2014 Payments Fraud Survey

Summary of Consolidated Results

Payments Information & Outreach Office
Federal Reserve Bank of Minneapolis

December 2014

Topics

- Survey Methodology & Respondent Profile
- Fraud Attempts & Losses
- Fraud Schemes
- Risk Mitigation
- Opportunities to Reduce Payments Fraud
- Conclusions

Survey Methodology & Respondent Profile

2014 FRB Payments Fraud Survey

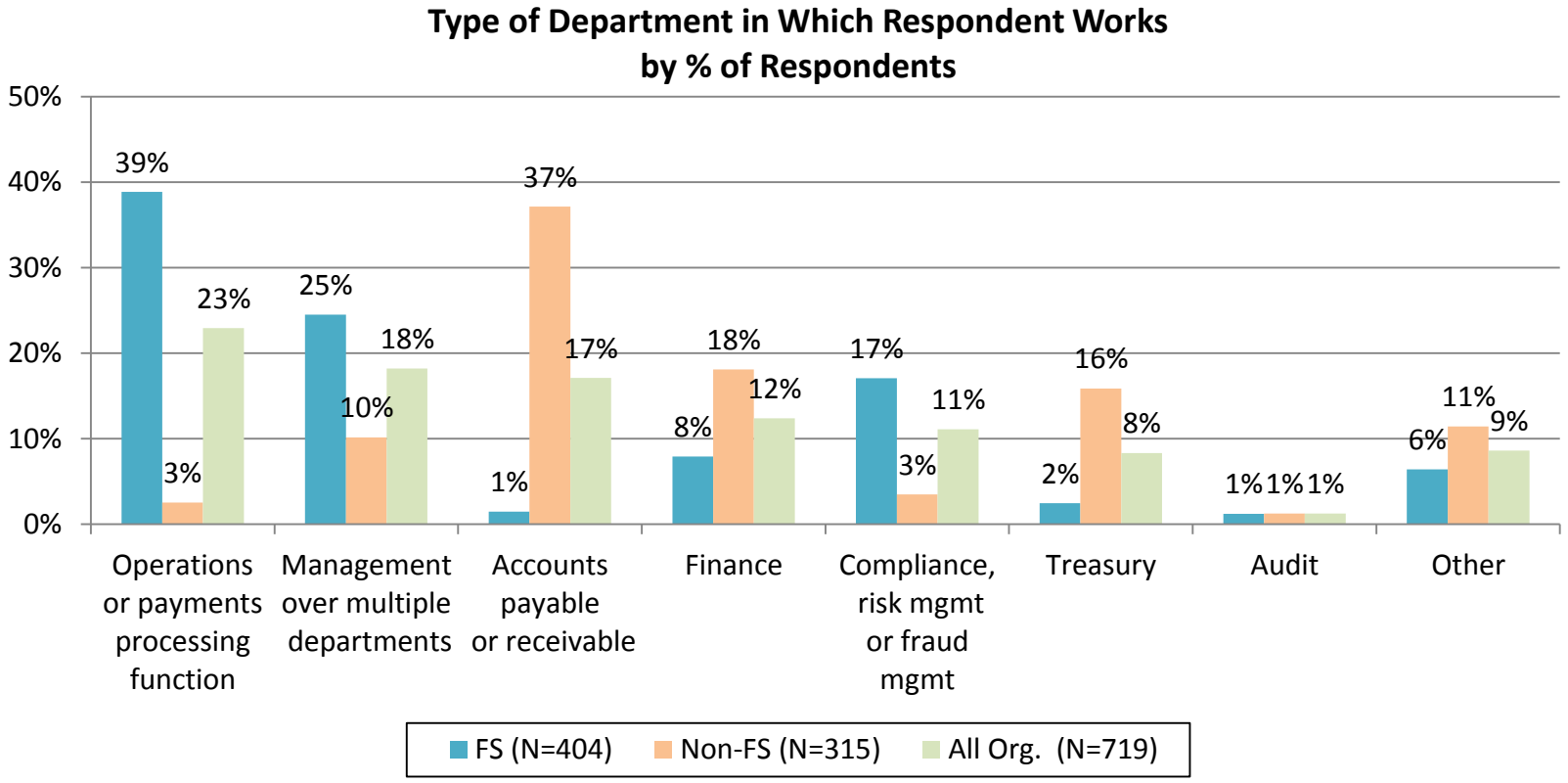
- This biennial survey seeks to uncover fraud trends & effective fraud mitigation strategies
- Sponsored by the Federal Reserve Banks (FRB) of Minneapolis, Boston, Chicago, Dallas, & Richmond
- Federal Reserve Banks (FRB) & trade associations distributed requests for participation; data was collected in April & May 2014
- 747 responses in 2014

Respondent Industry Classification	2014 (N=747)	2012 (N=740)
Financial Service Industry	56%	94%
Non-Financial Service Industry	44%	6%

The *2014 Payments Fraud Survey - Summary of Consolidated Results* & the survey questions can be found online at: http://www.minneapolisfed.org/about/whatwedo/paymentsinformation.cfm

Respondent's Area of Work

- Most respondents work in a payments processing area of their organization or manage multiple departments



Payments & Payments Risk Education

- Many respondents are members of multiple trade associations that provide education on payments
- Non-FS firms are less likely to belong to an association that focuses on payments (38%); this highlights the importance of providing accurate & timely information on payments & payments risk to non-FS firms

Respondent Membership in Trade Associations that Provide Education on Payments or Payments Risk by % of Respondents

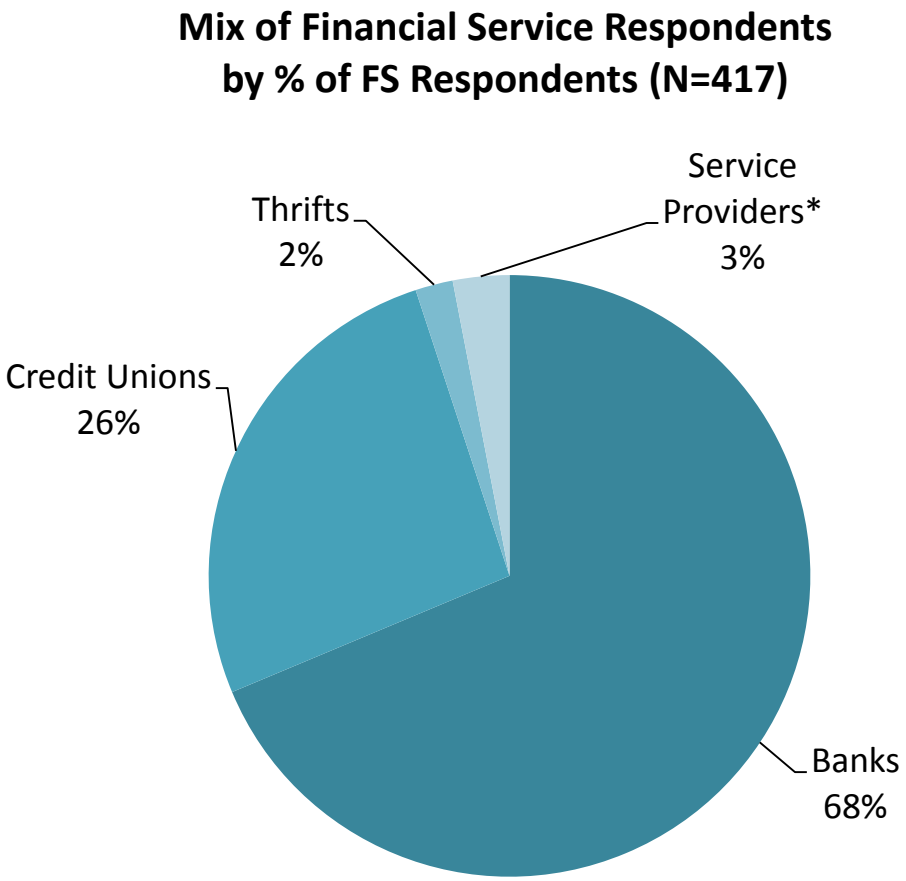
Trade Association	FS (N=399)	Non-FS (N=303)	All Org. (N=702)
NACHA The Electronic Payments Association	58%	8%	36%
Regional payments association (e.g., NEACH,SWACHA, WACHA,UMACHA, etc.)	51%	4%	30%
American Bankers Association (ABA)	48%	4%	29%
State banking association	45%	4%	27%
Independent Community Bankers of America (ICBA)	41%	3%	24%
Credit Union National Association (CUNA)	23%	1%	13%
Association for Financial Professionals (AFP)	4%	17%	10%
State AFP or treasury management association	2%	10%	5%
National Association of Federal Credit Unions (NAFCU)	6%	1%	4%
Regional Credit Union League or Network	2%	0%	1%
Credit Research Foundation (CRF)	0%	13%	6%
National Association of Credit Management (NACM)	0%	17%	8%
National Association of Purchasing Card Professionals (NAPCP)	0%	4%	2%
Other	7%	12%	8%
None	2%	38%	17%

Respondent Size by Revenue

- The majority of respondents (55%) are relatively small with annual revenues less than $100 million

Respondent Size by Annual Revenue	Year-end 2013			Year-end 2011		
	FS (N=417)	Non-FS (N=330)	All Org. (N=747)	FS (N=692)	Non-FS (N=48)	All Org. (N= 740)
Under $10 million	53%	10%	34%	61%	15%	58%
$10 million to $24.9 million	12%	6%	9%			
$25 million to $49.9 million	5%	6%	5%			
$50 – 99.9 million	5%	8%	6%	8%	13%	8%
$100 – 249.9 million	3%	11%	6%	9%	6%	9%
$250 - 499.9 million	1%	12%	6%	5%	10%	6%
$500 - 999.9 million	1%	10%	5%	4%	6%	4%
$1 – 4.9 billion	2%	18%	9%	3%	23%	4%
$5 – 9.9 billion	1%	5%	3%	0%	10%	1%
$10 billion or more	2%	6%	4%	0%	13%	1%
Don't Know	7%	5%	6%	9%	2%	9%
Not applicable	8%	5%	7%	1%	2%	1%

Financial Service (FS) Respondents



*In this survey the financial service, *service providers* are organizations such as payment processors, lockbox providers, card service providers, etc.

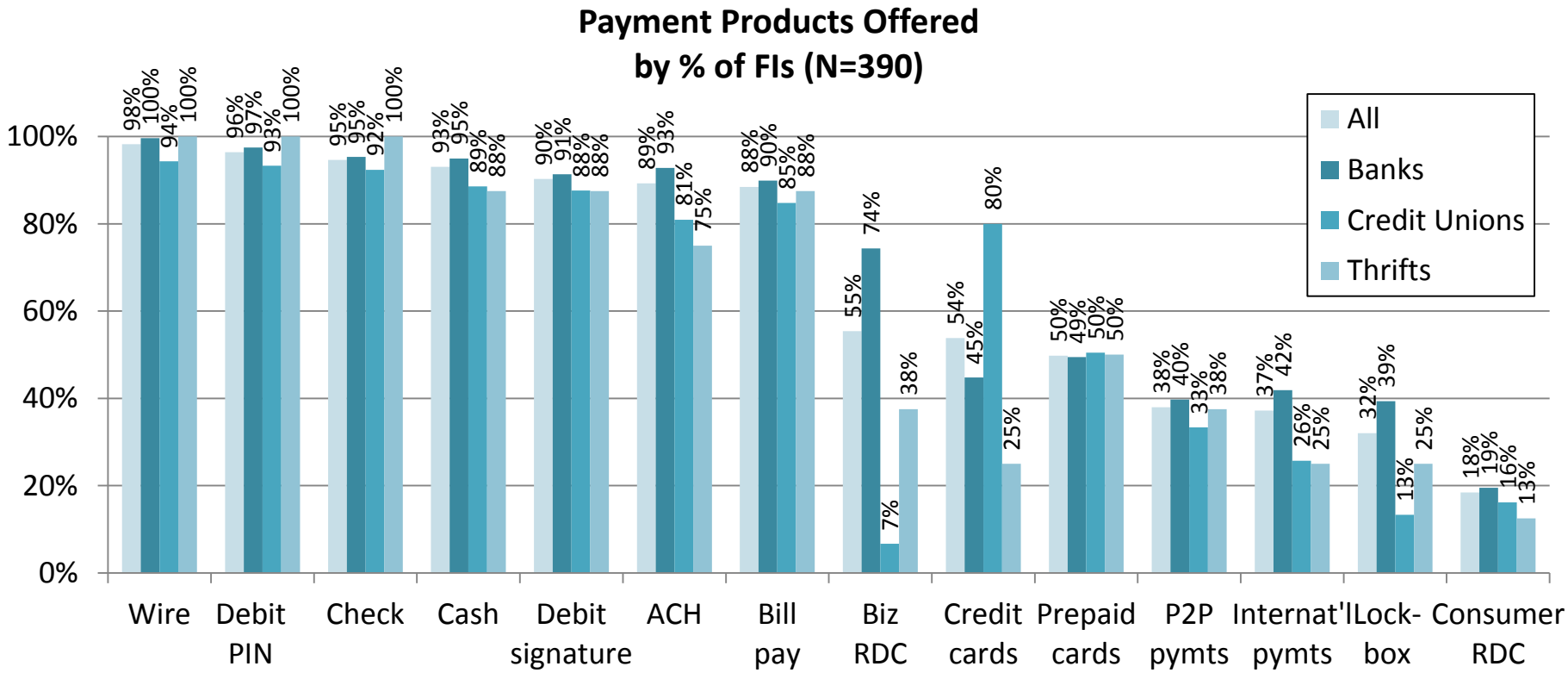
Financial Institution (FI) Respondents

Financial Institution Size by Assets	YE 2013	YE 2011
Under $50 million	19%	16%
$50 – 99.9 million	18%	17%
$100 – 249.9 million	20%	26%
$250 - 499.9 million	16%	18%
$500 - 999.9 million	11%	12%
$1 – 4.9 billion	10%	7%
$5 – 9.9 billion	2%	2%
$10 billion or more	4%	1%

Payment Product Customers	Banks	Credit Unions	Thrifts
Both consumer & business or commercial clients	85%	27%	63%
Primarily consumer clients	10%	73%	38%
Primarily business or commercial clients	5%	0%	0%

FI Payment Products Offered

- Nearly all FIs offer ACH, cash, check, debit card & wire products

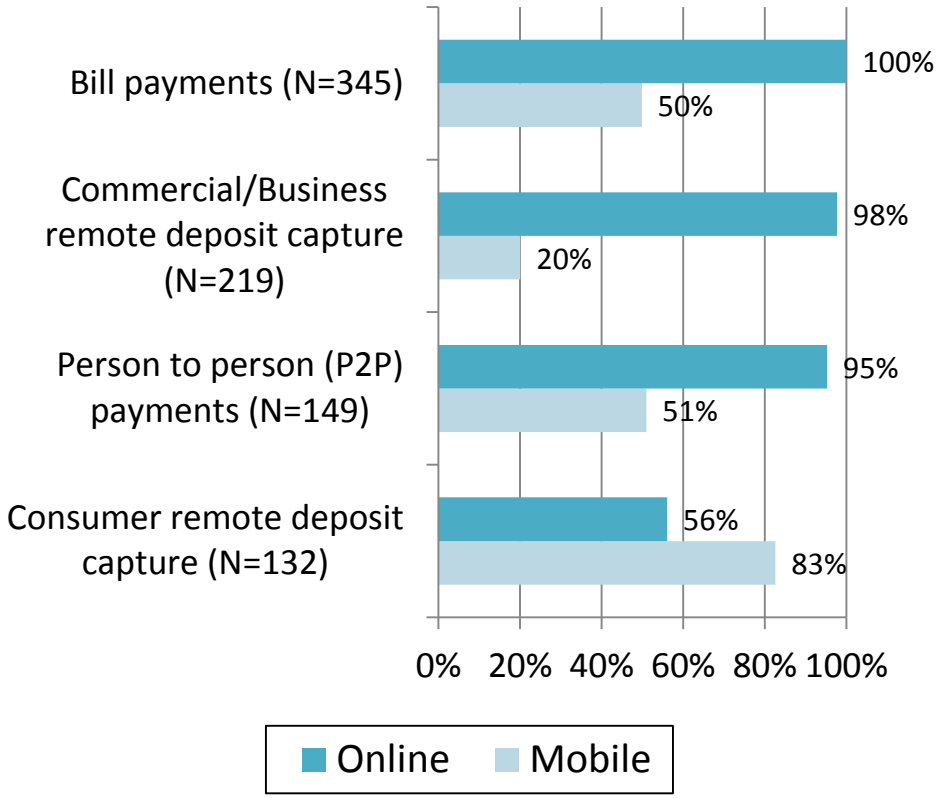


RDC is Remote Deposit Capture & P2P is person-to-person

FI Payment Products Offered

- FIs are more likely to offer bill payment, commercial RDC & P2P products for customer use online rather than via a mobile device
- However, FIs are more likely to offer *consumer* RDC products via a mobile device

Online & Mobile Services by % of FIs that Offer the Service



Non-FS Respondents' Industry Classification

- Respondents from non-financial firms represent a wide variety of industries

Industry Classification	2014 (N=330)	2012 (N=48)
Manufacturing	28%	10%
Wholesale Trade	14%	0%
Government	5%	19%
Software & Technology	5%	0%
Retail Trade	5%	8%
Construction	4%	6%
Business Services & Consulting	4%	2%
Educational Services	4%	0%
Transportation & Warehousing	4%	2%
Energy	3%	10%
Agriculture	3%	0%
Health Services	2%	8%
Insurance & Pension Funds	2%	2%
Brokers, Underwriters & Investment Companies	2%	4%
Hospitality & Travel	1%	6%
Real Estate, Rental & Leasing	1%	2%
Telecommunications	1%	2%
Nonprofit	0%	6%
Other	13%	10%

Non-FI Typical Payment Counterparties

- The majority of non-FIs responding to this survey primarily make & receive payments to & from other businesses (58%)

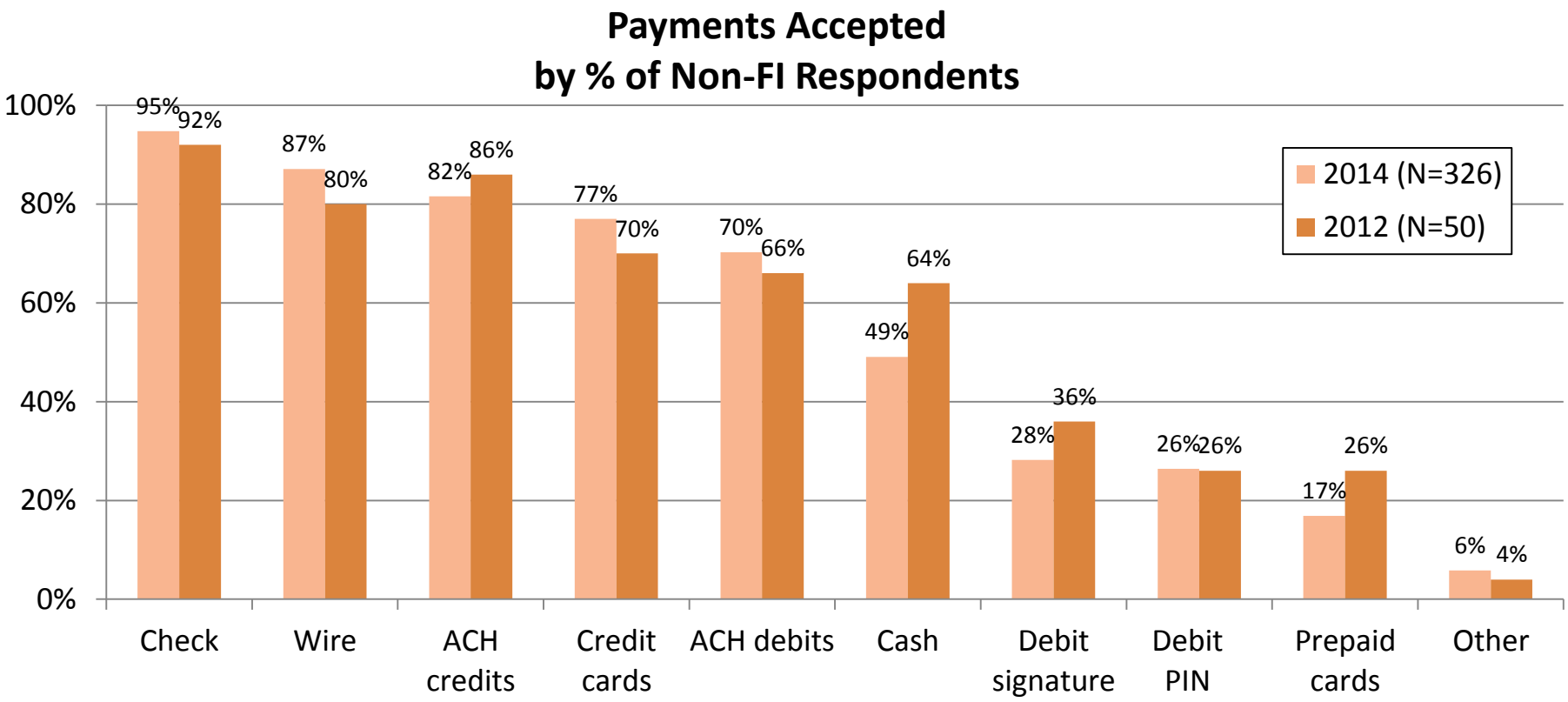
Non-FS Typical Payment Counterparties
by % of Non-FI Respondents

Payment Counterparties*	2014 (N=326)	2012 (N=51)
Primarily payments to/from other businesses	58%	39%
Payments to/from both consumers & businesses	38%	53%
Primarily payments to/from consumers	4%	8%

