud in the e-commerce channel.

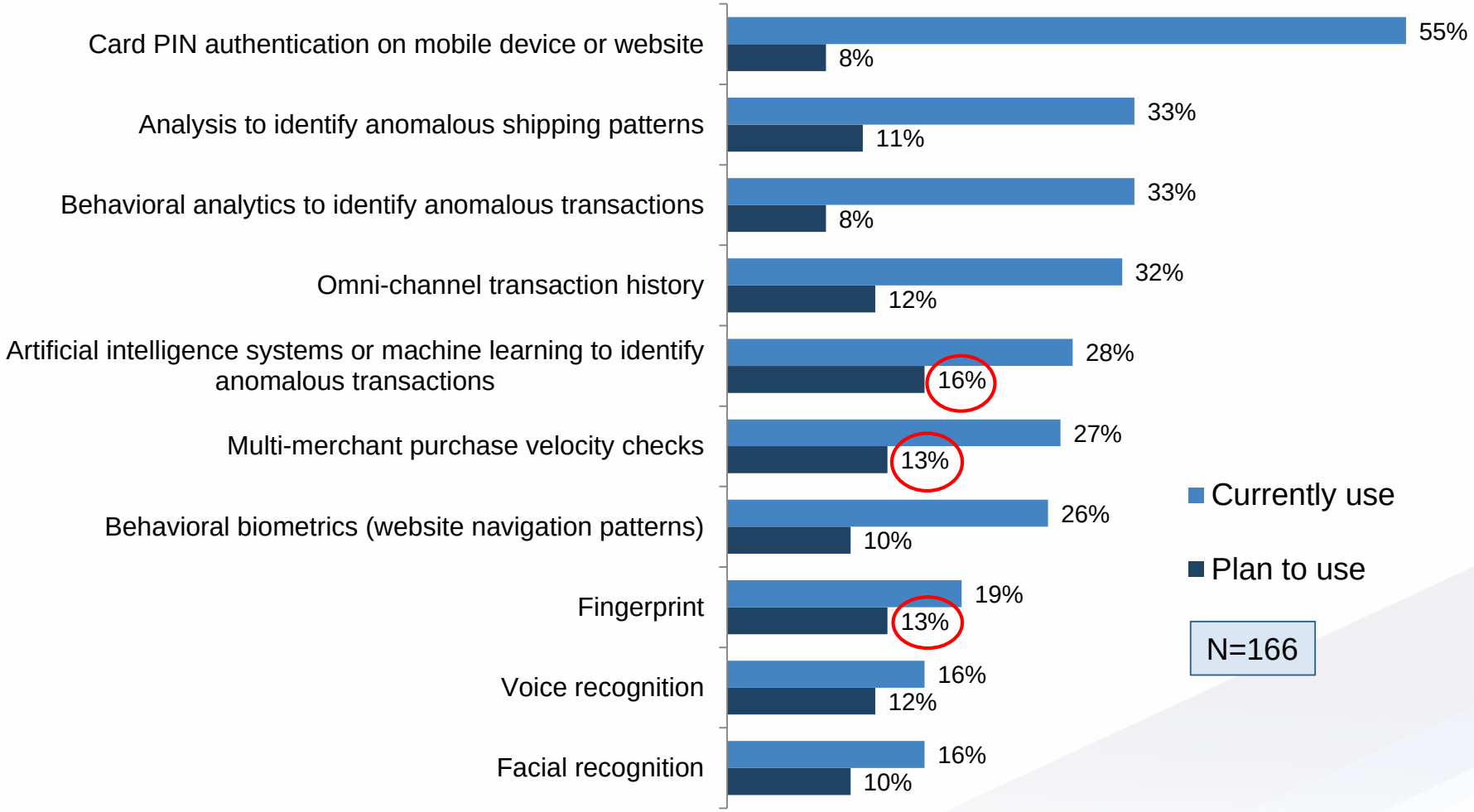
3. Surprisingly, 12 respondents said their companies used no fraud mitigation tools at all. This could be because they rely on their providers (such as processors or card associations) to supply fraud prevention services.

4. What are the top three fraud mitigation tools that retailers plan to adopt in the next 6 to 12 months?

   - About 14% say they plan to start using *3D Secure, Verified by Visa or similar systems*
   - About 11% plan to adopt *purchase velocity checks*
   - About 10% plan to use *geolocation to identify anomalous transactions*

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Use of any emerging fraud mitigation technologies is relatively low, with the exception of *card PIN authentication on mobile device or website.* Planned adoption is highest for artificial intelligence systems, multi-merchant purchase velocity checks and fingerprint.