*Businesses include government entities

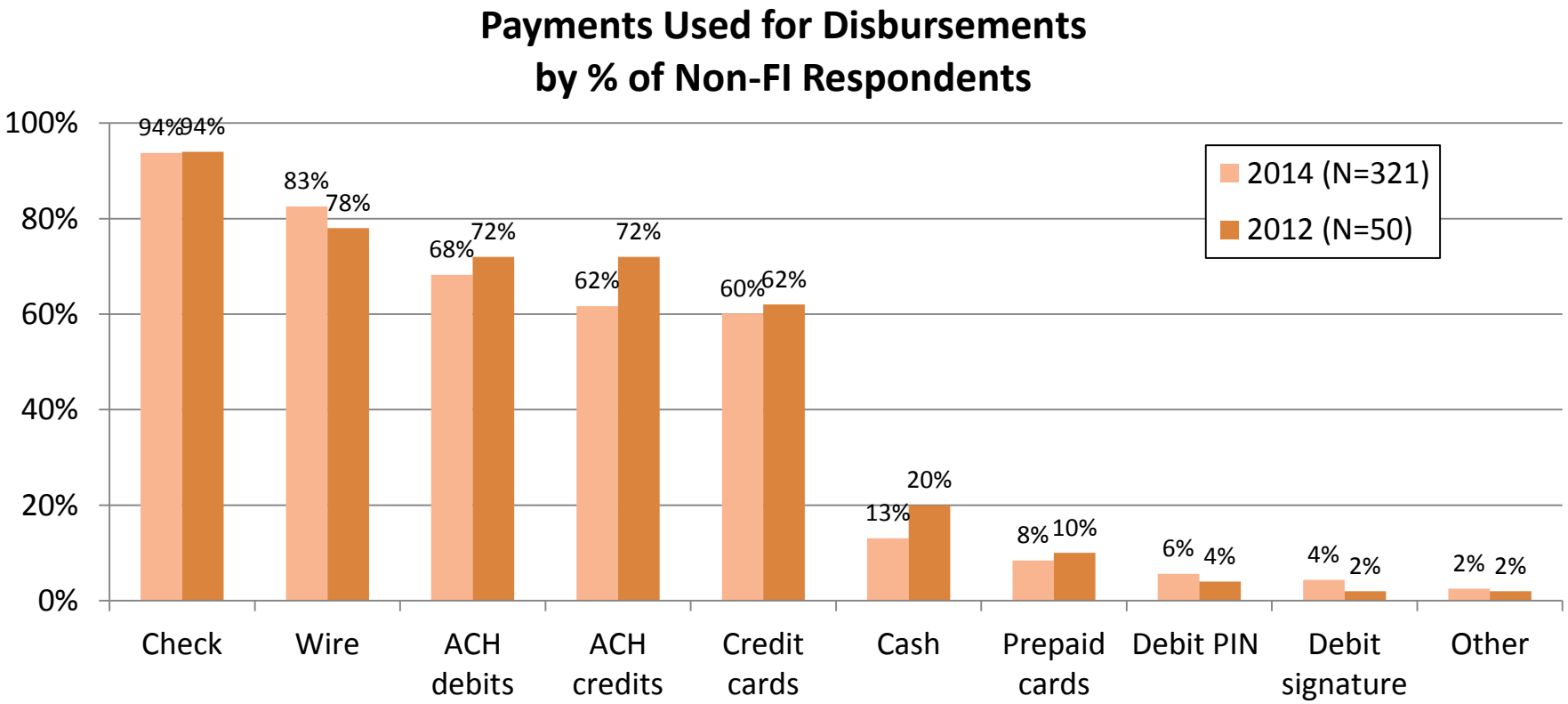
Non-FI Payment Types Used

- Over 3/4 of businesses accept check, ACH & wire payments



Non-FI Payment Types Used

- ACH, checks, credit card & wire payments are used by are greater share of non-FI firms for disbursements compared other payment types

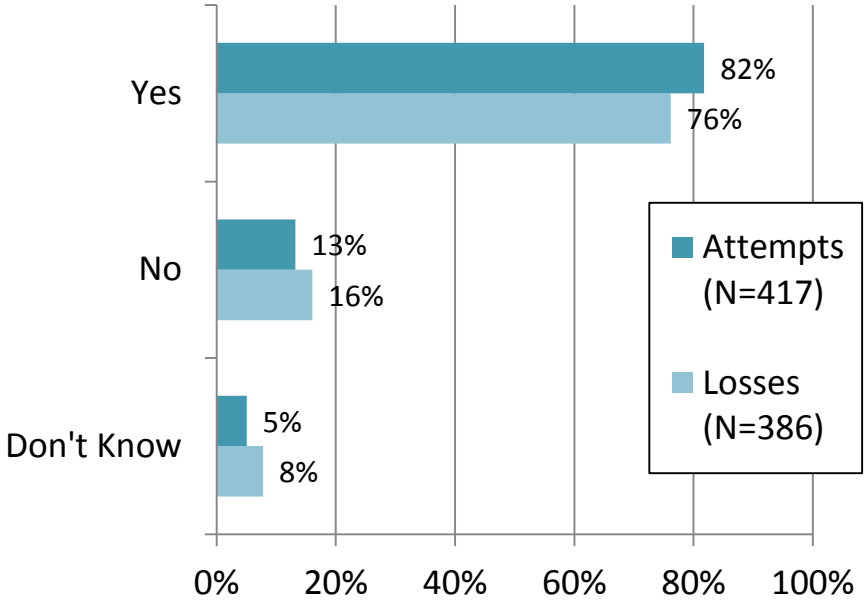


Fraud Attempts & Losses

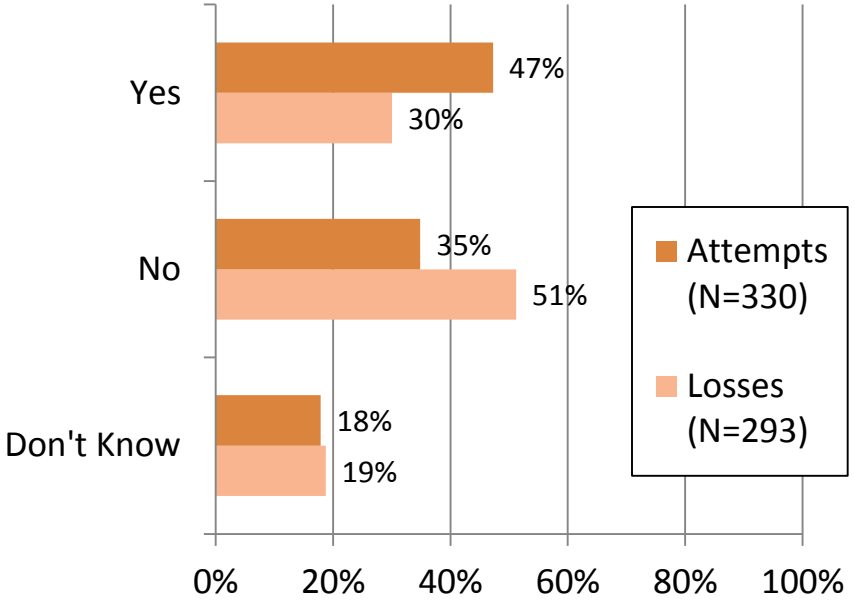
Payment Fraud Attempts & Losses

- 67% of those surveyed report payment fraud attempts against their organization; 56% report experiencing losses

Payment Fraud Attempts & Losses Experienced in 2013 by % of FS Respondents



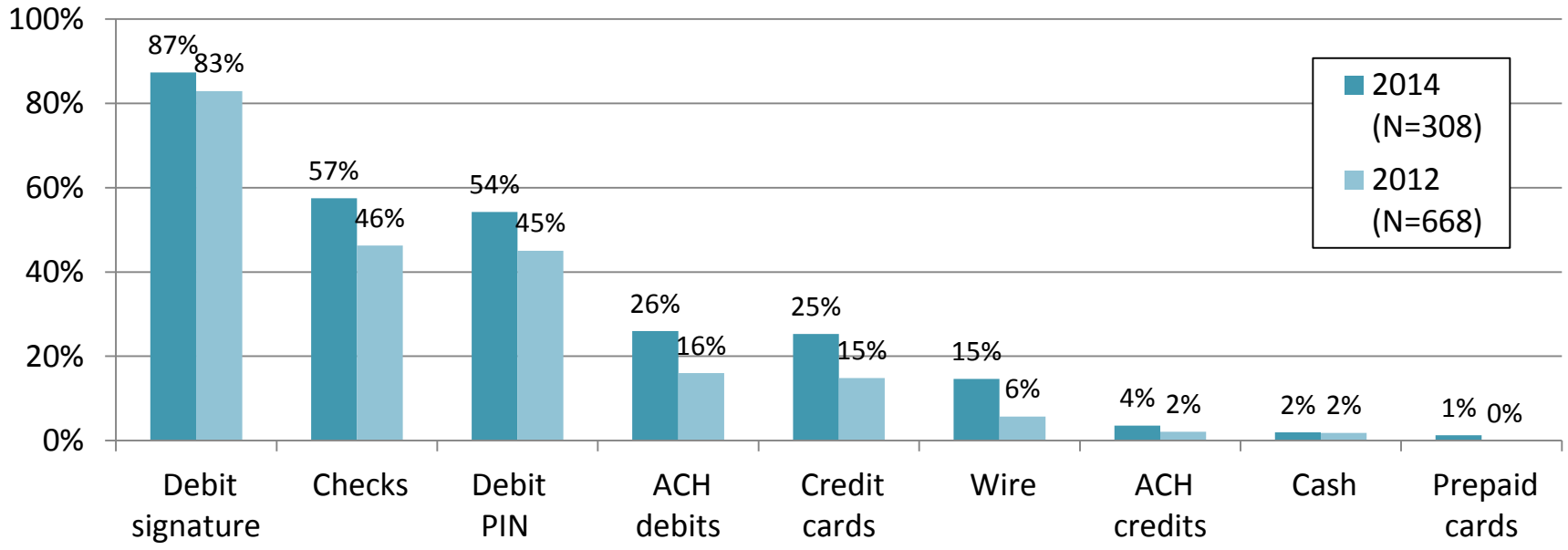
Payment Fraud Attempts & Losses Experienced in 2013 by % of Non-FS Respondents



FS Firms Are Most Prone to Signature Debit Card Fraud Attempts

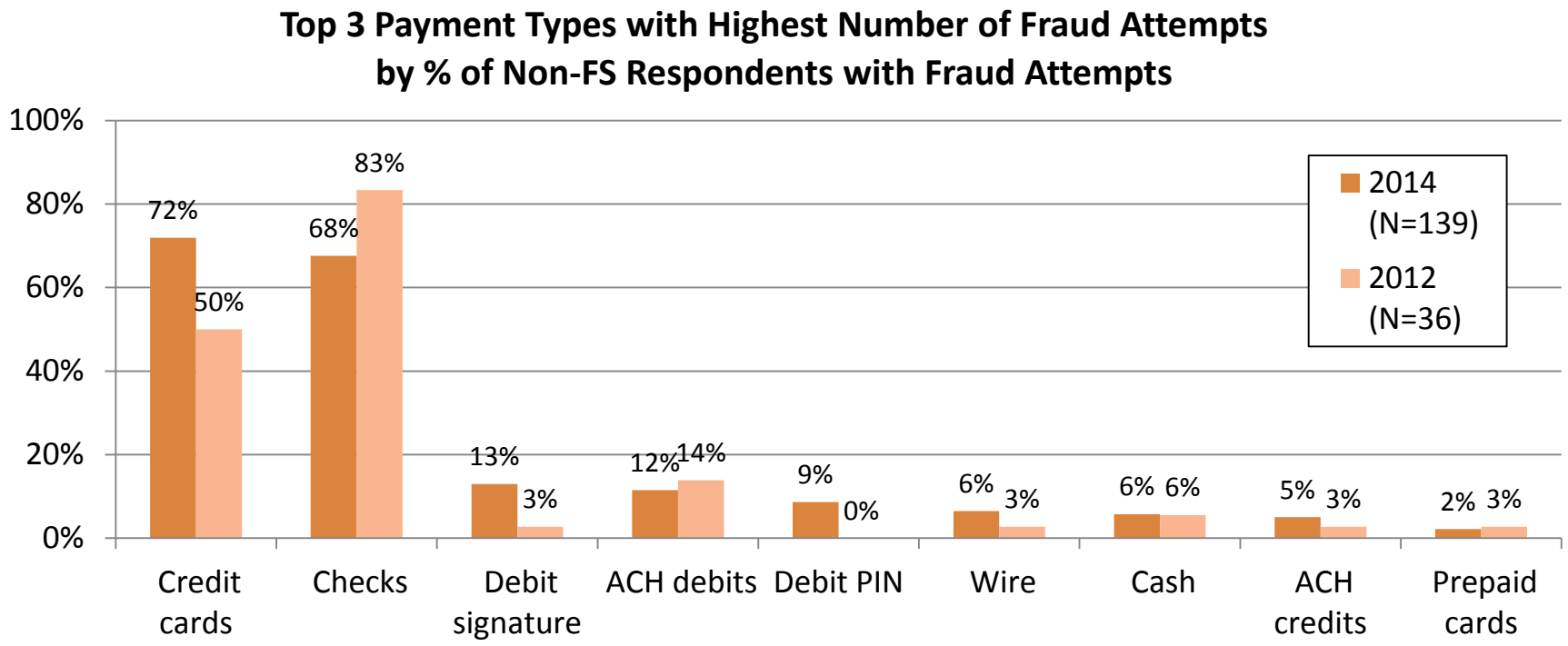
- 87% of FS respondents report signature debit in the top 3 payments with the highest number of fraud attempts
- 75% rank signature debit as the highest; 13% rank PIN debit as the highest

Top 3 Payment Types with Highest Number of Fraud Attempts by % of FS Respondents with Fraud Attempts



Non-FS Firms Are Most Prone to Credit Card & Check Fraud Attempts

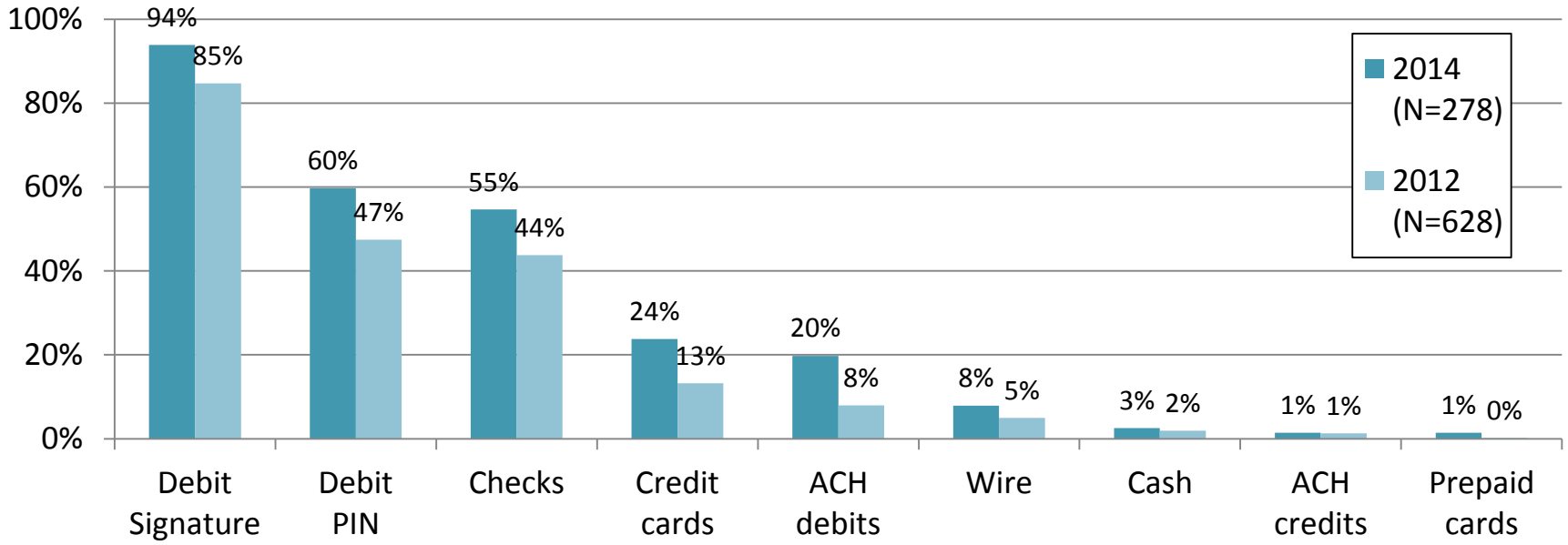
- 72% of non-FS respondents report credit cards in the top 3 payments with the highest number of fraud attempts; 68% report checks
- 50% rank credit cards as the highest; 37% rank check highest



FS Firms Attribute Their Highest Fraud Losses to Debit Cards

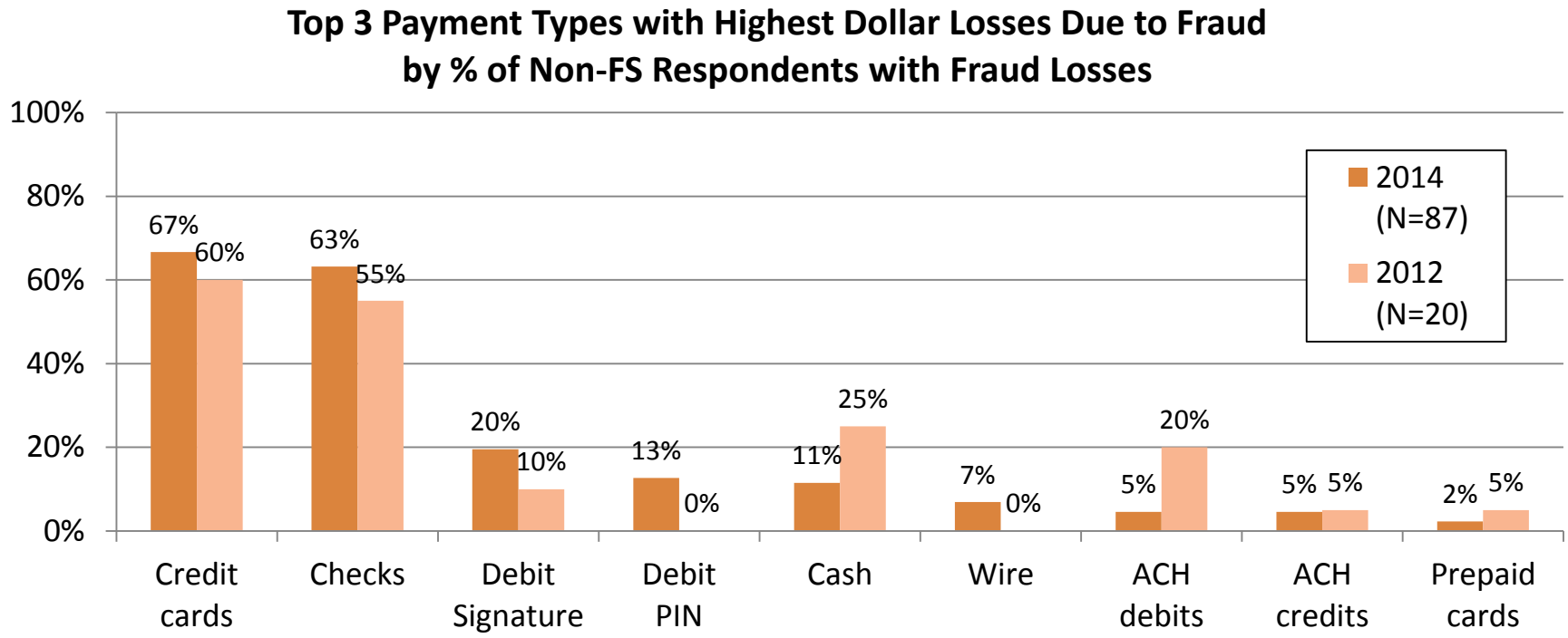
- 94% of FS respondents report signature debit in the top 3 payments with the highest dollar losses; 60% identify PIN debit
- 87% rank debit cards as the highest; 77% say signature debit, 10% say PIN debit

Top 3 Payment Types with Highest Dollar Losses Due to Fraud by % of FS Respondents with Fraud Losses



Non-FS Firms Attribute Their Highest Fraud Losses to Card & Check Fraud

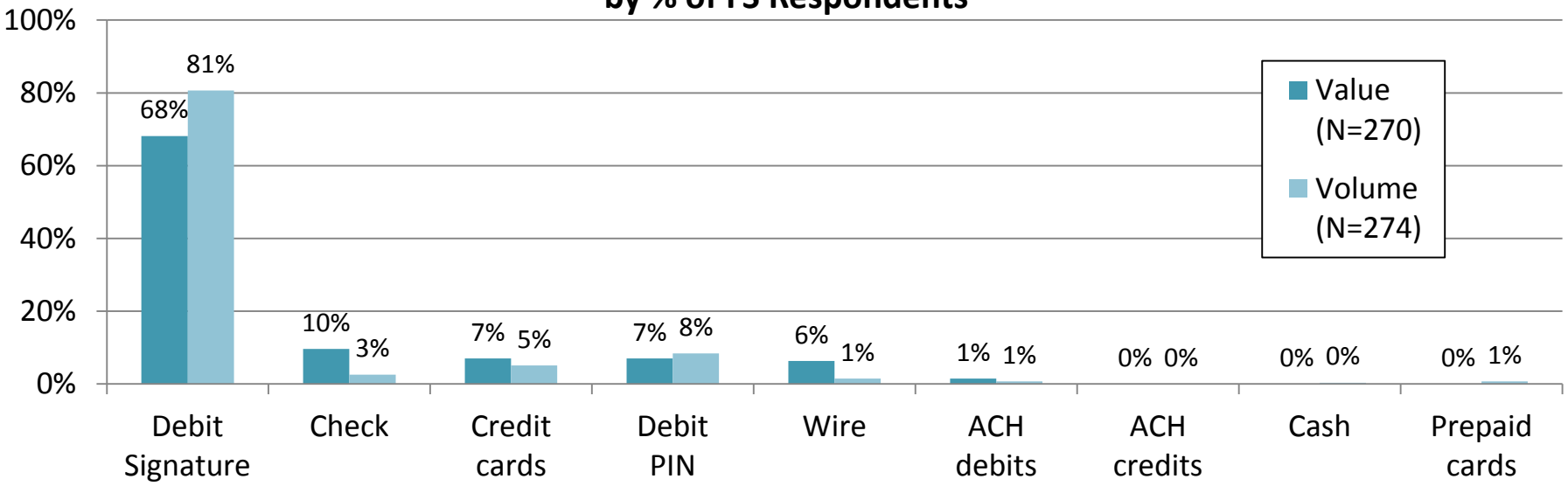
- Over 60% of non-FS respondents report credit cards & checks in the top the payments with the highest losses
- 41% rank credit cards as the highest; 39% rank check highest