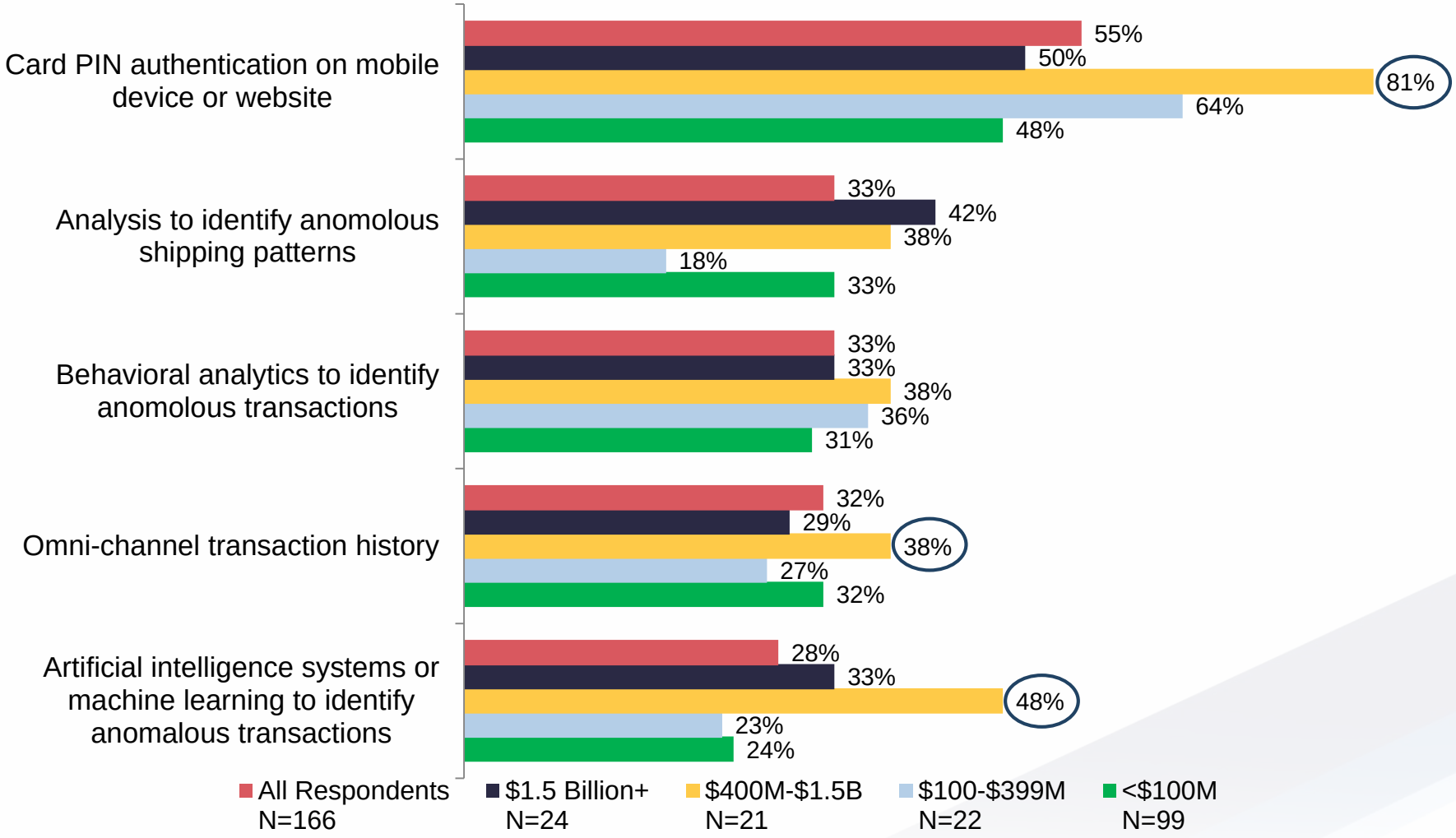


Q4A. Which of the following emerging fraud mitigation methods does your organization currently use in the e-commerce sales channel?
4C. [If not using] Which of these do you plan to use in next 6 to 18 months?

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Usage by Segment Sizes of Emerging Fraud Mitigation Tools: slide 1 of 2