Highest Loss Rate by Payment Type

- Based on volume & value of each payment type, FS firms identify signature debit as having the highest loss rate compared to the loss rates of other payments

Payment Type with the Highest Loss Rate Based on Volume & Value of Transactions for Each Payment Type by % of FS Respondents

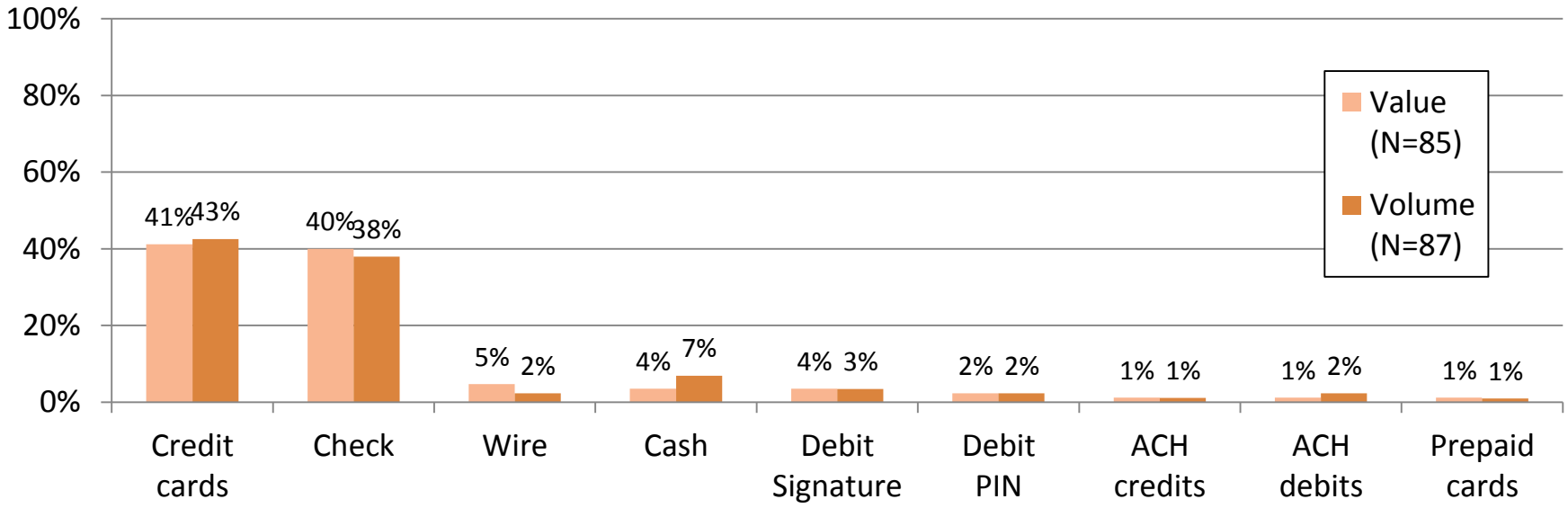


Respondents selected one payment based on value & one payment based on volume

Highest Loss Rate by Payment Type

- Based on volume & value of each payment type, the loss rates on credit cards & checks are equally problematic for non-FS firms

Payment Type with the Highest Loss Rate Based on Volume & Value of Transactions for Each Payment Type by % of Non-FS Respondents



Respondents selected one payment based on value & one payment based on volume

Payments Fraud Losses Are Relatively Low

- In 2013, 70% of respondents have either no losses or a loss rate of 0.3% or less of their annual revenue

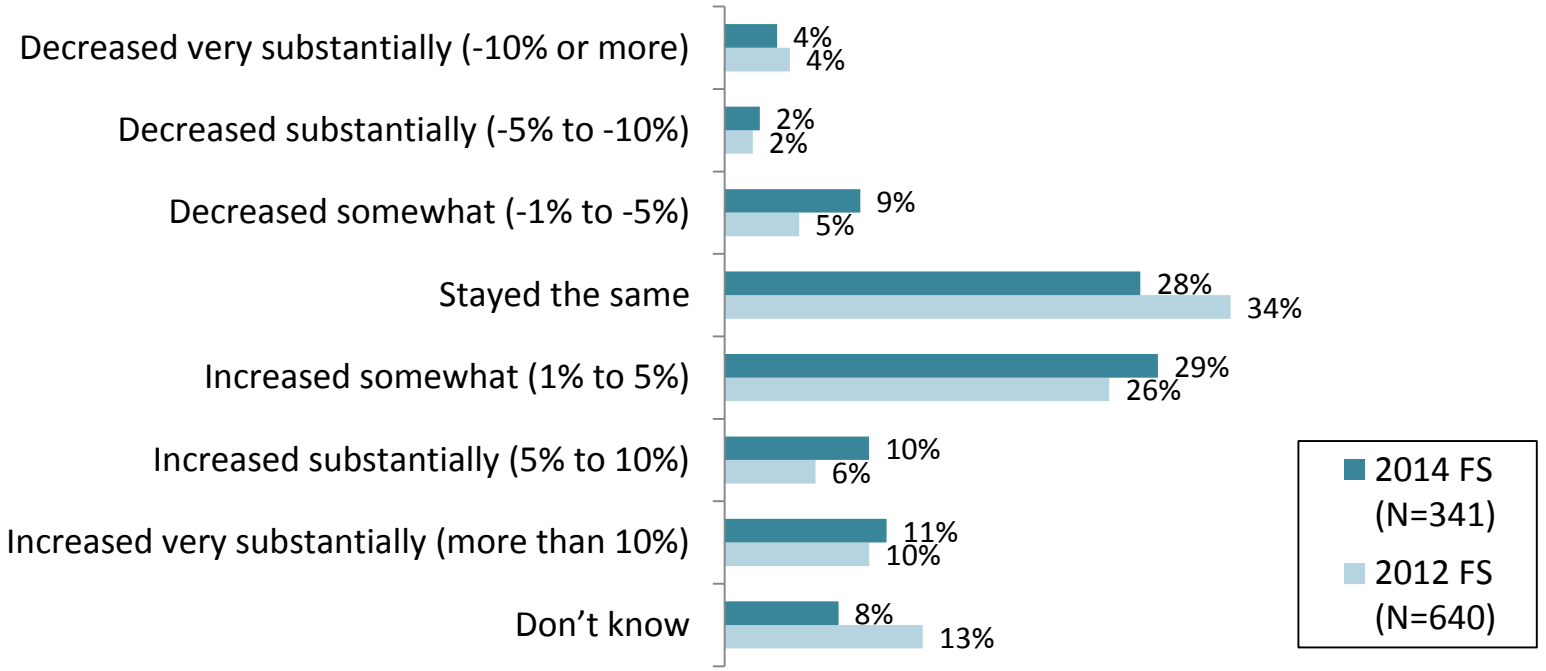
2013 Loss Range as a Percent of Annual Revenue	Financial Service Respondents (N=356)	Non-Financial Service Respondents (N=290)	All Respondents (N=646)
No losses	17%	52%	33%
Over 0% -.3%	49%	23%	37%
.3% - .5%	14%	3%	9%
.6% - 1%	6%	1%	4%
1.1% - 5%	5%	1%	3%
Over 5%	1%	0%	0%
Don't know	8%	19%	13%

There is a small difference in the percentages for “no losses” & “don’t know” in this table compared to charts on page 17 because of the lesser number of respondents (or N) answering the question on the loss rate range

Fraud Loss Trends

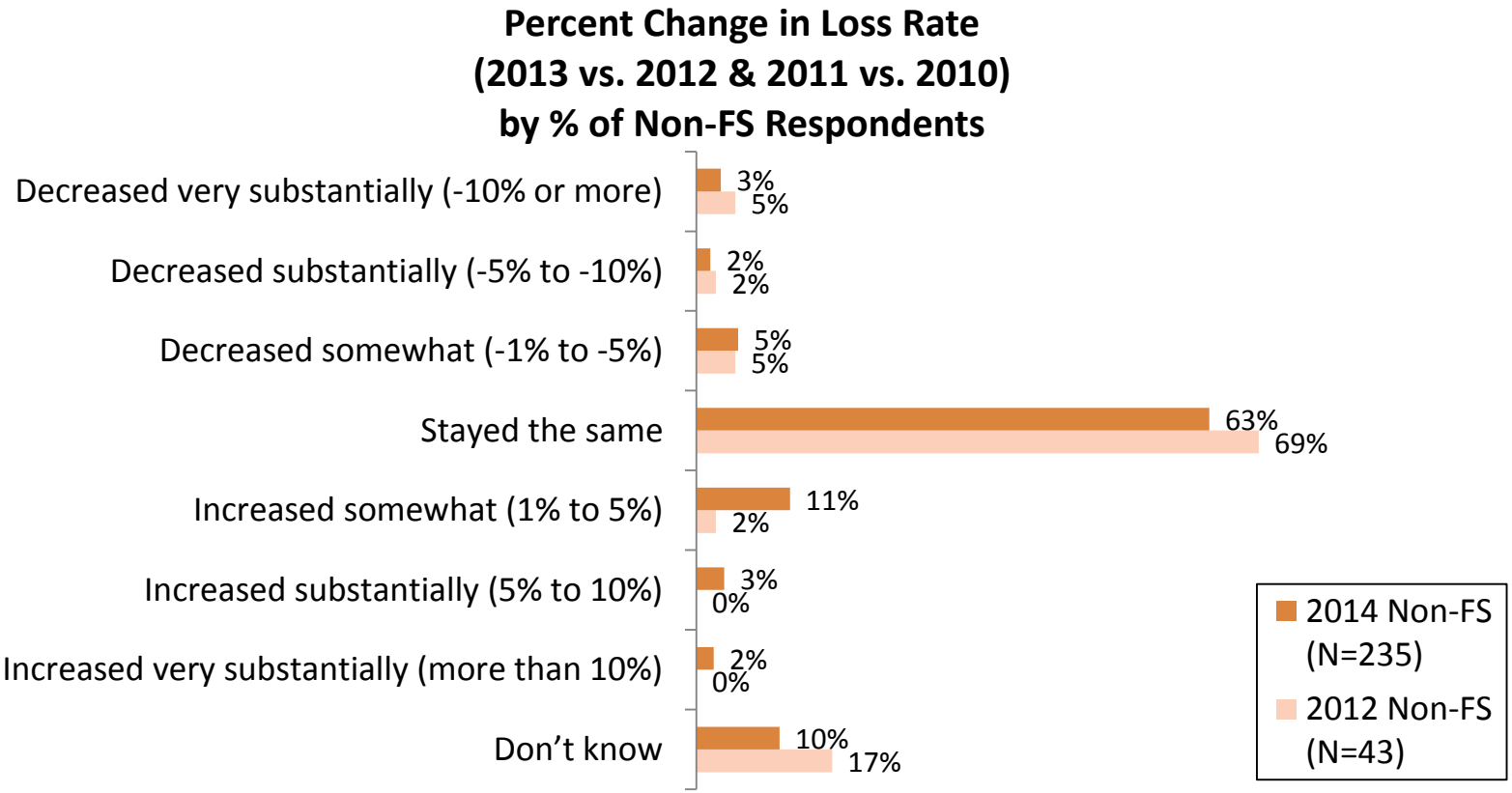
- 50% of the FS respondents report their loss rate increasing in 2013 compared to 2012, 28% report losses stayed about the same, & only 15% report a decrease

Percent Change in Loss Rate
(2013 vs. 2012 & 2011 vs. 2010)
by % of FS Respondents



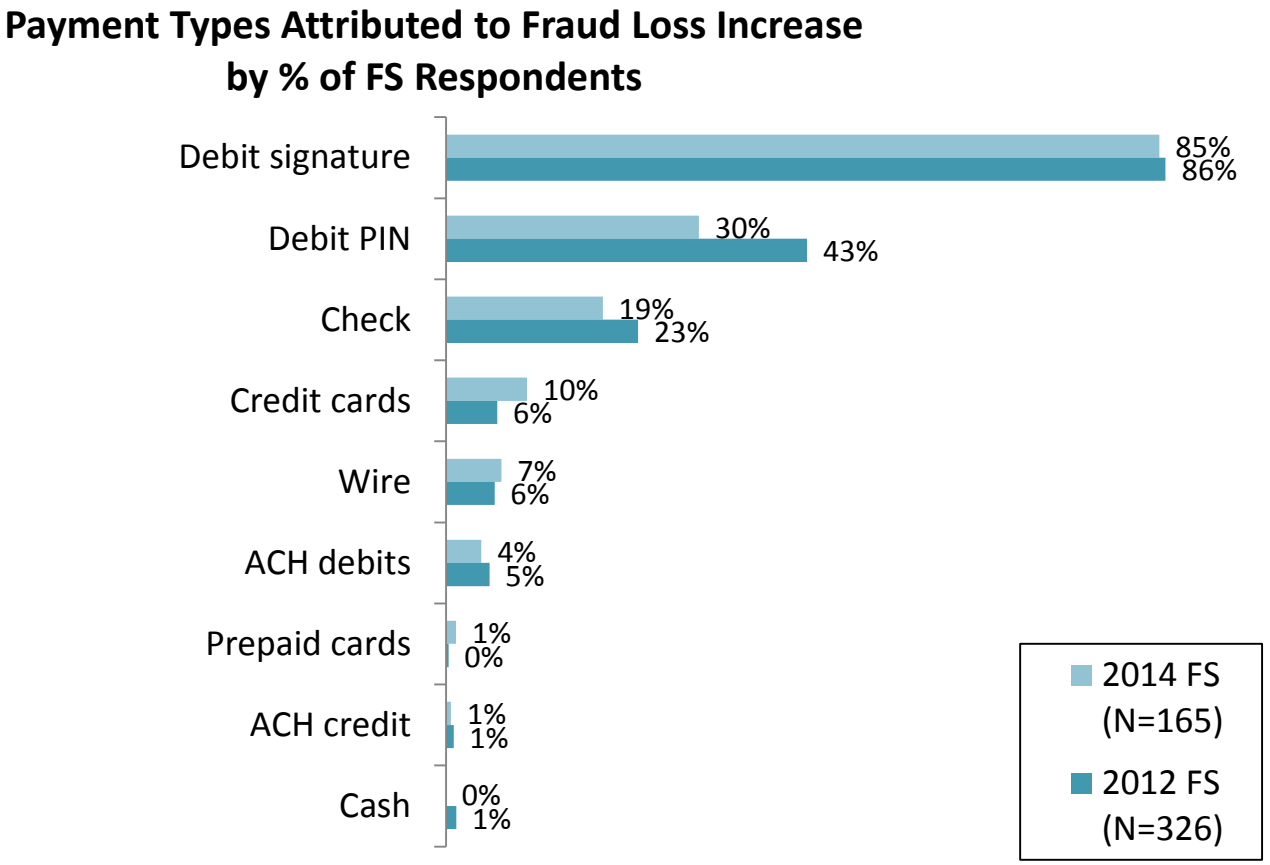
Fraud Loss Trends

- Over 60% of non-FS firms report their loss rate stayed about the same in 2013 compared to 2012, 17% report an increase, & 10% report a decrease



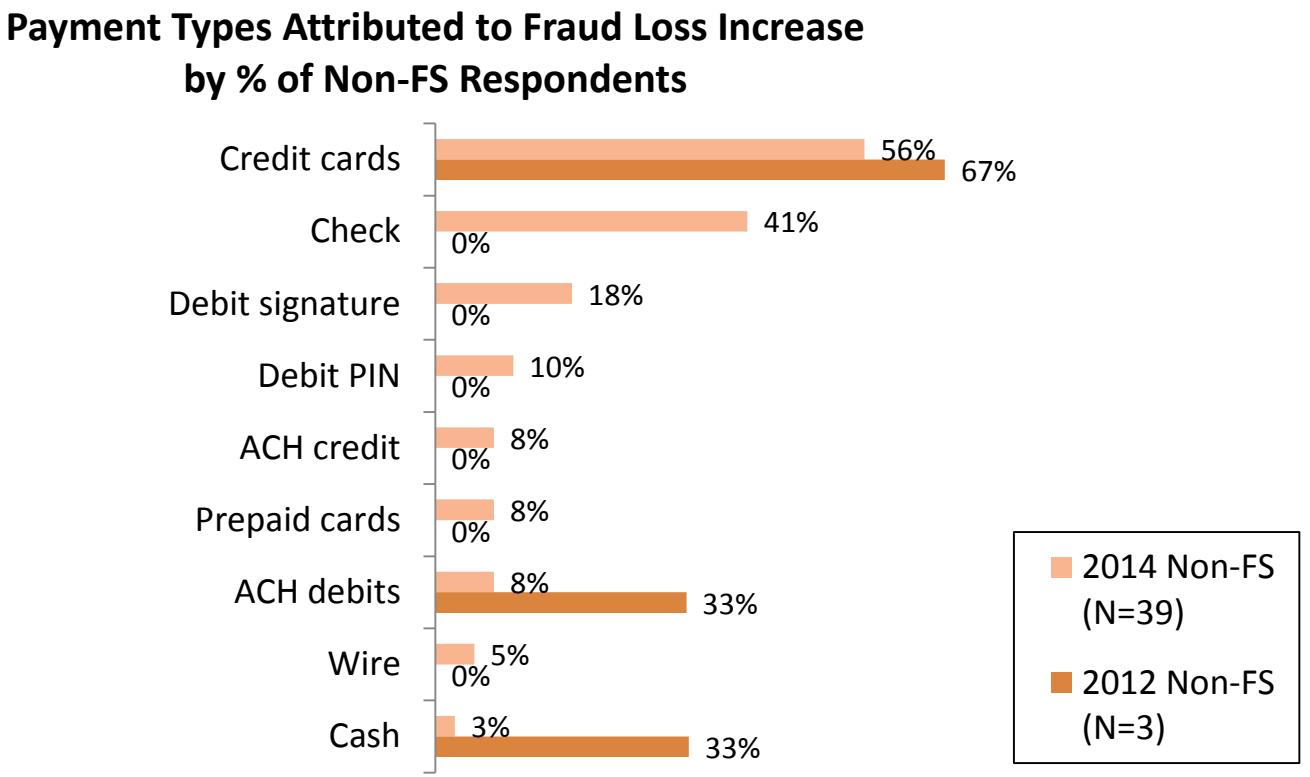
Payment Types Attributed to Loss Rate Increases

- The vast majority of FS respondents attribute increased losses to signature debit cards



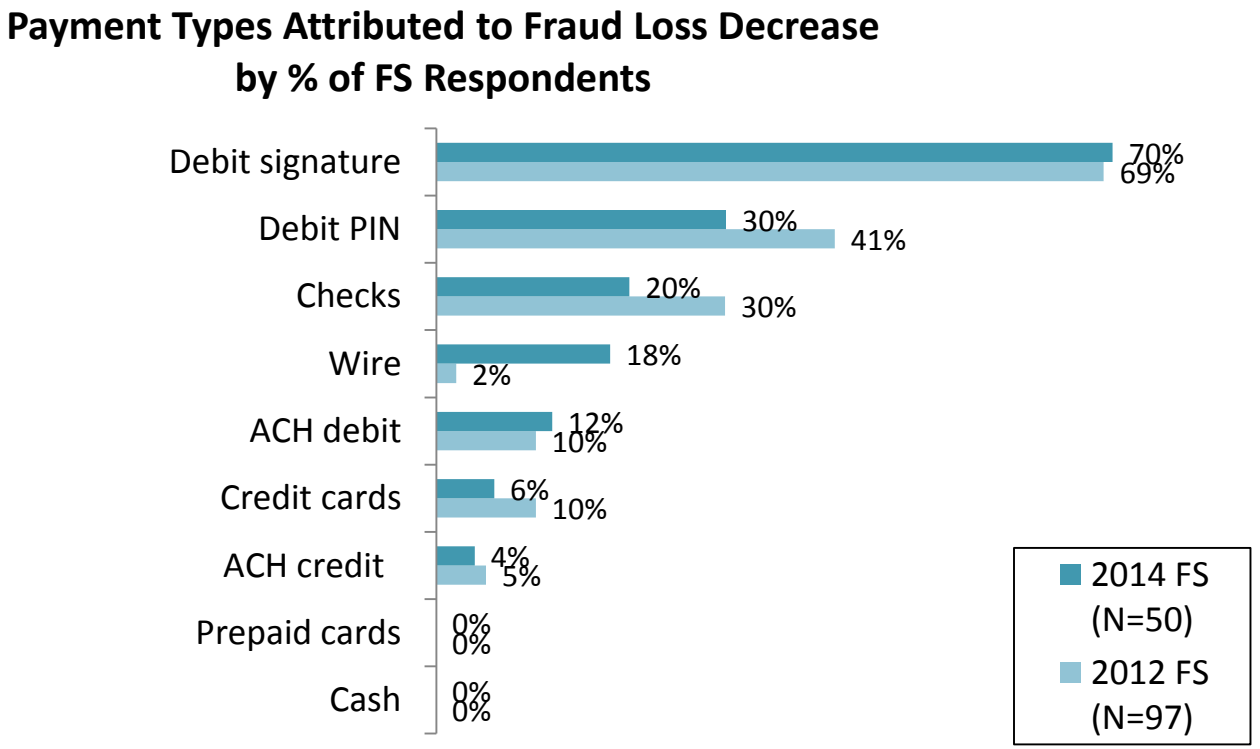
Payment Types Attributed to Loss Rate Increases

- Non-FS respondents indicate credit card & checks losses among payments causing a rise in their loss rate; keep in mind only a few non-FS respondents reported an increase in losses in the past two surveys