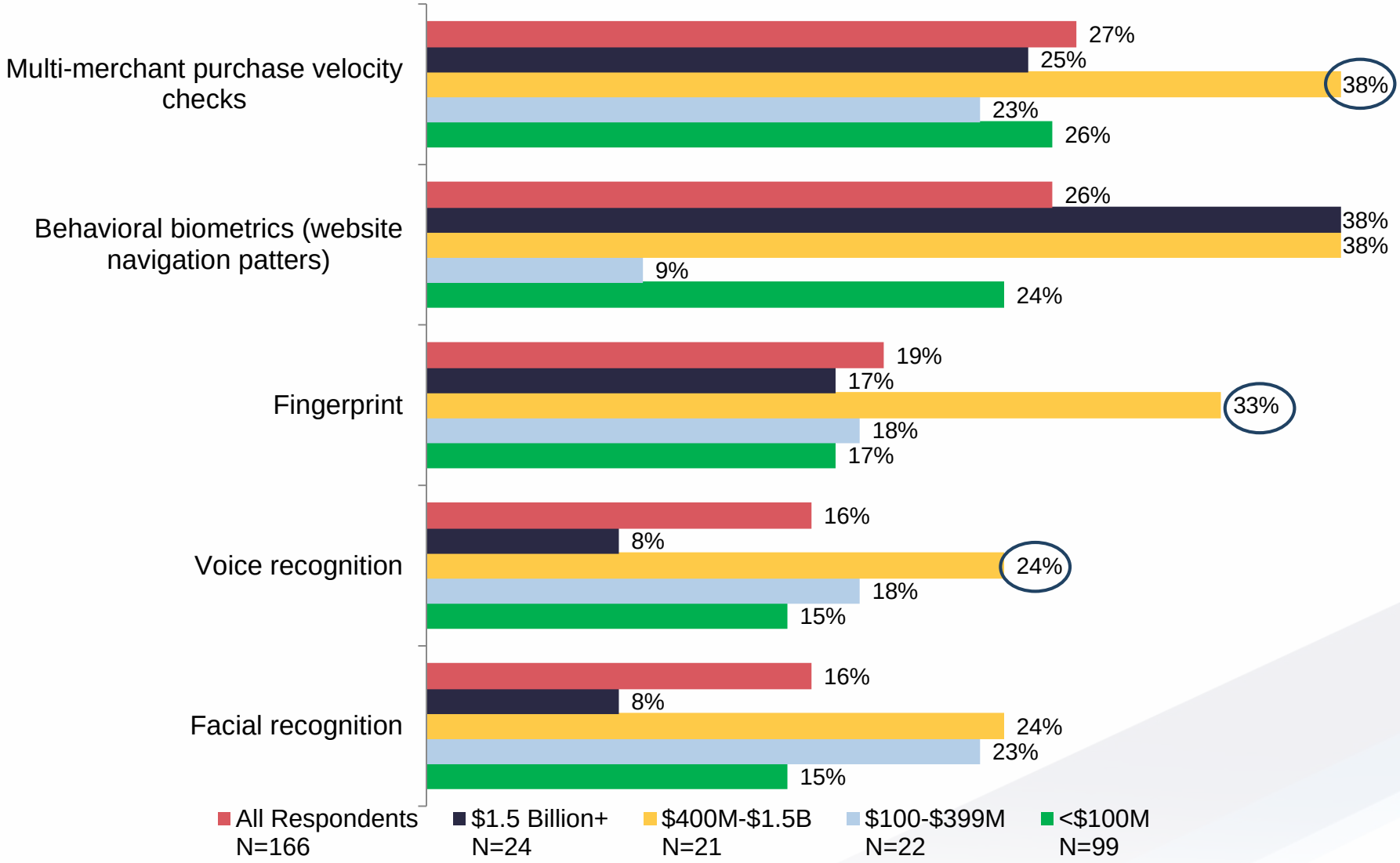
Notably, compared to other segments, retailers in the size segment $400M - $1.5B (in gold) report higher usage of several emerging tools on this and the next page.



Q4A. Which of the following emerging fraud mitigation methods does your organization currently use in the e-commerce sales channel?

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Usage by Segment Sizes of Emerging Fraud Mitigation Tools: slide 2 of 2



Q4A. Which of the following emerging fraud mitigation methods does your organization currently use in the e-commerce sales channel?

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Adoption of emerging tools is fairly low, but users rate some tools high in effectiveness.

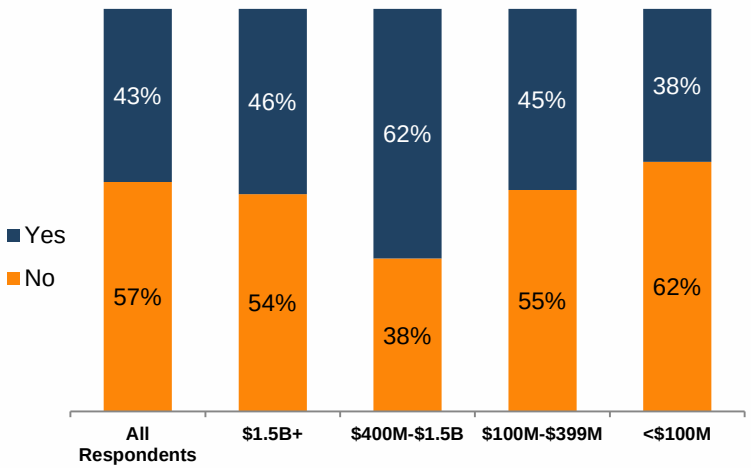
	All Respondents N=166	$1.5B+ N=24	$400M-$1.5B N=21	$100M-$399M N=22	<$100M N=99
Artificial intelligence systems	8.2	7.8	8.3	8.0	8.3
Facial recognition	7.9	8.0	8.4	7.8	7.8
Voice recognition	7.9	8.0	9.0	7.8	7.6
Card PIN authentication	7.8	7.5	8.5	7.1	7.9
Multi-merchant purchase velocity checks	7.8	7.3	8.9	7.8	7.6
Behavioral biometrics	7.7	8.1	8.1	9.5	7.2
Omni-channel transaction history	7.6	7.9	8.0	8.0	7.4
Fingerprint	7.6	7.8	8.7	8.0	7.0
Behavioral analytics	7.6	7.4	8.1	8.0	7.4
Analysis to identify anomalous shipping patterns	7.5	7.4	8.1	7.3	7.4

Numbers on this chart are mean or average values based on respondents rating each fraud tool on a 10-point scale, with 10 meaning "Extremely Effective."

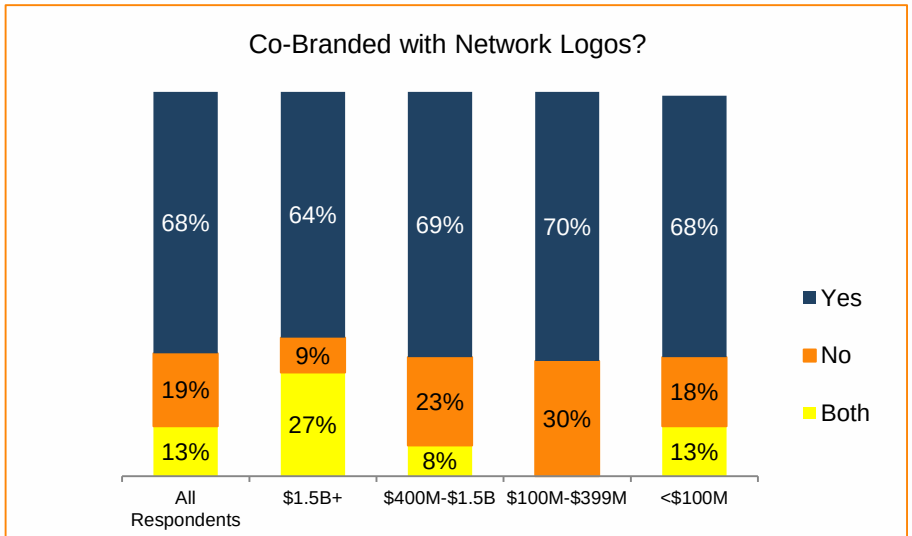
4b. How effective is [each] in helping your company combat current fraud threats and possible attacks? (On a 10-point scale where 1 means Not at all Effective and 10 means Extremely Effective.)

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

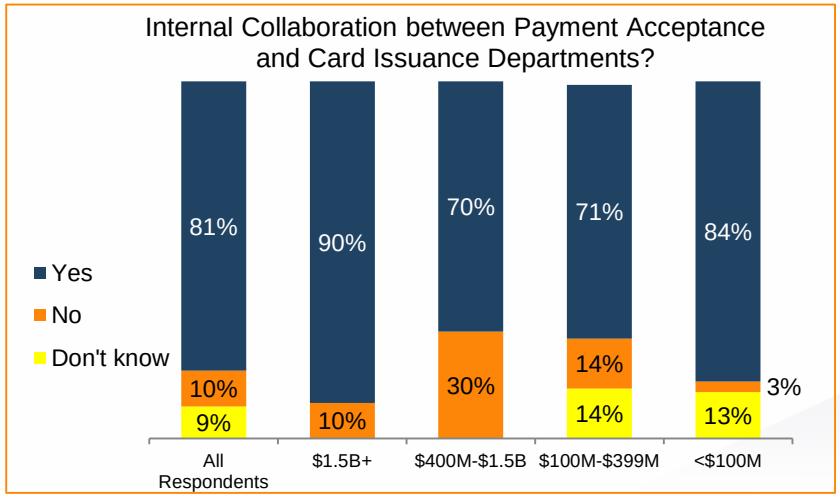
About four in ten (43%) retailers issue store-branded cards. Most card-issuing retailers collaborate or share fraud-related information between departments.



Q5. Does your organization issue store-branded cards to your customers?



Q5a. Are these co-branded with card network logos such as Visa or MasterCard? Yes, No, Both (some cards have network logo/some do not)