Payment Types Attributed to Loss Rate Decreases

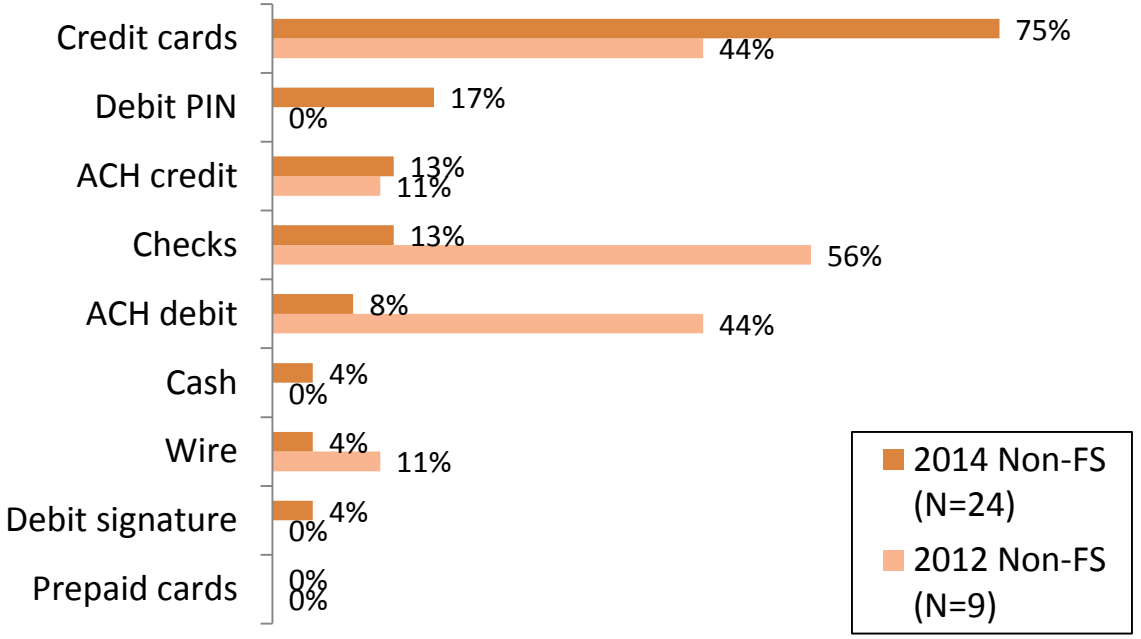
- Lower loss rates are attributed to reductions in debit cards losses
- This finding seems to indicate that fraud prevention strategies implemented by these organizations are working to reduce losses on payments with the highest losses



Payment Types Attributed to Loss Rate Decreases

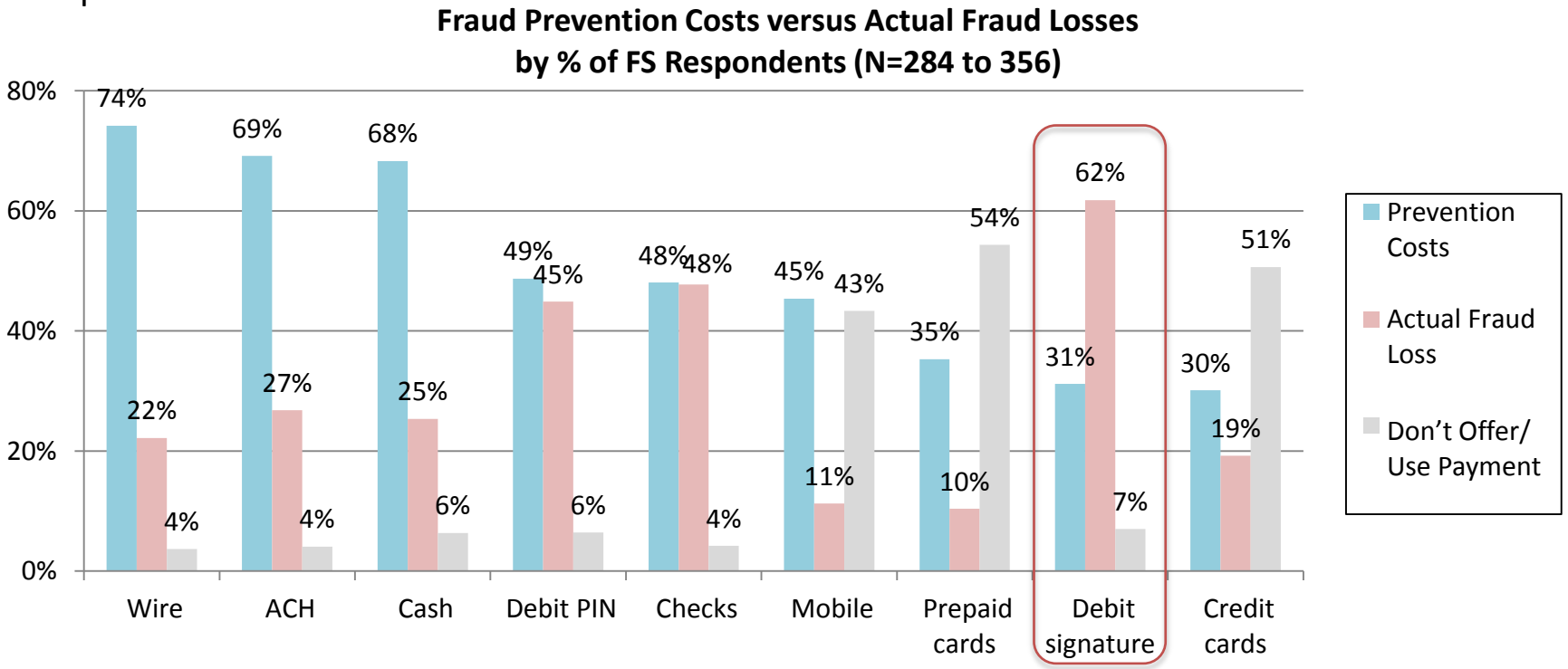
- In the 2014 survey, lower loss rates in 2013 compared to 2012 are attributed to credit card payments by 75% non-FS respondents with decreased loss rates
- This finding suggests that non-FS respondents are focusing on measures to reduce card losses

Payment Types Attributed to Fraud Loss Decrease
by % of Non-FS Respondents with a Lower Loss Rate



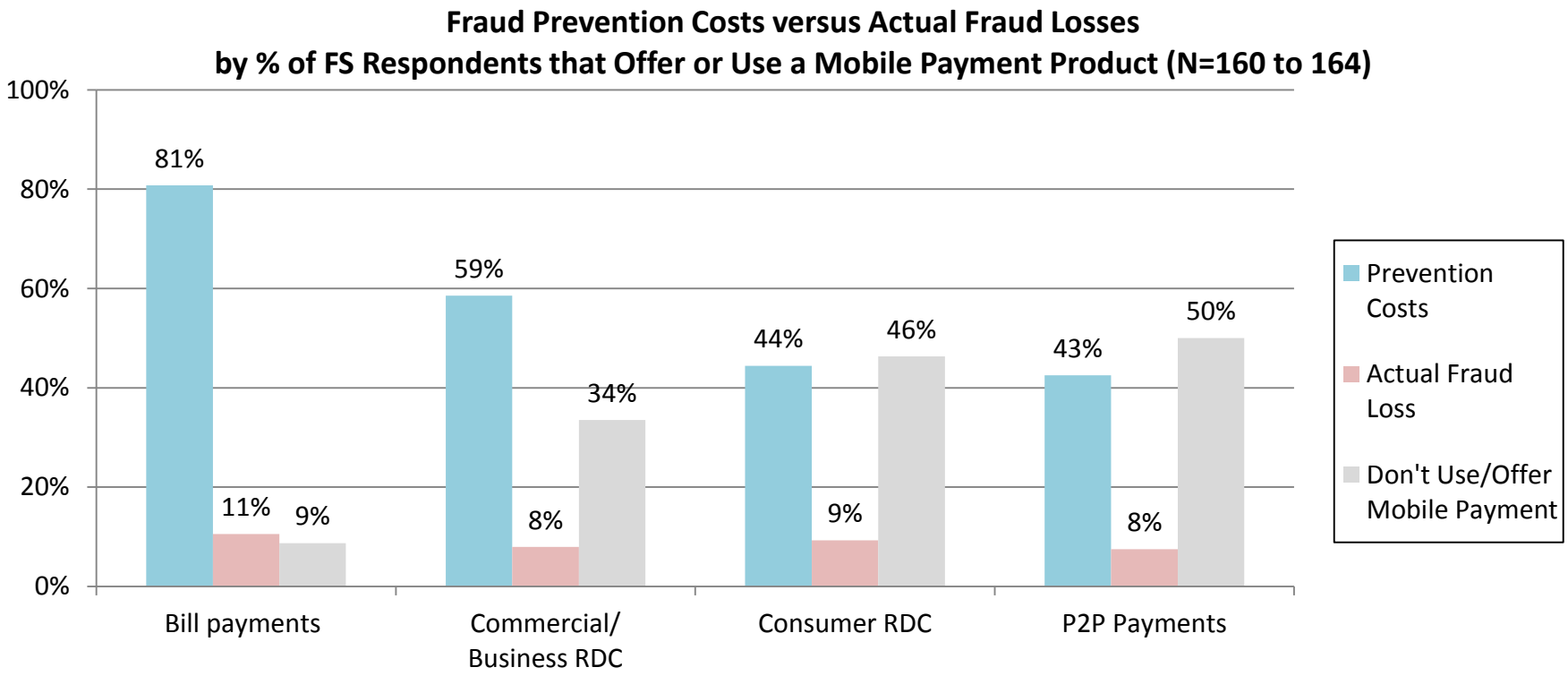
Prevention Costs versus Actual Fraud Losses

- For most payment types, FS investments in fraud prevention exceed actual losses with one exception; signature based debit cards
- Nearly half of the FS respondents report that Debit PIN & check fraud losses exceed prevention costs



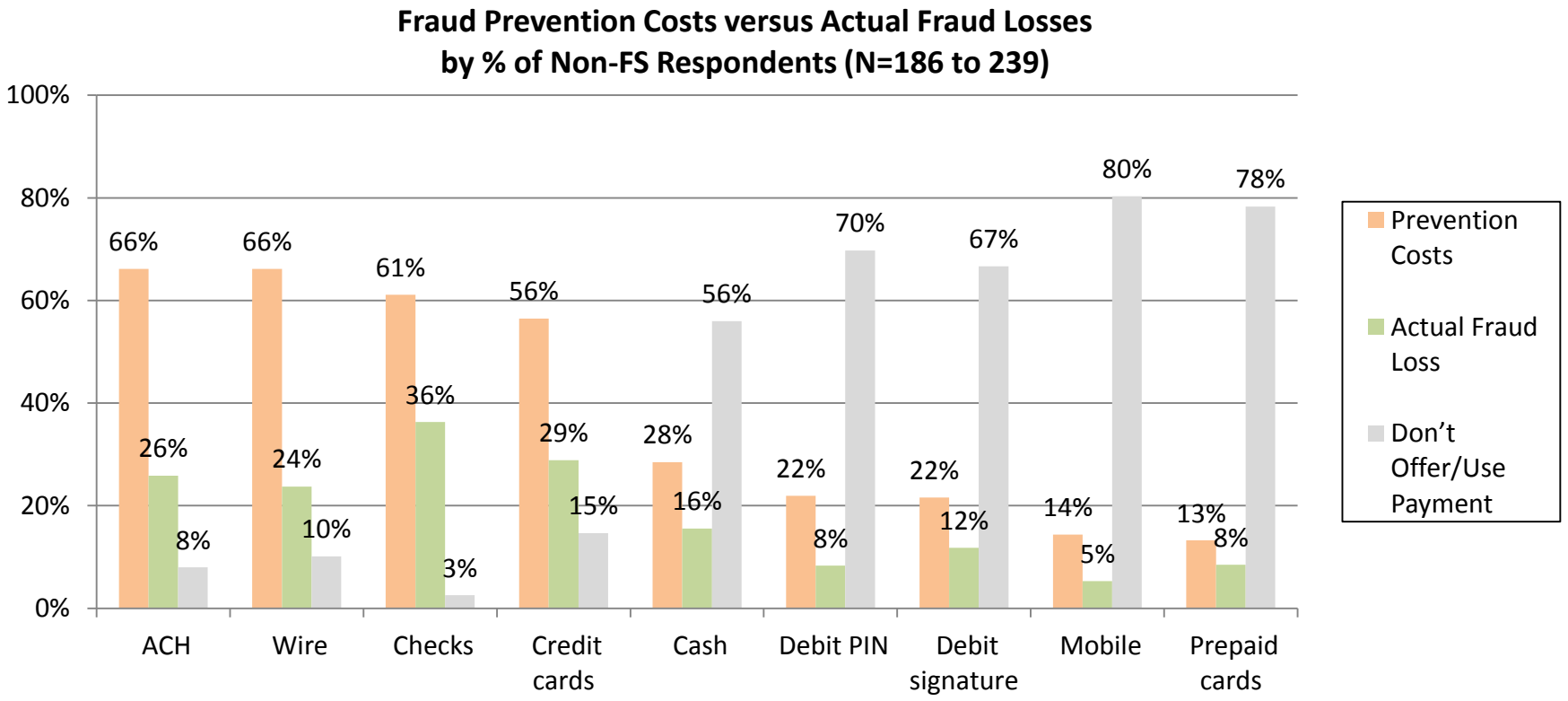
Prevention Costs versus Actual Fraud Losses - Mobile Payment Products

- Most FS respondents that offer mobile payment products report higher prevention costs than actual losses



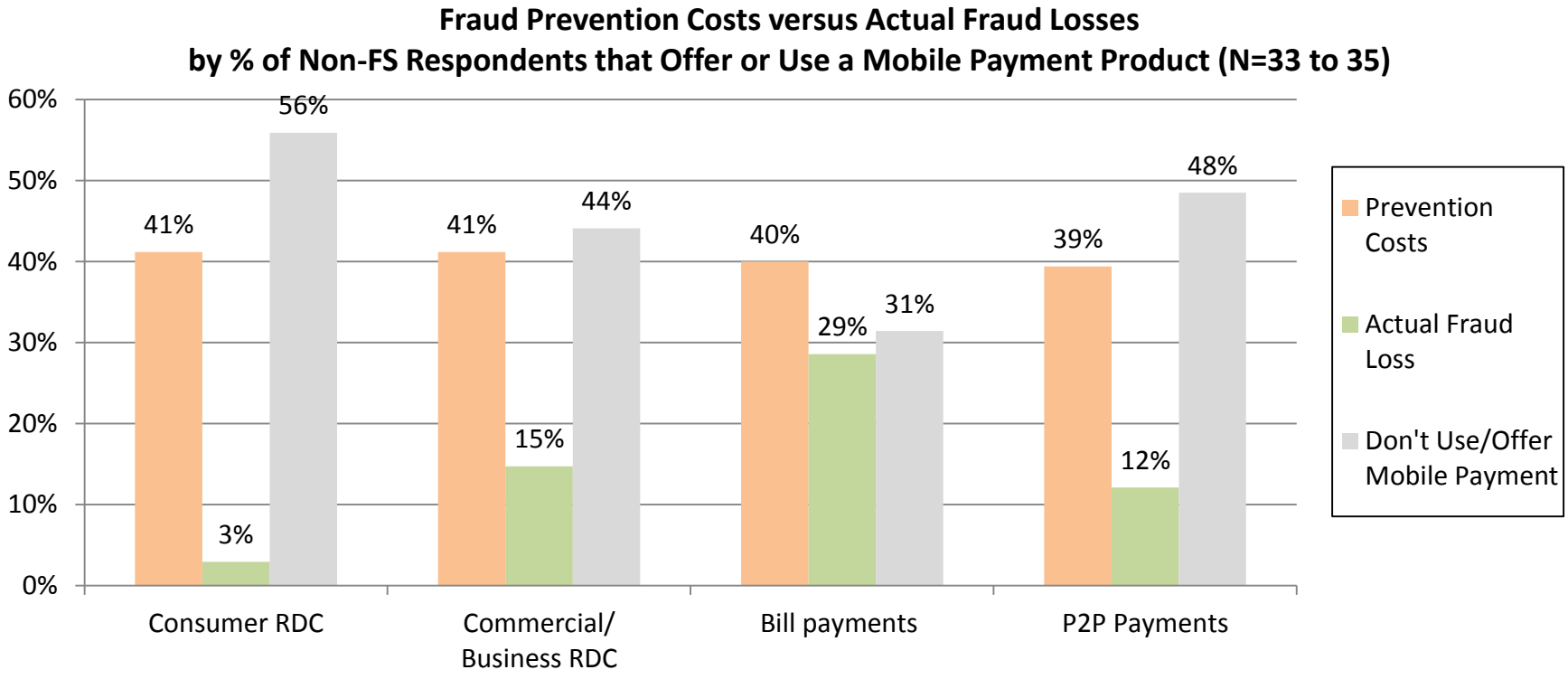
Prevention Costs versus Actual Fraud Losses

- For every payment type, a higher percentage of non-FS firms respond that prevention costs exceed actual losses



Prevention Costs versus Actual Fraud Losses - Mobile Payment Products

- Non-FS firms are more likely to report higher losses than prevention costs in two categories: mobile bill payments (29%) & commercial RDC products (15%)



Investments in Payments Fraud Mitigation

- 63% of respondents report they had implemented changes to payment risk management that led to a decrease in losses or helped to control fraud losses

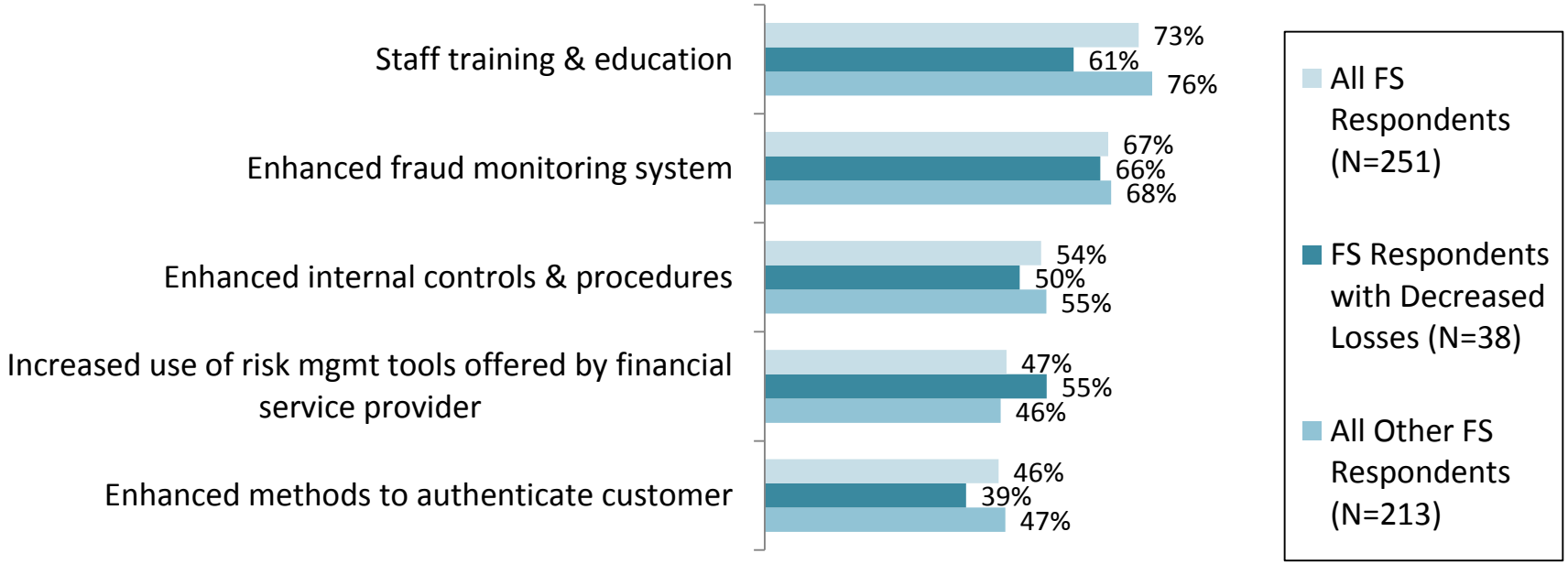
Implemented Key Changes to Payments Risk Management Practices (by % of Respondents)

Made Key Changes to Risk Management Practices	Percent of Organizations with Decreased Losses		Percent of All Other Organizations		Percent of All Respondents
	Financial Services (N=51)	Non-Financial Services (N=24)	Financial Services (N=111)	Non-Financial Services (N=82)	All Respondents (N=657)
Yes	76%	67%	67%	54%	63%
No	22%	29%	33%	46%	37%
Don't Know	2%	4%	na	na	<1%

Controlling Fraud Losses FS Respondents

- Changes are being made on multiple fronts

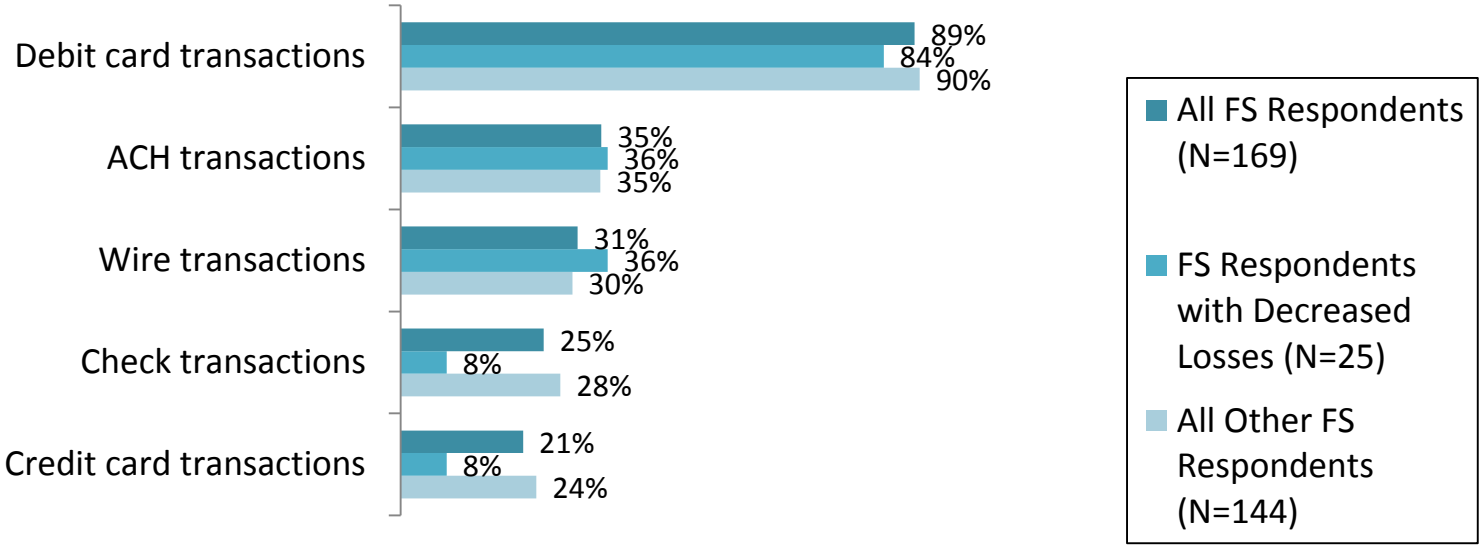
Key Changes Made to Payments Risk Management Practices by % of FS Respondents that Made Changes