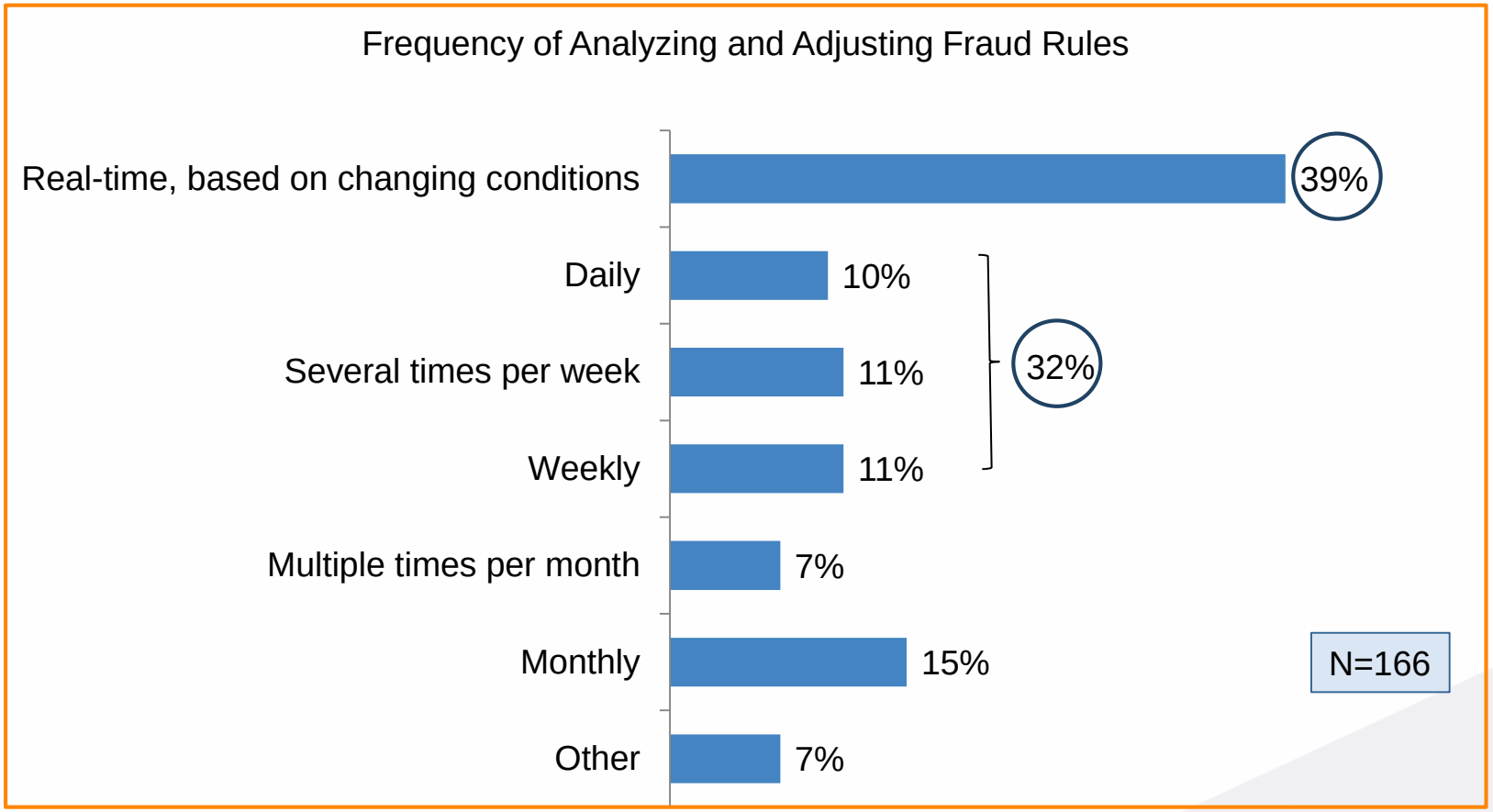


All Respondents (N=166)
$1.5B+ (N=24)
$400M - <$1.5B (N=21)
$100 - $399M (N=22)
<$100M (N=99)

Q5b. Do the groups at your organization that manage payment acceptance and card issuance collaborate or share information with each other on fraud trends or mitigation techniques?

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

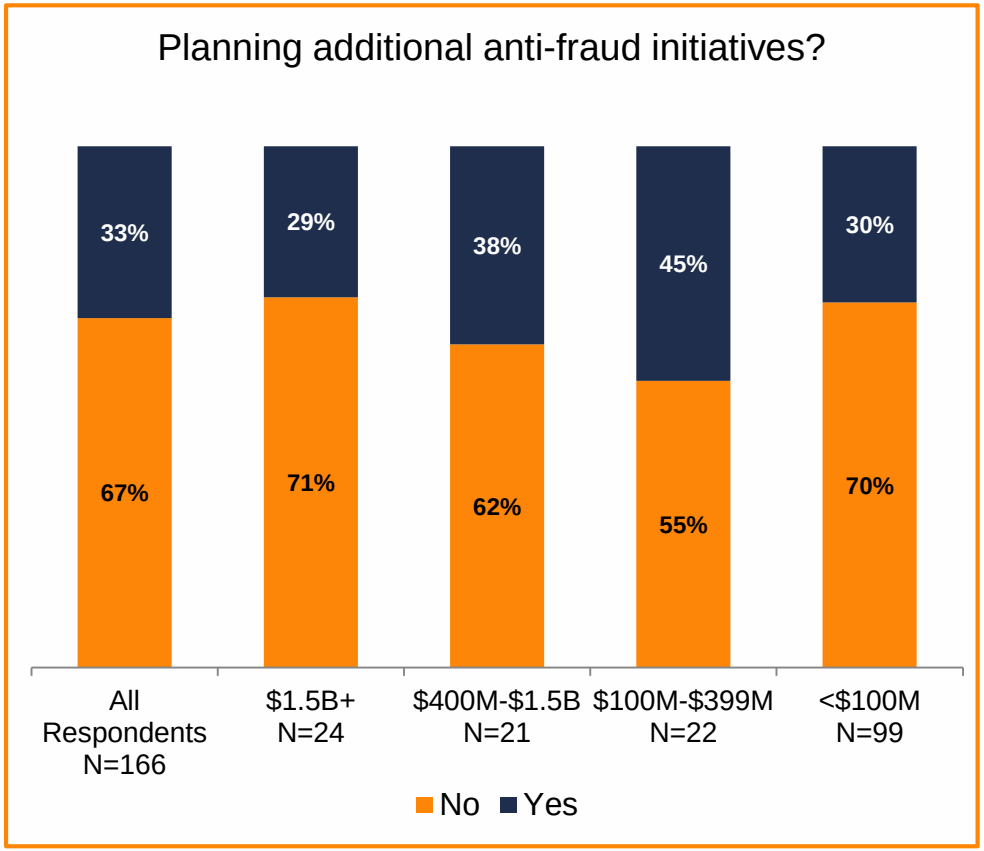
Nearly four in ten (39%) of companies analyze and adjust fraud rules in real time based on changing conditions; about one-third (32%) make adjustments at least weekly.