Enhanced Fraud Monitoring Systems

- About 9 out of 10 FS respondents that enhanced fraud monitoring systems applied them to debit card transactions

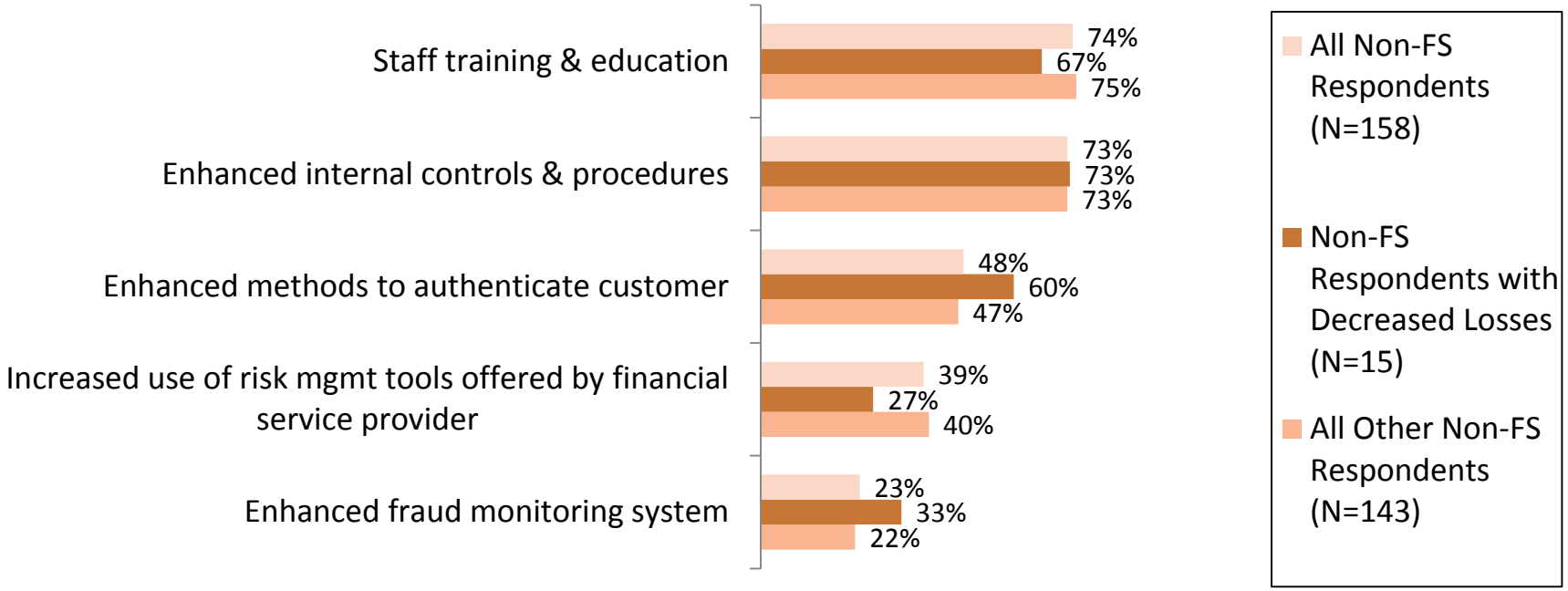
Payments to Which Enhanced Fraud Monitoring Applies by % of FS Respondents



Controlling Fraud Losses Non-FS Respondents

- Nearly 3 out of 4 Non-FS respondents report changes made to staff training & education & internal controls & procedures

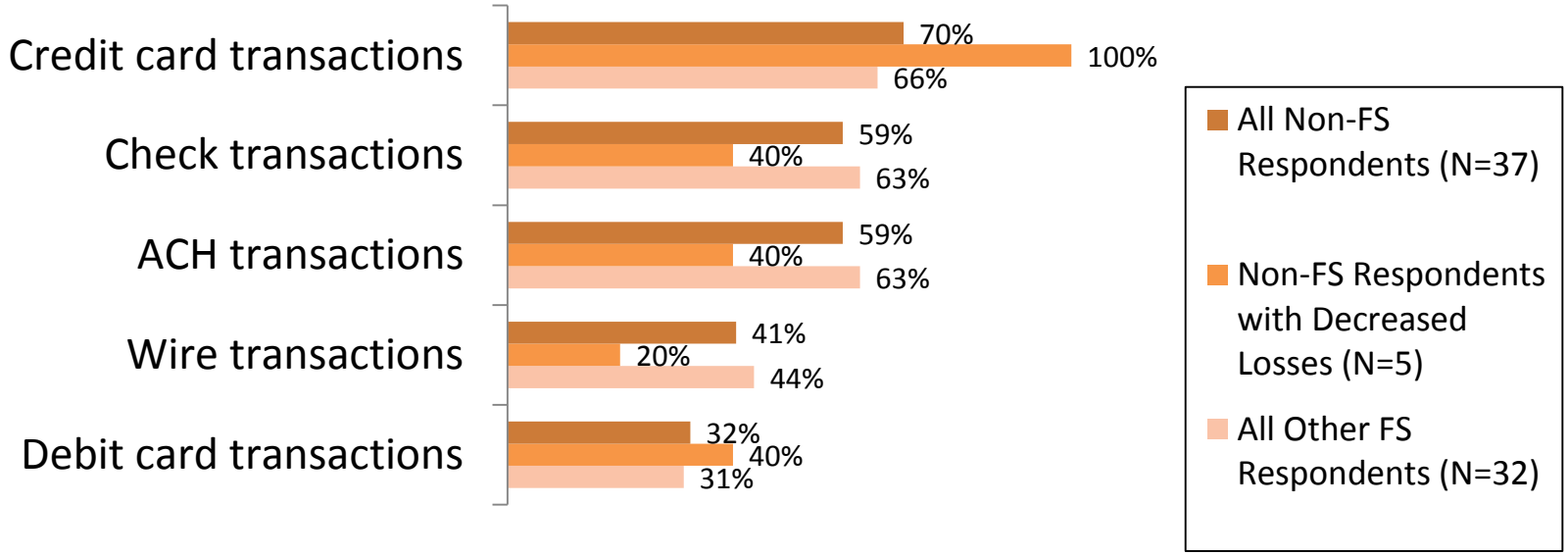
Key Changes Made to Payments Risk Management Practices by % of FS Respondents that Made Changes



Enhanced Fraud Monitoring Systems

- Although a smaller share of Non-FS firms (23%) indicated that they enhanced fraud monitoring systems, those that did, apply them to multiple transaction types

Payments to Which Enhanced Fraud Monitoring Applies by % of Non-FS Respondents

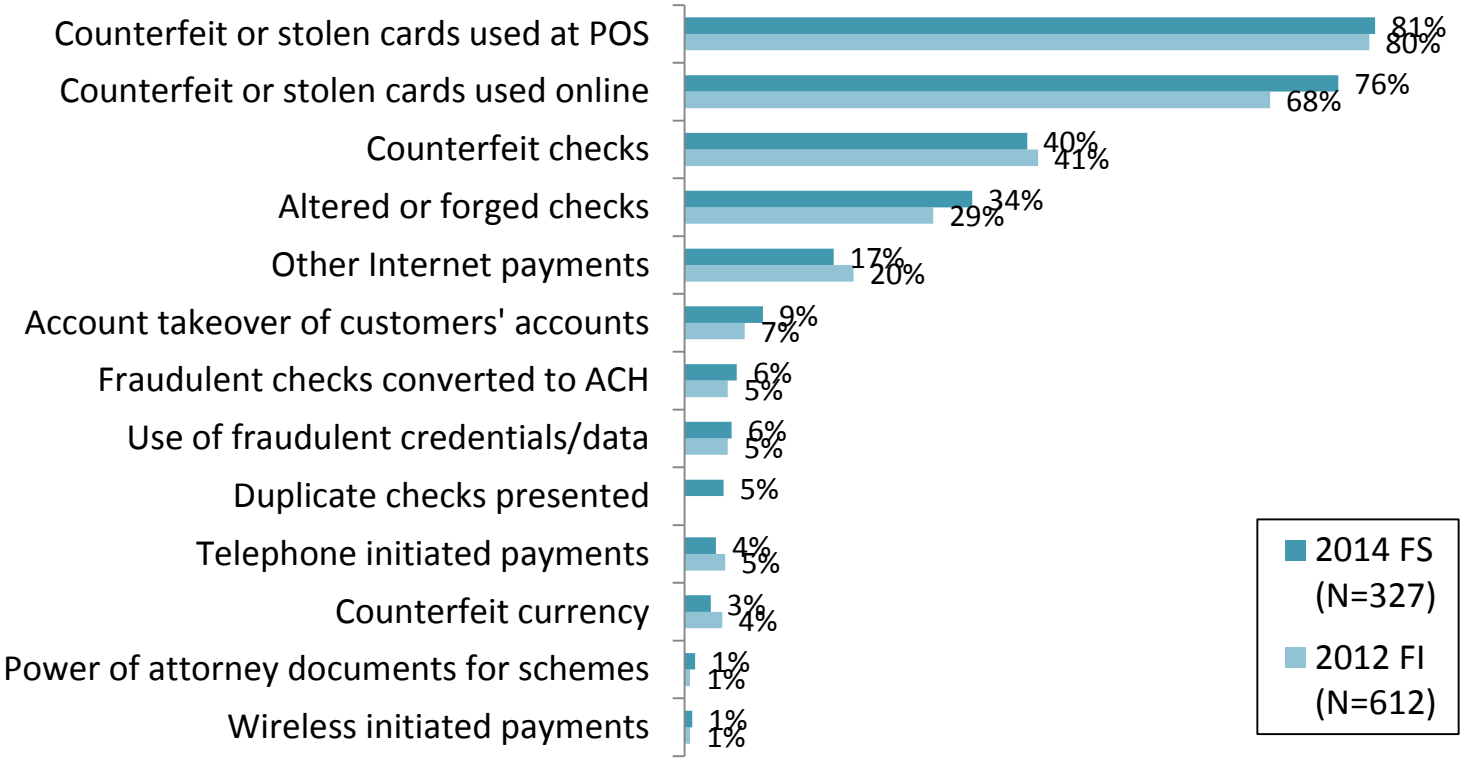


Fraud Schemes

Most Used Fraud Schemes Involving FS Customers' Accounts

- Most used schemes are counterfeit or stolen cards used at point-of-sale (POS) or online
- Top schemes have shown little change since the 2012 survey

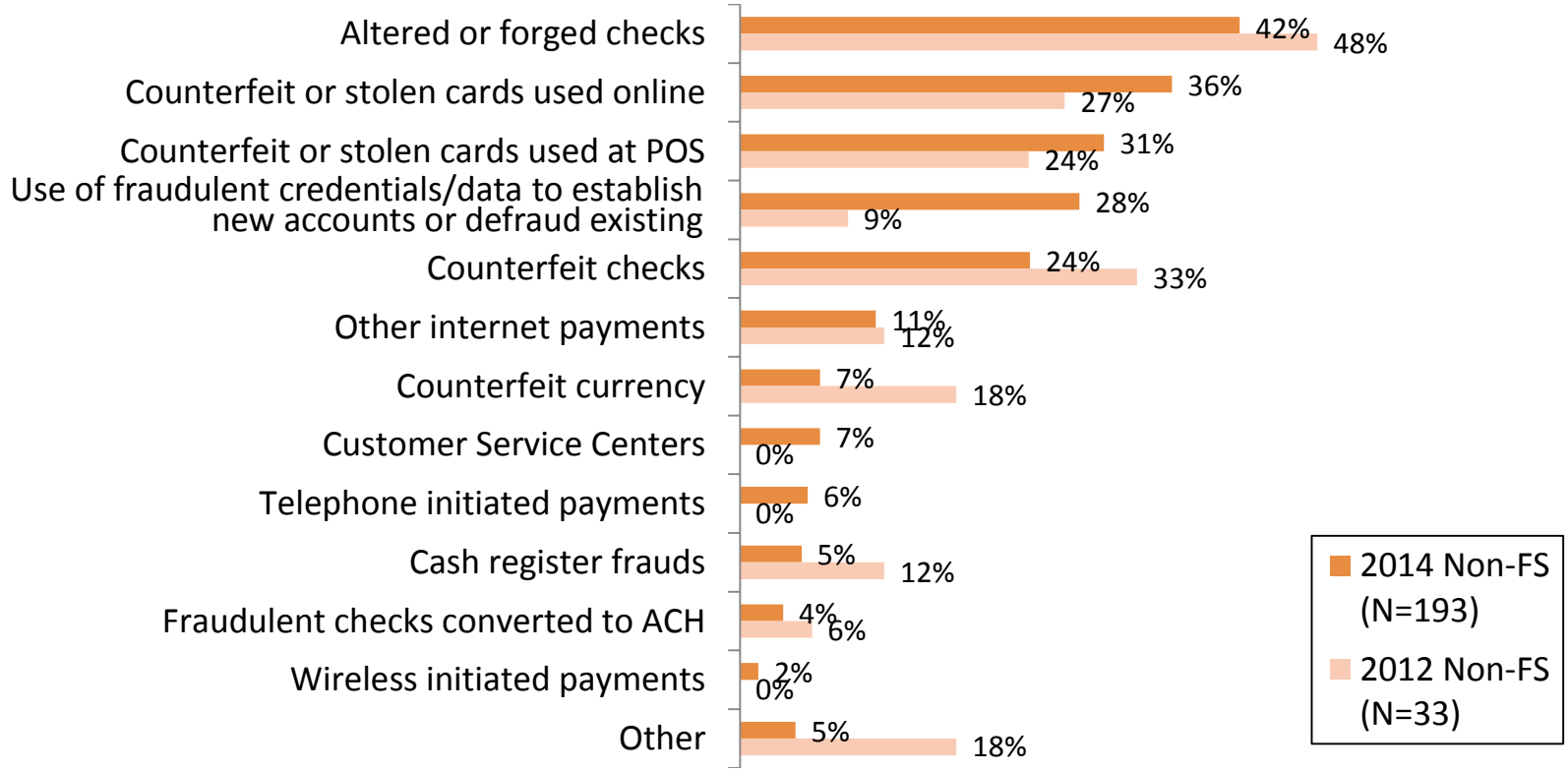
Top 3 Current Fraud Schemes Most Often Used Involving Payments by or on Behalf of Financial Services Customers by % of FS Respondents



Most Used Fraud Schemes Involving Payments Received

- For payments received by non-FS firms, altered or forged checks continue to be common schemes
- The share of non-FS respondents reporting the fraudster use of fraudulent credentials or data to establish new accounts or defraud existing increased to 28% in 2014, compared to 9% in 2012

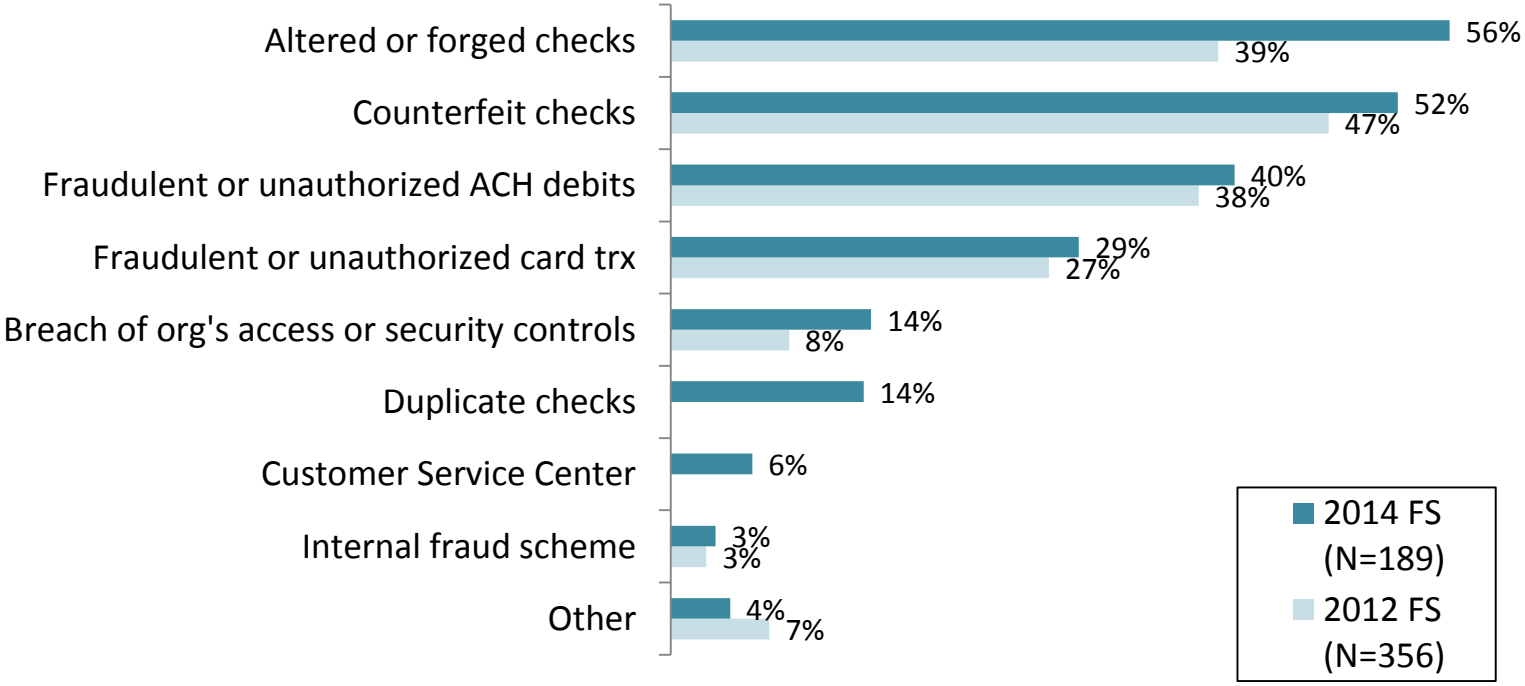
Top 3 Current Fraud Schemes Most Used Involving Payments Accepted by % of Non-FS Respondents



Most Used Fraud Schemes Against Organization's Own Banking Accounts

- Altered or forged & counterfeit check schemes are most common against FS respondent's own banking accounts

Top 3 Fraud Schemes Most Used Against Organization's Own Banking Accounts by % of FS Respondents

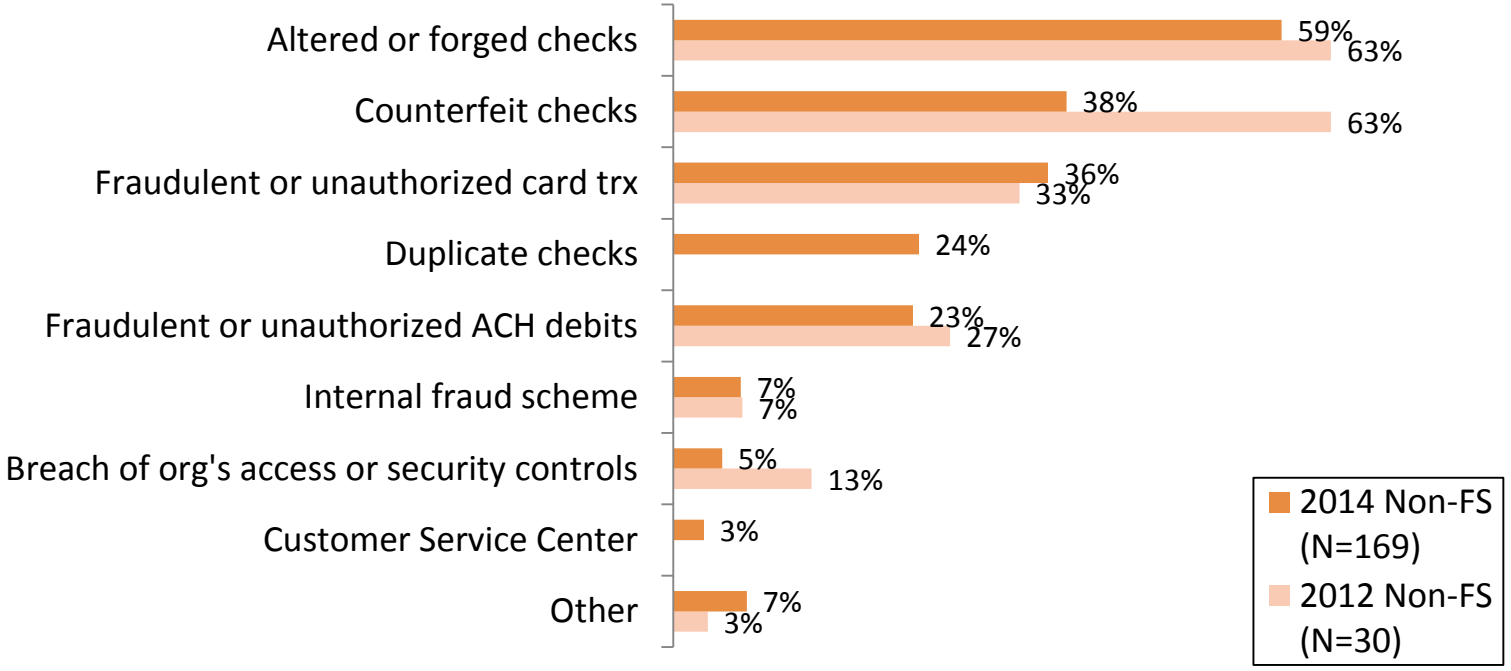


Schemes with no value for the % in 2012 were new choices in 2014

Most Used Fraud Schemes Against Organization's Own Banking Accounts

- Altered or forged & counterfeit check schemes are most common against non-FS firm's own banking accounts too

Top 3 Fraud Schemes Most Used Against Organization's Own Banking Accounts by % of Non-FS Respondents



Schemes with no value for the % in 2012 were new choices in 2014

Source of Data Used in Schemes

- "Sensitive" information obtained from lost or stolen card, check, or other physical document or device while in consumer's control is identified as the top source of information used in schemes, although this information source declined from the previous survey
- For first time, respondents could choose “Unknown” as a top information source, & two out of five respondents report the information source is unknown; this shows that organizations often remain unaware of the nature of the information compromise that led to successful payments fraud

Top 3 Information Sources Used in Payments Fraud Schemes	2014			2012		
	FS (N=310)	Non-FS (N=191)	All Org. (N=501)	FS (N=590)	Non-FS (N=33)	All Org. (N=623)
"Sensitive" information obtained from lost or stolen card, check, or other physical document or device while in consumer's control	45%	30%	40%	64%	39%	63%
Unknown	34%	47%	39%	na	na	na
Email & webpage cyber attacks to obtain "sensitive" customer information , e.g., phishing, spoofing & pharming	35%	24%	31%	33%	21%	32%
Physical device tampering e.g., use of skimmer on POS terminal to obtain magnetic stripe information	37%	10%	27%	38%	3%	36%
Data breach due to computer hacking	34%	9%	25%	26%	15%	25%
Organization's information obtained from a legitimate check issued by your organization	18%	35%	25%	17%	67%	20%
Information about customer obtained by family or friend	25%	9%	19%	24%	3%	23%
Social engineering	14%	10%	12%	na	na	na
Employee with legitimate access to organization or customer information	2%	9%	5%	1%	18%	2%
Lost or stolen physical documentation or electronic devices while in control of the organization	1%	6%	3%	3%	9%	3%

Perpetrators Involved in Successful Payments Fraud

- Respondents continue to report external parties as the main perpetrators of successful payments fraud
- In the 2014 survey, 74% of respondents report external parties are responsible for 100% of the payments fraud against their organization; this is up from 2012

Portion of Successful Fraud by Perpetrators Involved
By % of Respondents with Payment Fraud Losses

Perpetrator Category	2014 (N=270)					2012 (N=627)				
	100%	76% - 99%	51% - 75%	26% - 50%	1% - 25%	100%	76% - 99%	51% - 75%	26% - 50%	1% - 25%
Internal Only	2%	2%	1%	0%	4%	2%	2%	2%	4%	4%
Internal w/External Parties	1%	0%	1%	2%	4%	3%	0%	1%	5%	4%
External Only	74%	5%	3%	2%	1%	58%	7%	2%	3%	4%
Could Not Determine	4%	1%	0%	1%	6%	8%	1%	1%	2%	6%

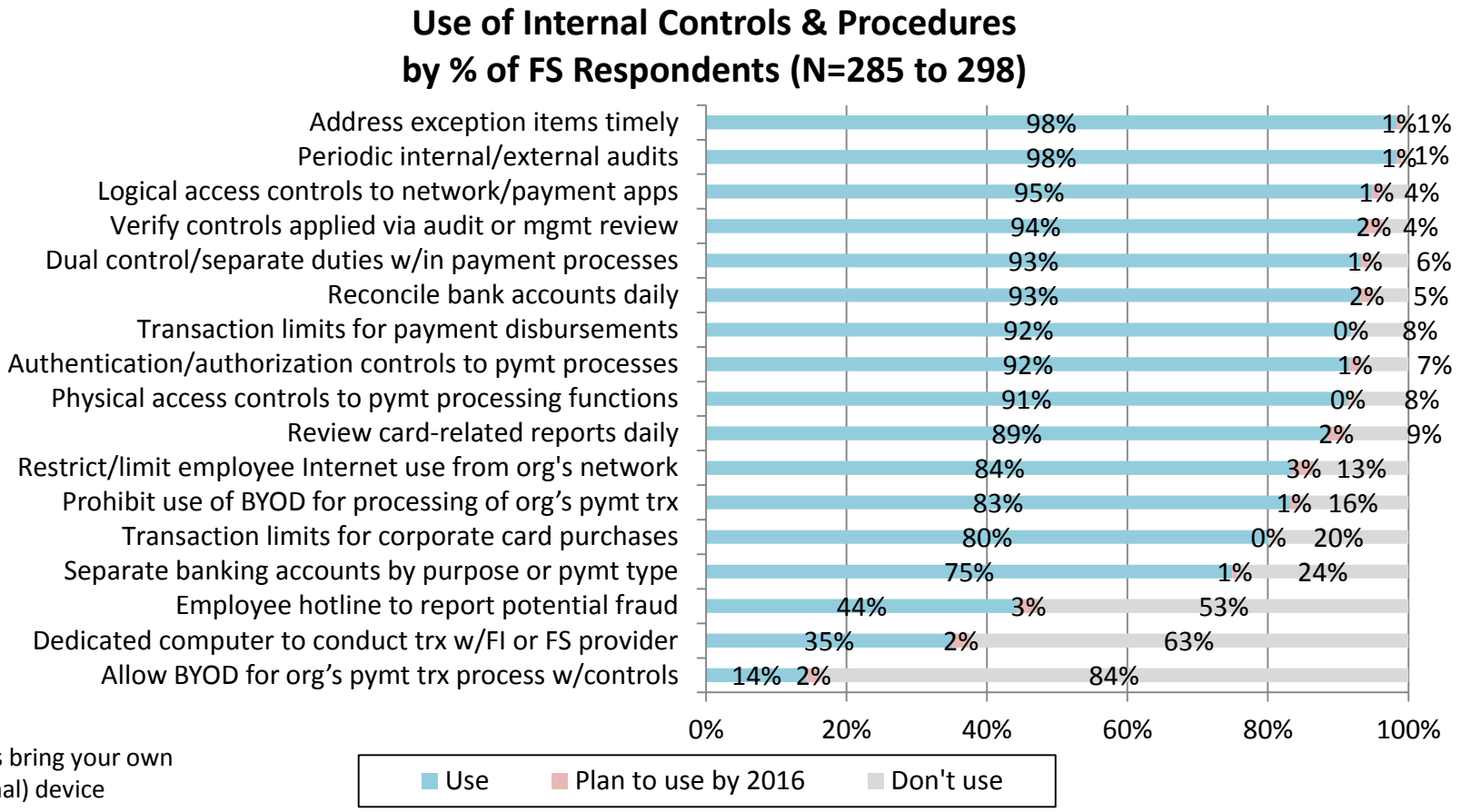
Risk Mitigation

Risk Mitigation

- In order to keep up with the constantly evolving strategies that criminals use to commit payments fraud, firms must be vigilant in developing & implementing a variety of strategies to prevent fraud from occurring & lessen its impact in cases when it is successful
- For the purposes of this survey, fraud mitigation strategies are broken down into four categories & the relative effectiveness is captured
- These categories are:
  1. Internal controls & procedures
  2. Customer authentication methods
  3. Transaction screening & risk management methods
  4. Risk mitigation services provided by FS organizations

Use of Internal Controls & Procedures by FS Respondents

- FS respondents are heavy users of Internal controls & procedures

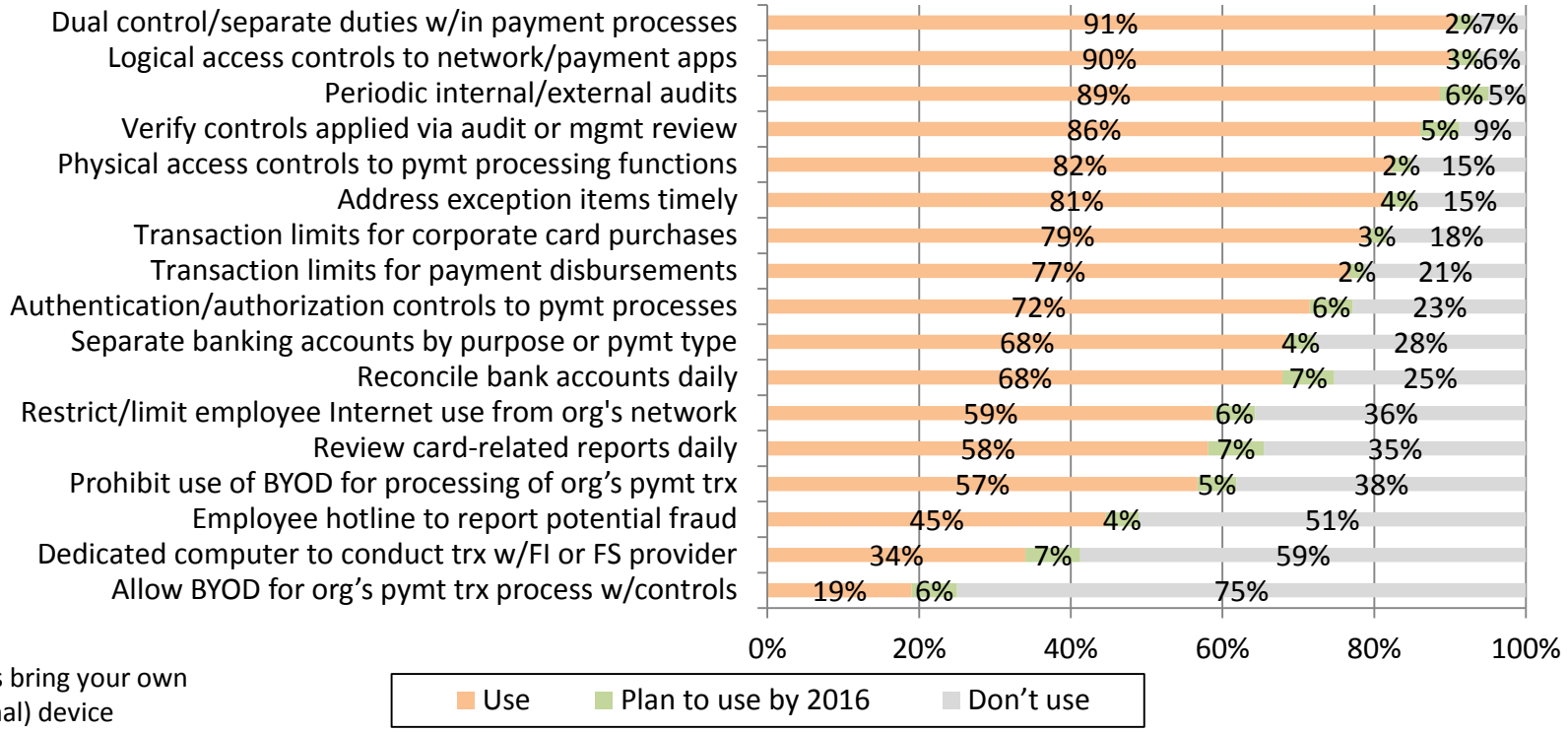


BYOD is bring your own (personal) device

Use of Internal Controls & Procedures by Non-FS Respondents

- While non-FS firms are somewhat less likely to use these internal controls, usage rates are still high

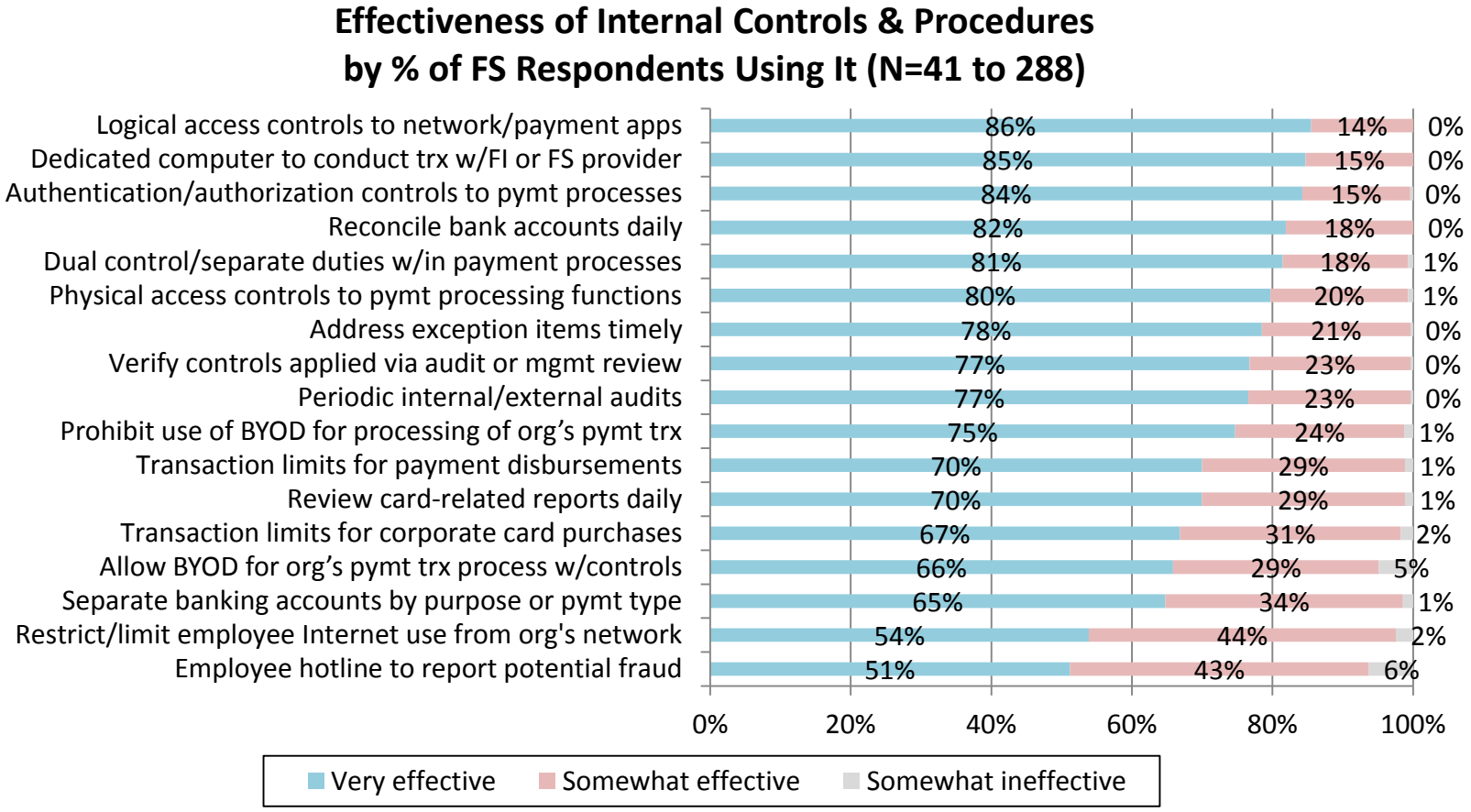
Use of Internal Controls & Procedures by % of Non-FS Respondents (N=184 to 204)



BYOD is bring your own (personal) device

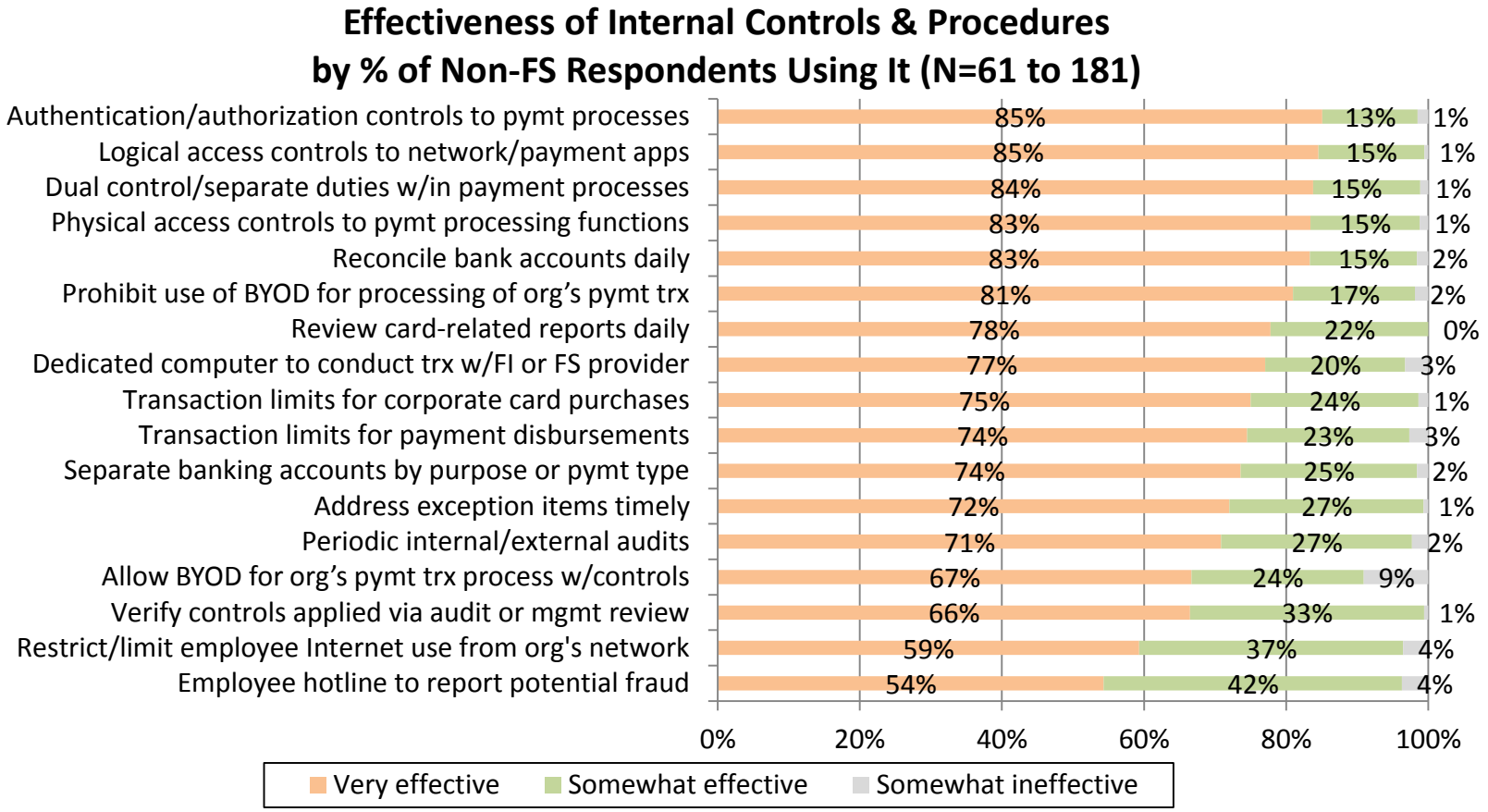
Effectiveness of Internal Controls & Procedures Rated by FS Respondents

- Over 2/3 of FS respondents rate 14 of the 17 tools as very effective



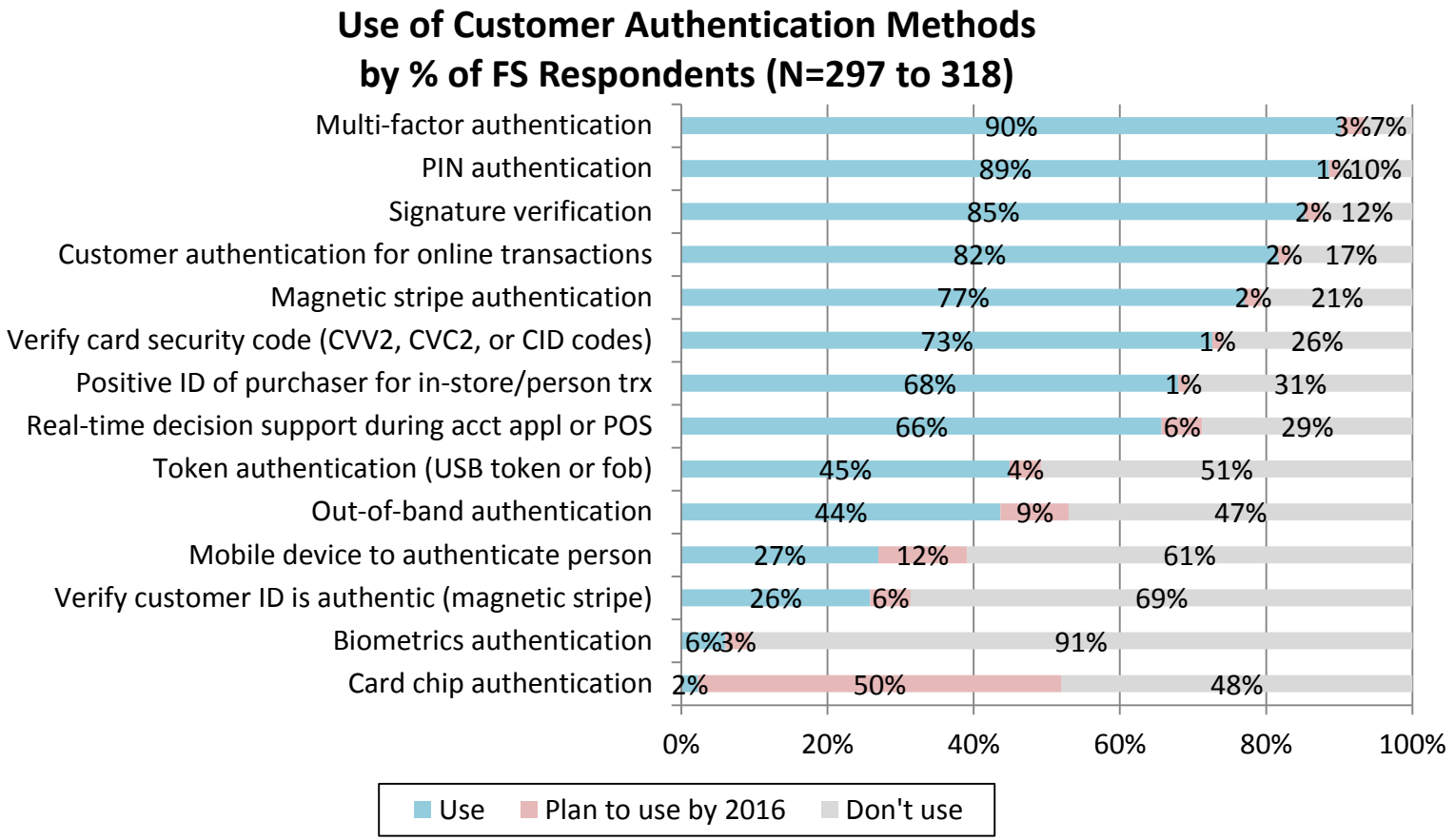
Effectiveness of Internal Controls & Procedures Rated by Non-FS Respondents