Q6. How frequently do you analyze and adjust fraud rules?

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Combatting e-commerce fraud requires ongoing attention; about one-third of companies plan to take additional steps in this area.



Q7 Thinking about the tools and techniques you are using or planning to use, are you taking or planning to take any other steps to combat e-commerce fraud?

New efforts mentioned:

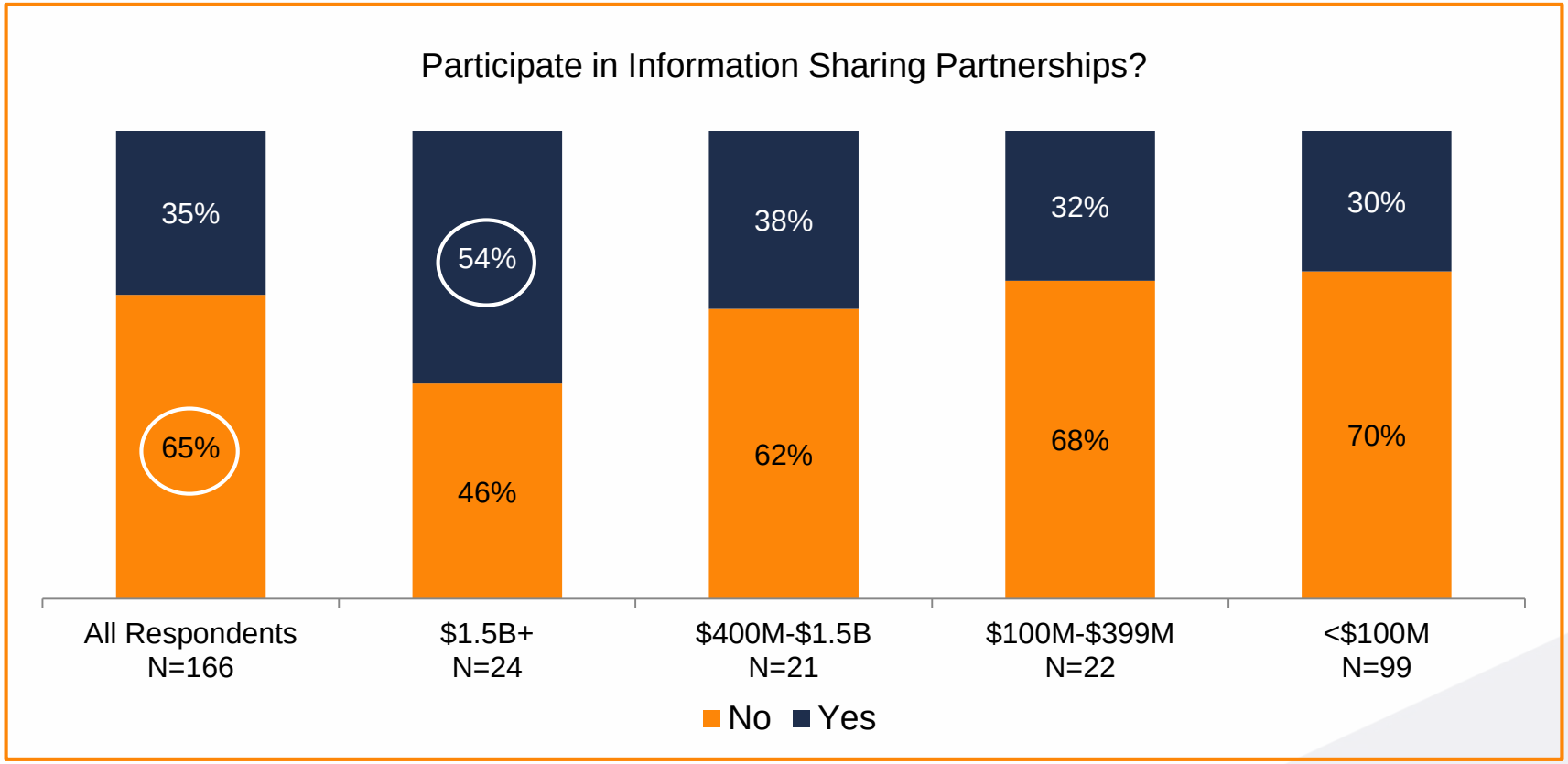
- *"…implement a "big data" e-commerce fraud detection tool…"* ($1.5B+)
- *"…roll-out multi-factor authentication…across all products"* ($1.5B+)
- *"…multi-layered…security checks for authenticity"* ($400M-$1.5B+)
- Multiple mentions of "employee education and training" ($100M - $399M)
- *"New technology as it releases, better on-site software and (fraud) recognition programs"* ($<100M)

Retailers indicate they will pursue varying strategies, such as emphasizing basics like education and training while maintaining ongoing evaluations of emerging technologies to help them combat all types of fraud.

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Section III:
Information Sharing Partnerships

Nearly two-thirds or all retailers (65%) do <u>not</u> participate in an information sharing partnership or trade group committee to exchange fraud threat information. Participation is highest among the largest retailers (annual sales $1.5B+).

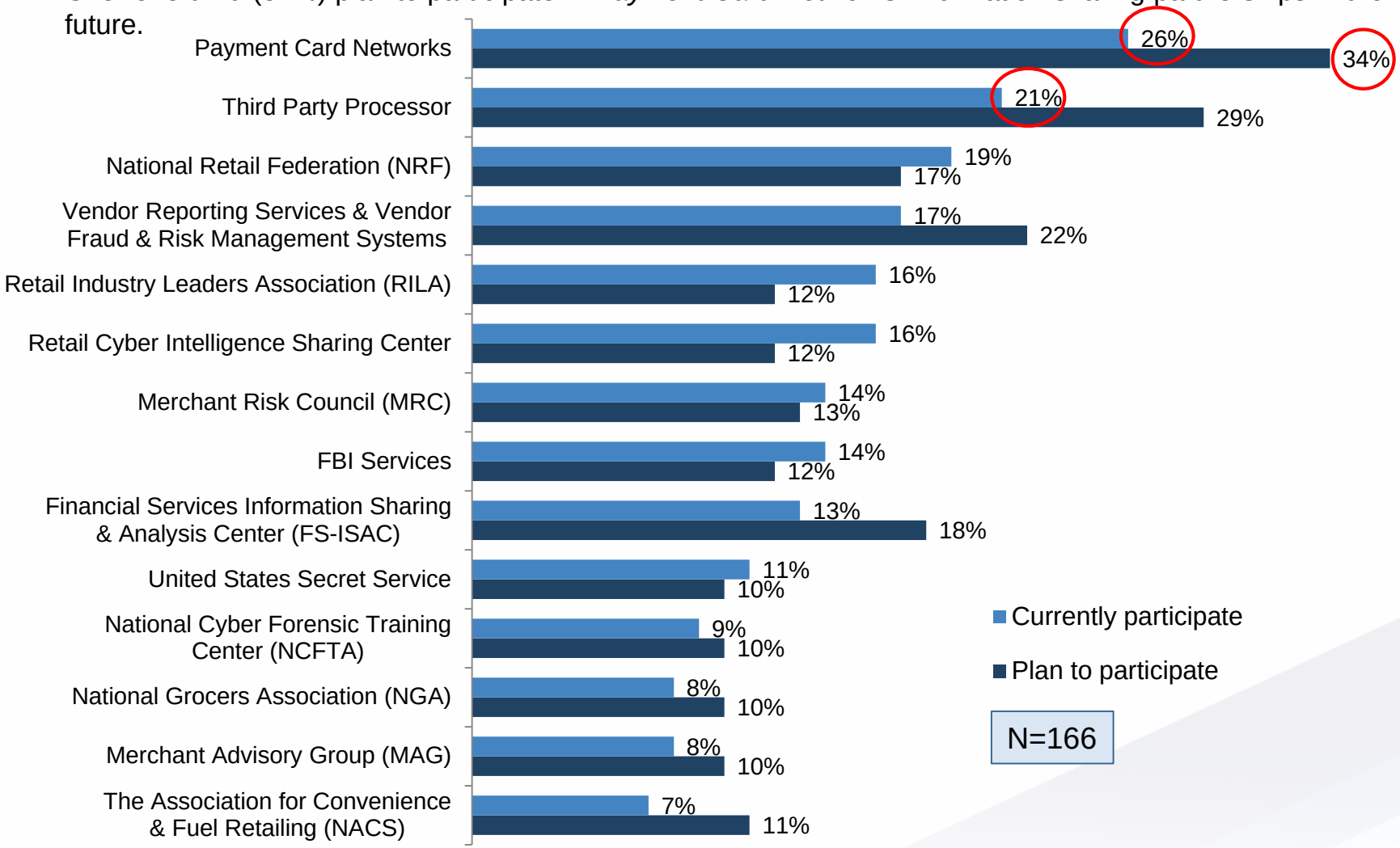


Q8. Fraud information sharing partnerships allow organizations to exchange threat information in a secure way which helps increase awareness of risk. Is your company or are you personally a participant in any industry fraud information sharing partnerships or committees of trade groups that are focused on fraud issues?