- 2/3 of non-FS firms rate 15 of the 17 controls as very effective



Use of Customer Authentication Methods by FS Respondents

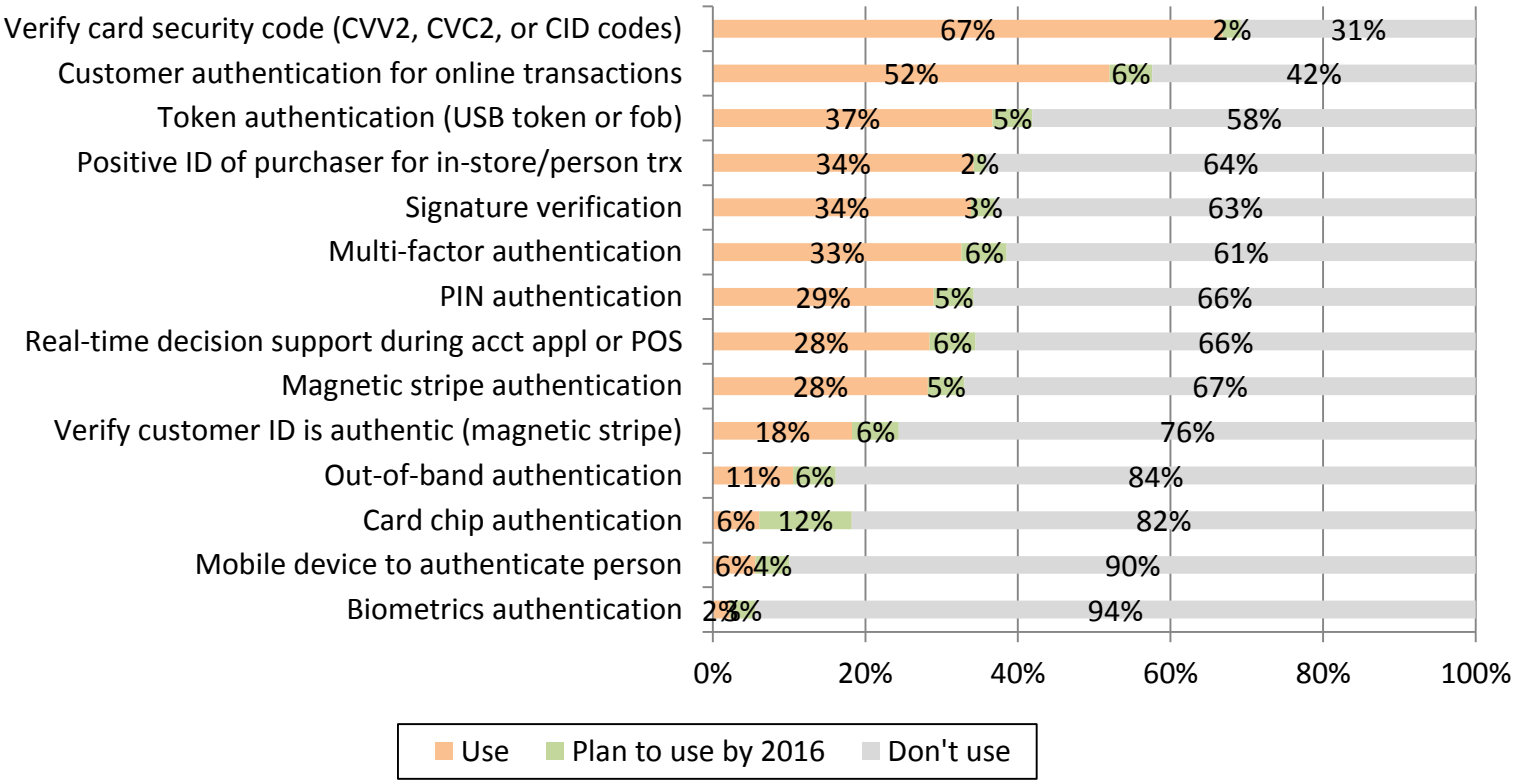
- 50% of FS respondents plan to use card chip authentication by 2016



Use of Customer Authentication Methods by Non-FS Respondents

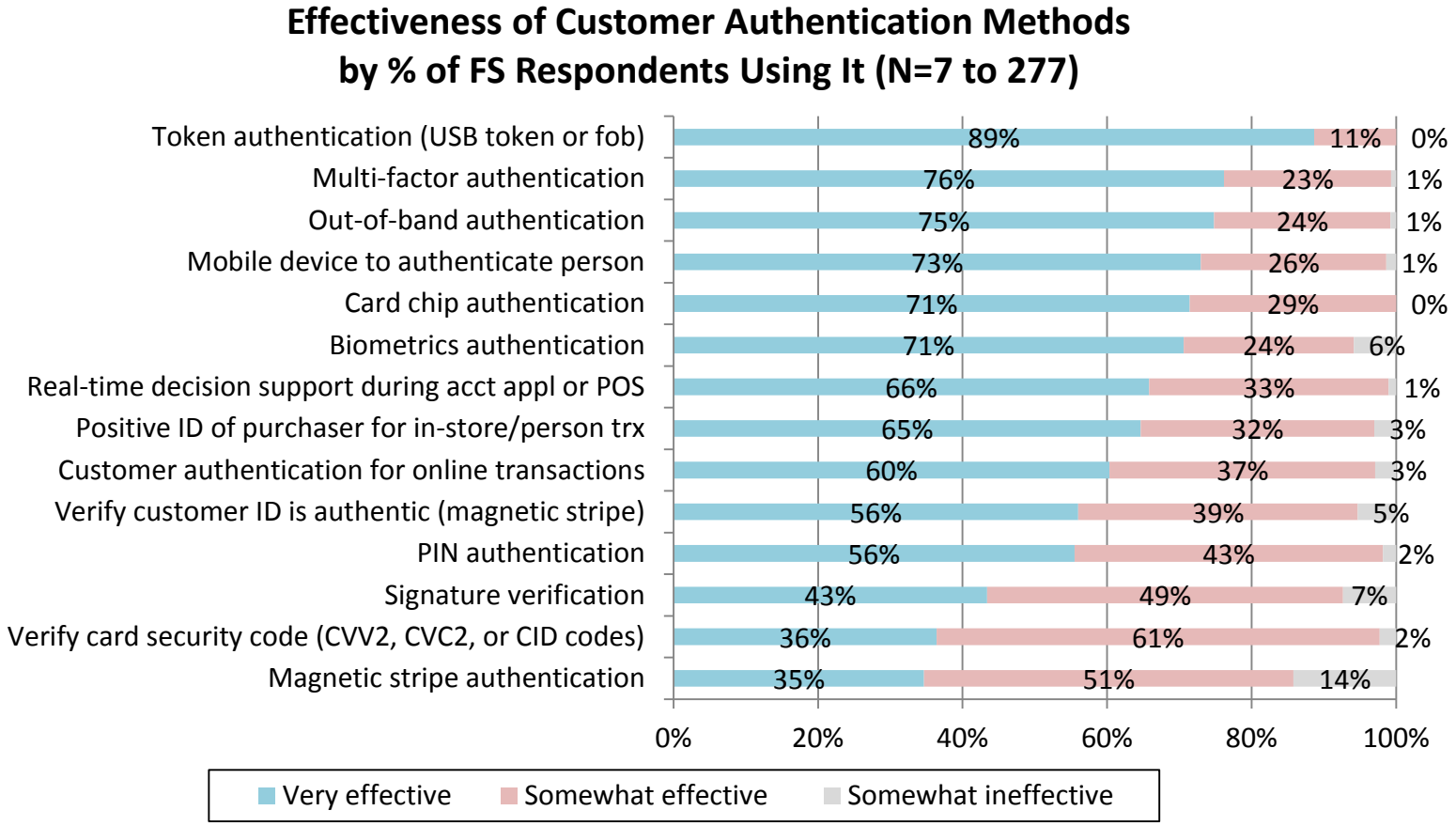
- Only 2 customer authentication methods are in use by half of the non-FS respondents

Use of Customer Authentication Methods by % of Non-FS Respondents (N=179 to 208)



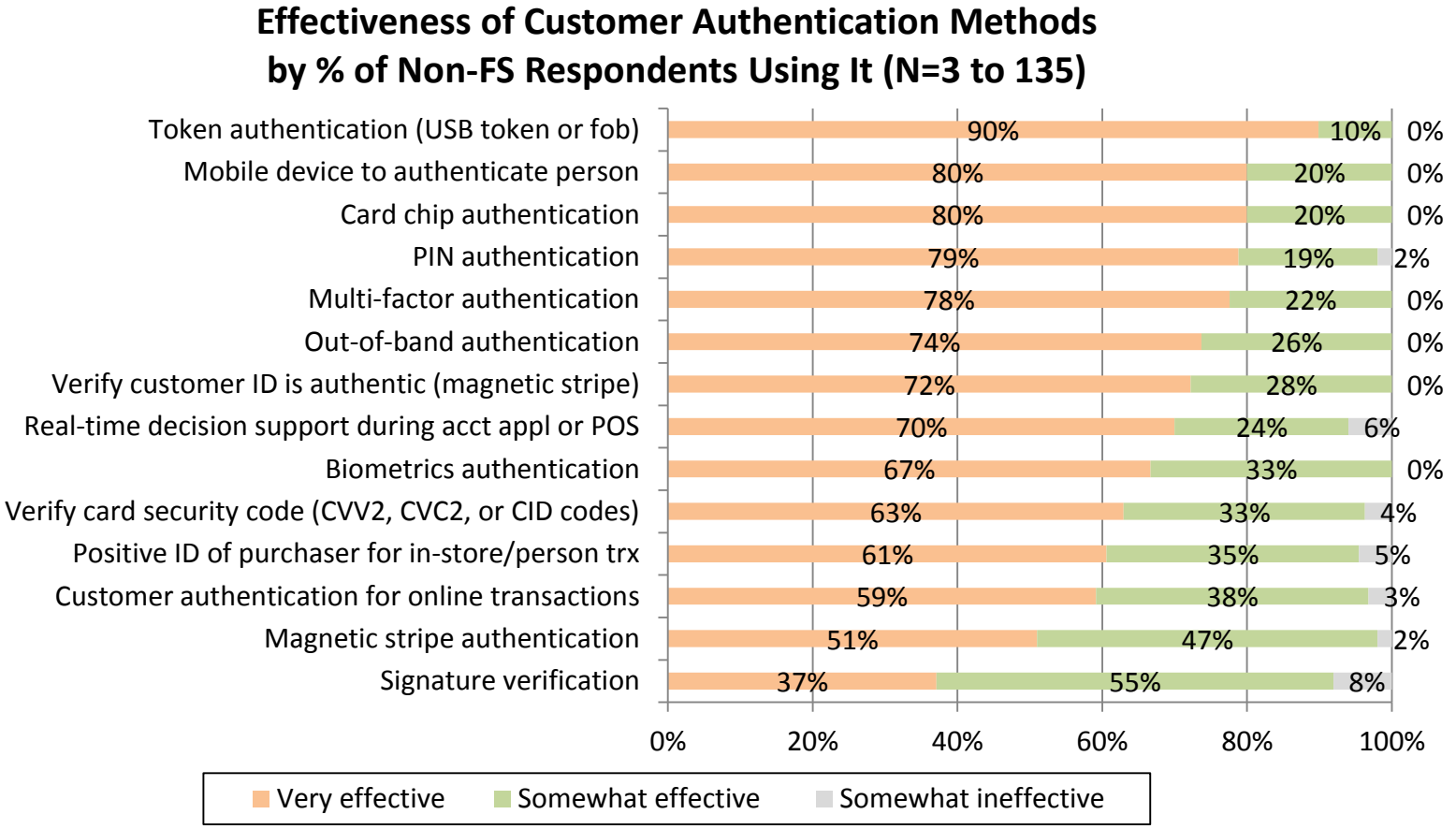
Effectiveness of Customer Authentication Methods Rated by FS Respondents

- Multi-factor authentication is rated very effective by 3/4 of FS respondents using it



Effectiveness of Customer Authentication Methods Rated by Non-FS Respondents

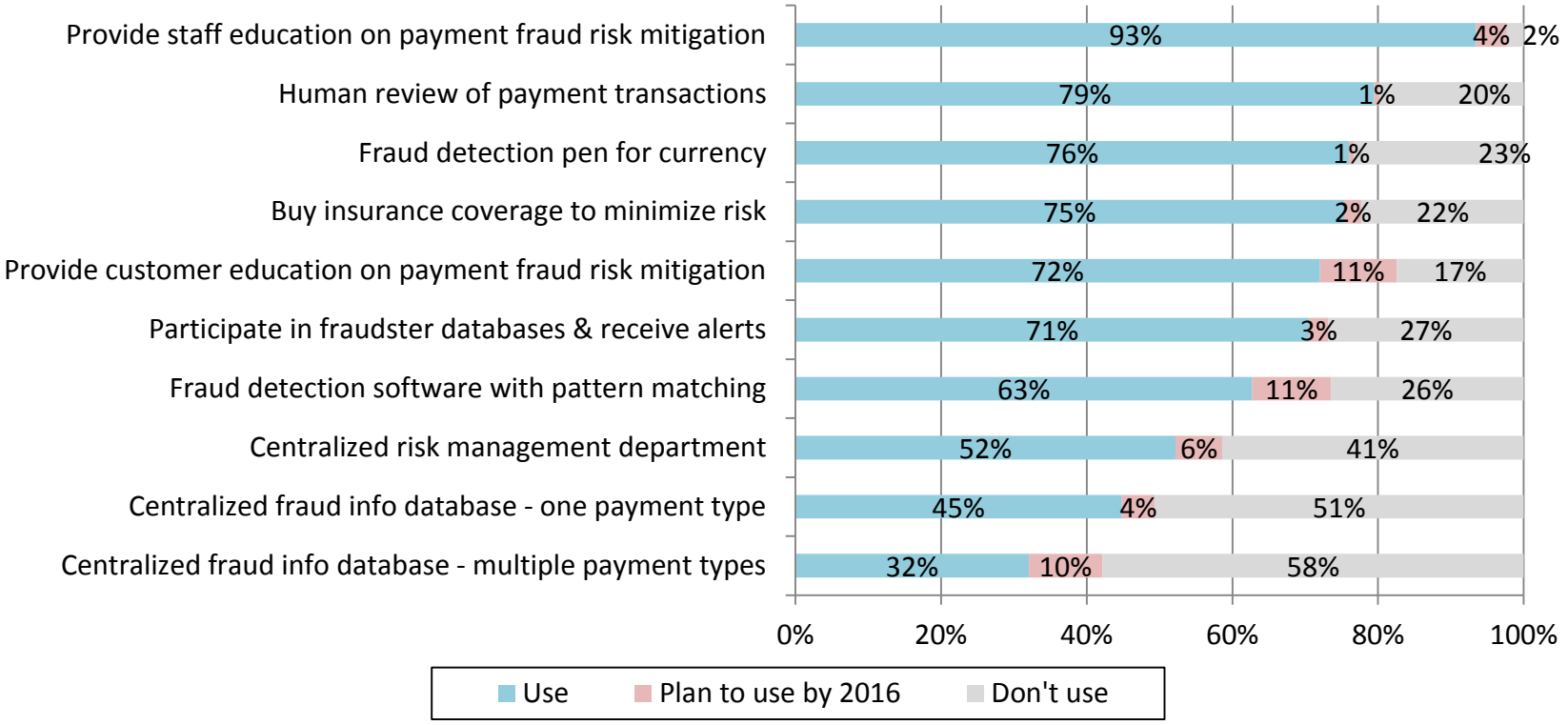
- More than 90% of firms that use these authentication methods find them effective



Use of Transaction Screening & Risk Management Methods by FS Respondents

- A layered approach may use a combination of both human review & software tools

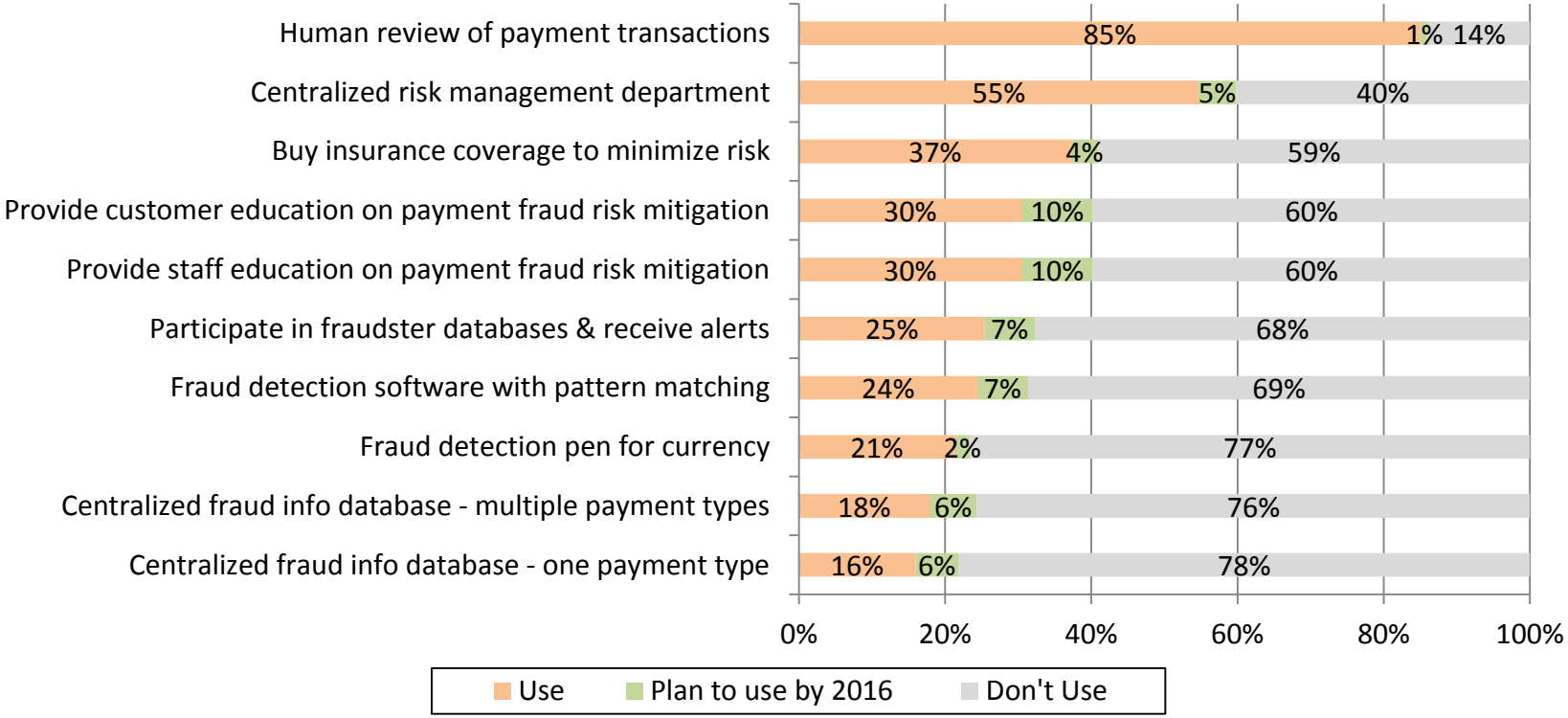
Use of Transaction Screening & Risk Management Methods by % of FS Respondents (N=287 to 306)