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Payment Card Networks (26%) and _Third Party Processor_ (21%) partnerships are the most highly utilized resources retailers rely on to get alerts about new fraud attacks and threats.

Over one-third (34%) plan to participate in _Payment Card Networks_ information sharing partnerships in the future.



Q8a. Which of the following fraud information sharing partnerships do you currently participate in? 8C. [If not using] Which of these do you plan to participate in next 6 to 12 months?

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Participation in any fraud information sharing partnerships is relatively low, but those retailers that participate in these partnerships find them effective in identifying current fraud threats and possible attacks.

	All Respondents N=166	$1.5B+ N=24	$400M-$1.5B N=21	$100M-$399M N=22	<$100M N=99
Note: this question used a 5-point scale, with 5 meaning "Extremely effective."					
Financial Services Information Sharing and Analysis Center (FS-ISAC)	4.5	4.7	4.4	4.7	4.4
Merchant Advisory Group (MAG)	4.4	4.3	4.4	5.0	-
Vendor reporting services and vendor fraud and risk mgmt. systems	4.3	4.5	4.8	4.7	4.1
Payment Card Networks (Visa, MasterCard, American Express and Discover)	4.3	4.5	4.5	4.0	4.2
Third Party Processor	4.3	4.3	4.2	4.8	4.2
Retail Industry Leaders Association (RILA)	4.3	4.2	4.3	3.7	4.4
Merchant Risk Council (MRC)	4.3	4.0	4.0	4.3	4.5
The Association for Convenience & Fuel Retailing (NACS)	4.3	3.5	4.0	4.5	4.6

8B. [Repeat for each yes] How effective do you think the efforts of [Pipe in answer] are in helping Your Company identify current fraud threats and possible attacks, on a scale of 1 to 5 where 1 means "Not effective" and 5 means "Extremely effective".

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Effectiveness of Fraud Information Sharing Partnerships, continued

Note: this question used a 5-point scale, with 5 meaning "Extremely effective."	All Respondents N=166	$1.5B+ N=24	$400M-$1.5B N=21	$100M-$399M N=22	<$100M N=99
National Retail Federation (NRF)	4.2	4.3	4.3	4.0	4.2
Retail Cyber Intelligence Sharing Center	4.2	4.3	4.8	4.5	4.0
National Cyber-Forensics and Training Center (NCFTA)	4.2	3.8	4.7	5.0	4.1
FBI services	4.1	3.8	4.2	5.0	4.1
U.S. Secret Service services	3.9	3.7	3.8	4.0	4.1
National Grocers Association (NGA)	3.9	3.0	4.8	4.0	3.7

Numbers on this chart are mean or average values based on users rating each partnership on a 5-point scale, with 5 meaning "Extremely effective."

8B. [Repeat for each yes] How effective do you think the efforts of [Pipe in answer] are in helping Your Company identify current fraud threats and possible attacks, on a scale of 1 to 5 where 1 means "Not effective" and 5 means "Extremely effective".

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

Study Methodology

- The initial sample was derived by combining a Dun & Bradstreet extract of U.S. based companies above $250 million (M) in annual sales with internal Phoenix Marketing International contact files. This process resulted in a national database of approximately 1,700 companies. Later the sample universe was expanded to all companies above $25M with a retail customer presence with e-commerce activity. This expansion was targeted at companies above $25M but smaller companies could qualify if they had an e-commerce presence. The final result is that the sample was drawn from the 12,500 largest U.S. retailers with about $25M or more in annual sales.
- Respondents were qualified via telephone interviews. Qualified respondents were then sent a link to the online survey.
- As an incentive, participants who completed the online survey were given access to a secure online portal which enabled them to compare their own answers to all respondents and to these four retail segments based on annual sales:
    - $1.5B+
    - $400M - <$1.5B
    - $100 - $399M
    - <$100 M
- The end sample consists of 166 surveys completed by the largest approximately 12,500 U.S. retailers. Data was collected from December 2017 to March 2018.
- The study was conducted by Phoenix Marketing International.
- The study was sponsored by the Payments, Standards, and Outreach Group of the Federal Reserve Bank of Minneapolis.

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.

For additional information or to share your comments, please send an email to:

mpls.psog.events@mpls.frb.org

©2018 Federal Reserve Bank of Minneapolis. Materials are not to be used without consent.