Use of Transaction Screening & Risk Management Methods by Non-FS Respondents

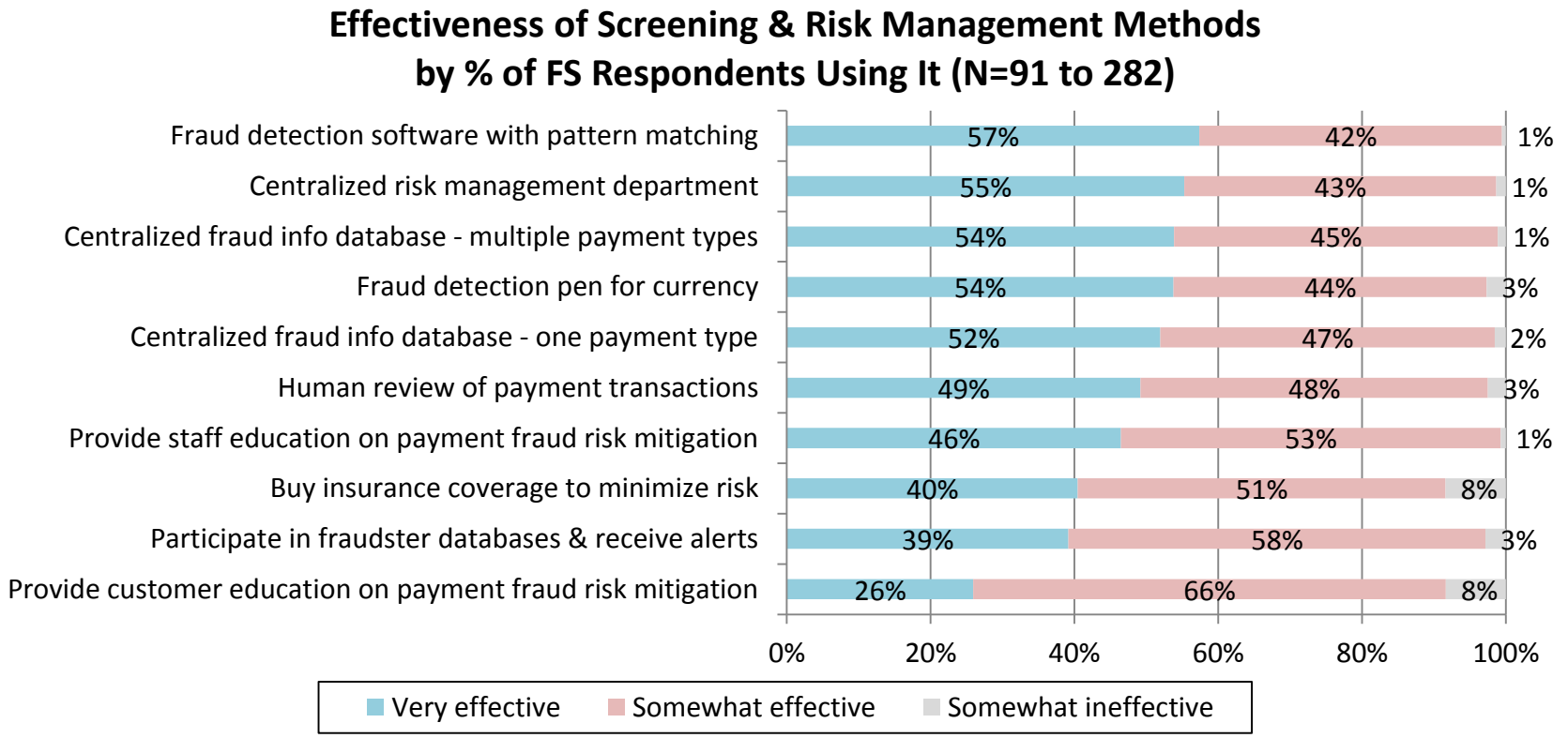
- Non-FS respondents are less likely to use the screening & risk management tools listed; only two are used by half of the non-financial firms

Use of Transaction Screening & Risk Management Methods by % of Non-FS Respondents (N=185 to 201)



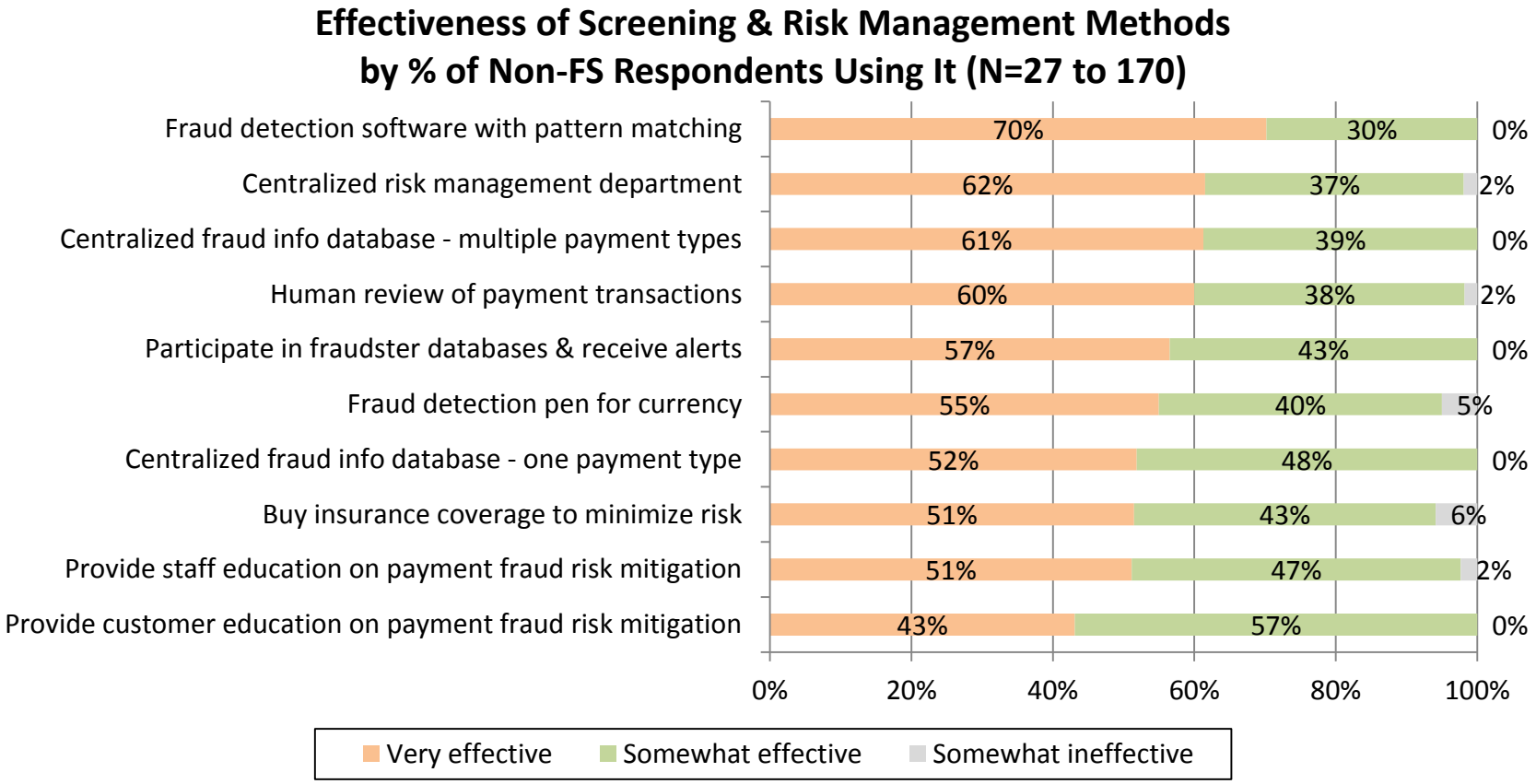
Effectiveness of Transaction Screening & Risk Management Methods Rated by FS Respondents

- Between 50-60% of the FS respondents that use fraud detection software with pattern matching, centralized risk management, centralized fraud information databases, & a fraud detection pen for currency rate them as "very effective"



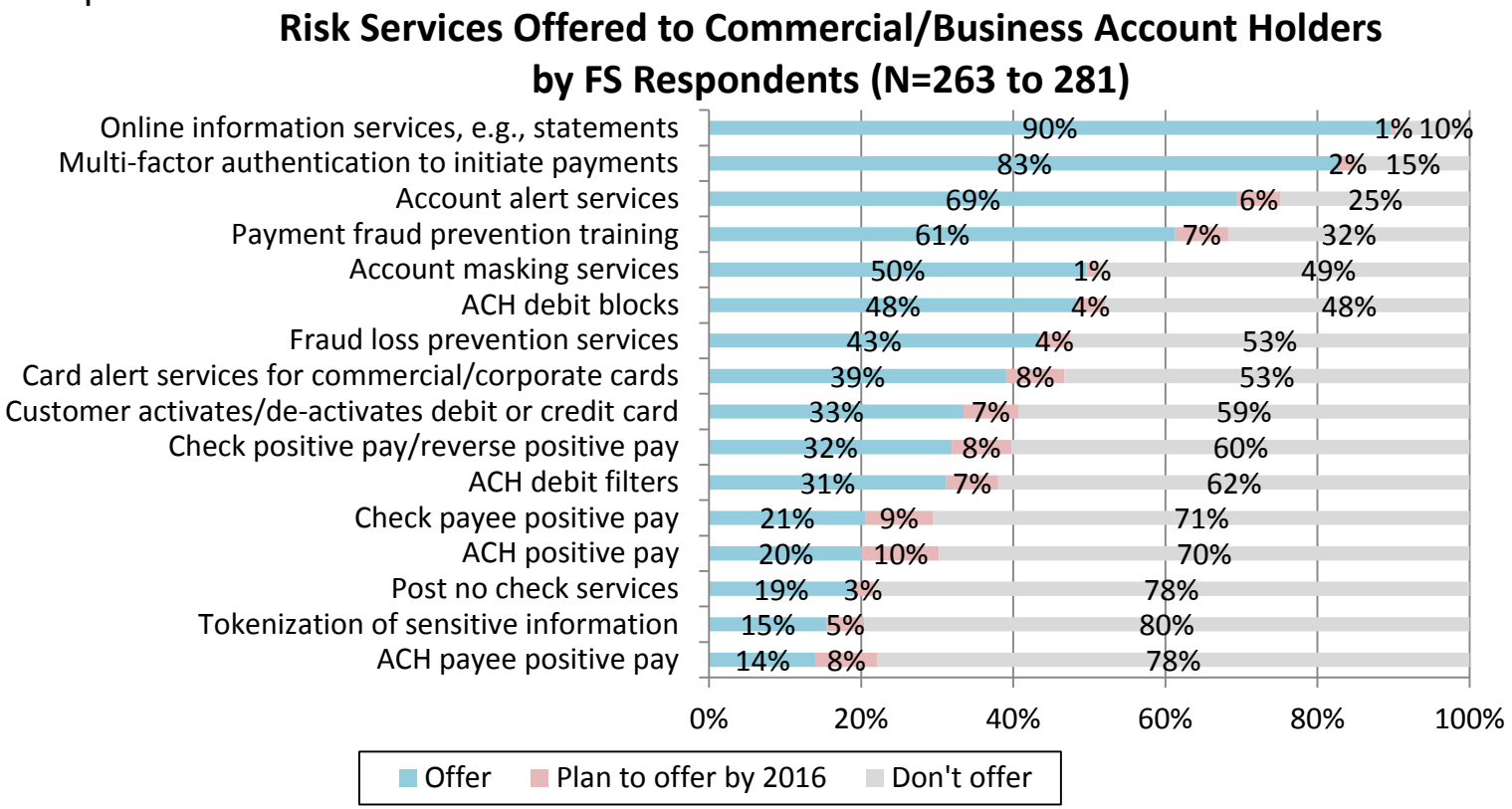
Effectiveness of Transaction Screening & Risk Management Methods Rated by Non-FS Respondents

- Non-FS firms seem satisfied with the tools they are currently using; over 90% of firms that use the specific tools listed, rate them as very or somewhat effective



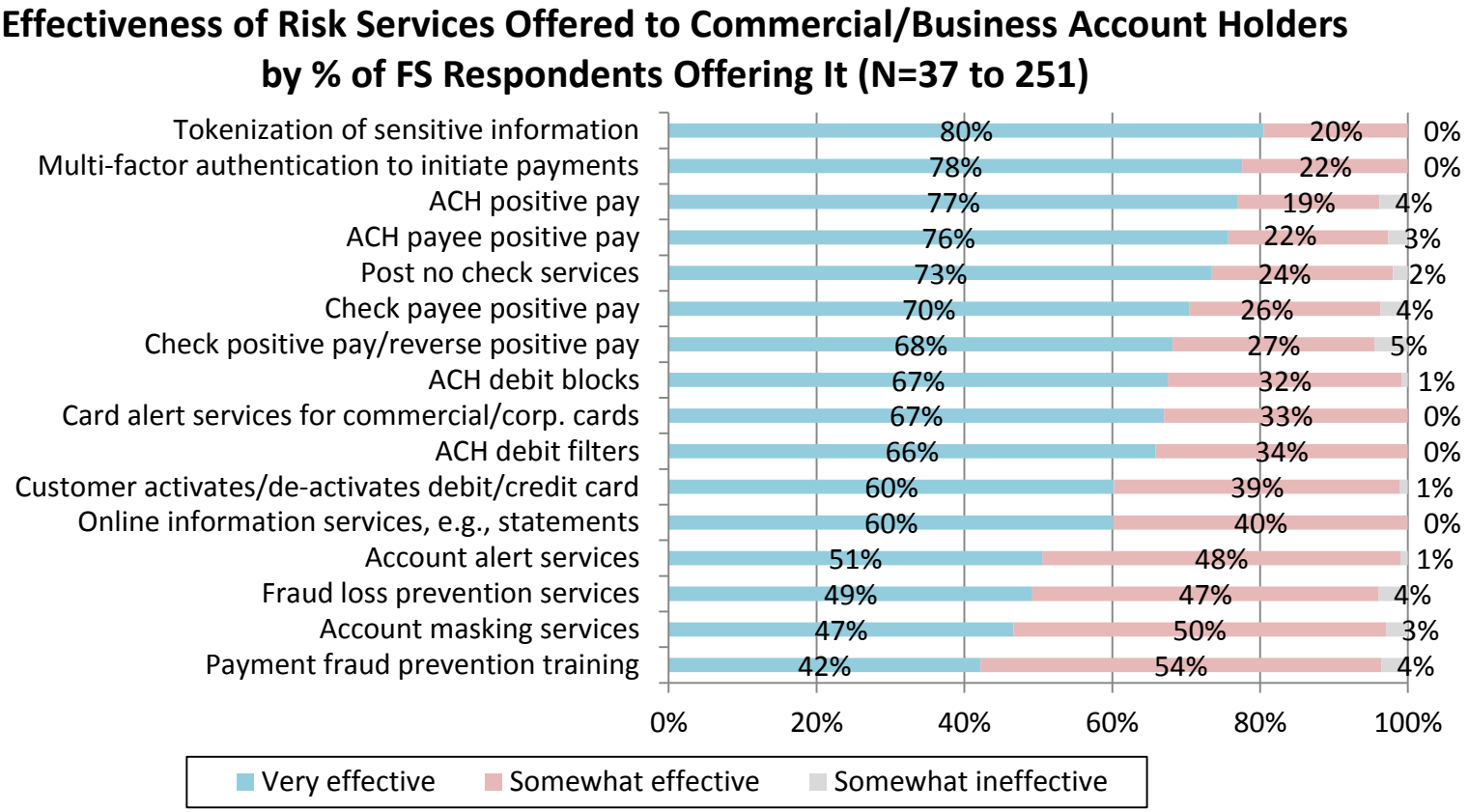
Risk Services Offered to Commercial Account Holders by FS Respondents

- With few exceptions, risk services offered by FS to commercial/business clients varies widely
- Services rated very effective by a higher share of users tend to be offered by a smaller share of FS respondents



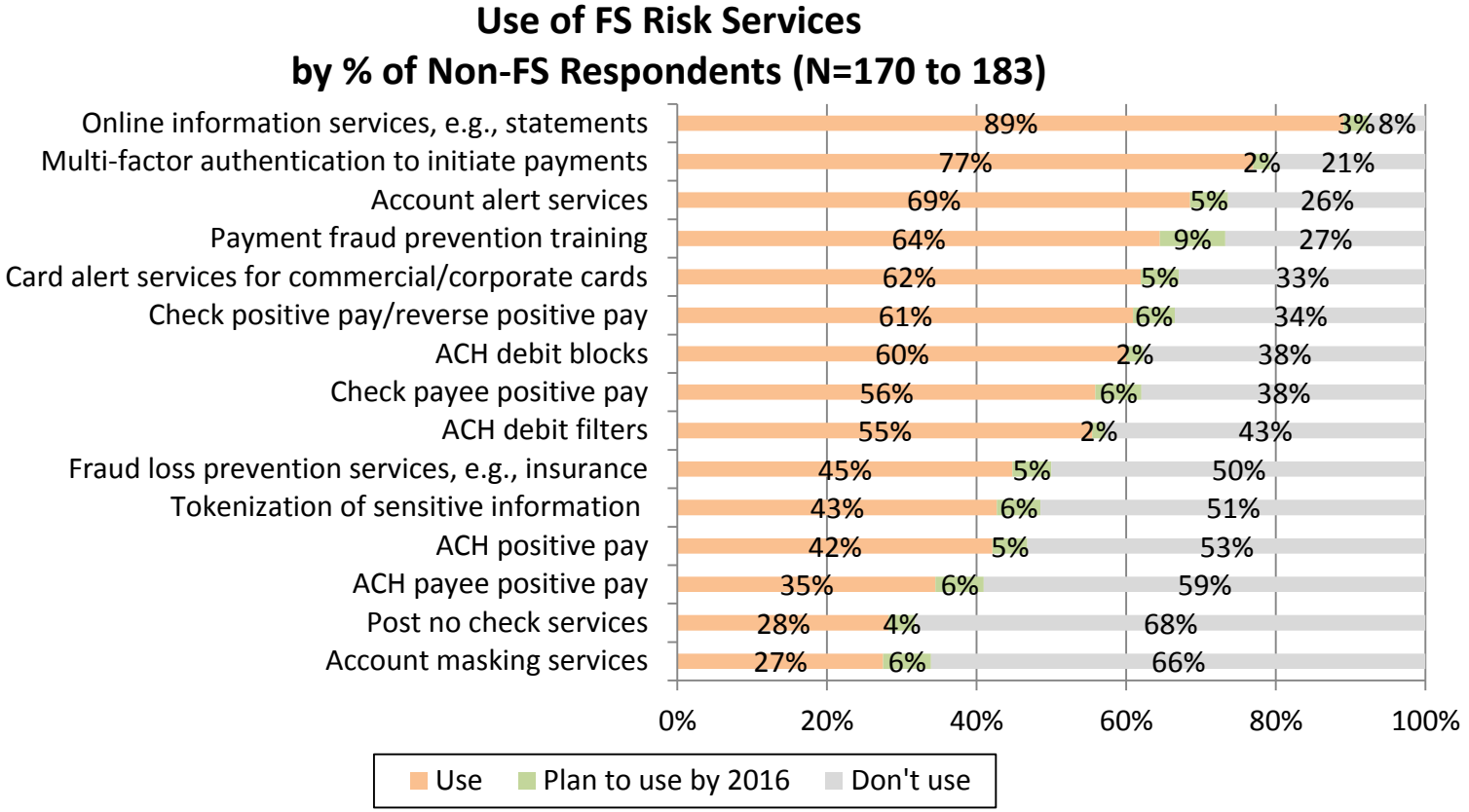
Effectiveness of FS Risk Services Offered to Commercial Accounts Rated by FS Respondents

- FS respondents are confident in the services they offer; 10 of the risk services listed are rated very effective by 2/3 or more of the FS firms that offer the service



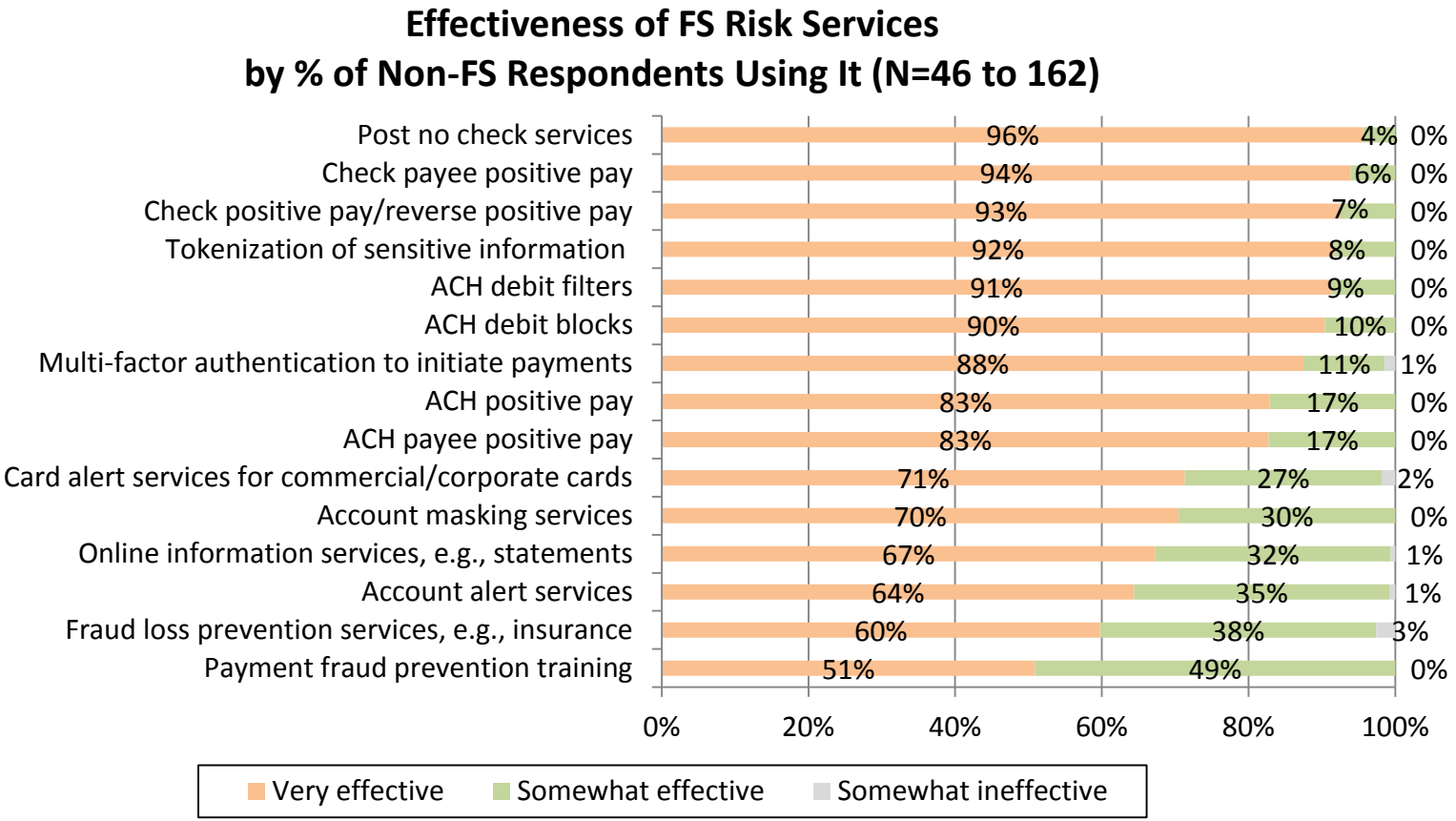
Use of FS Risk Services by Non-FS Respondents

- Services used by more than 3/4 of the non-FS firms are also most readily available—online information services & multi-factor authentication for payments initiation



Effectiveness of FS Risk Services Rated by Non-FS Respondents

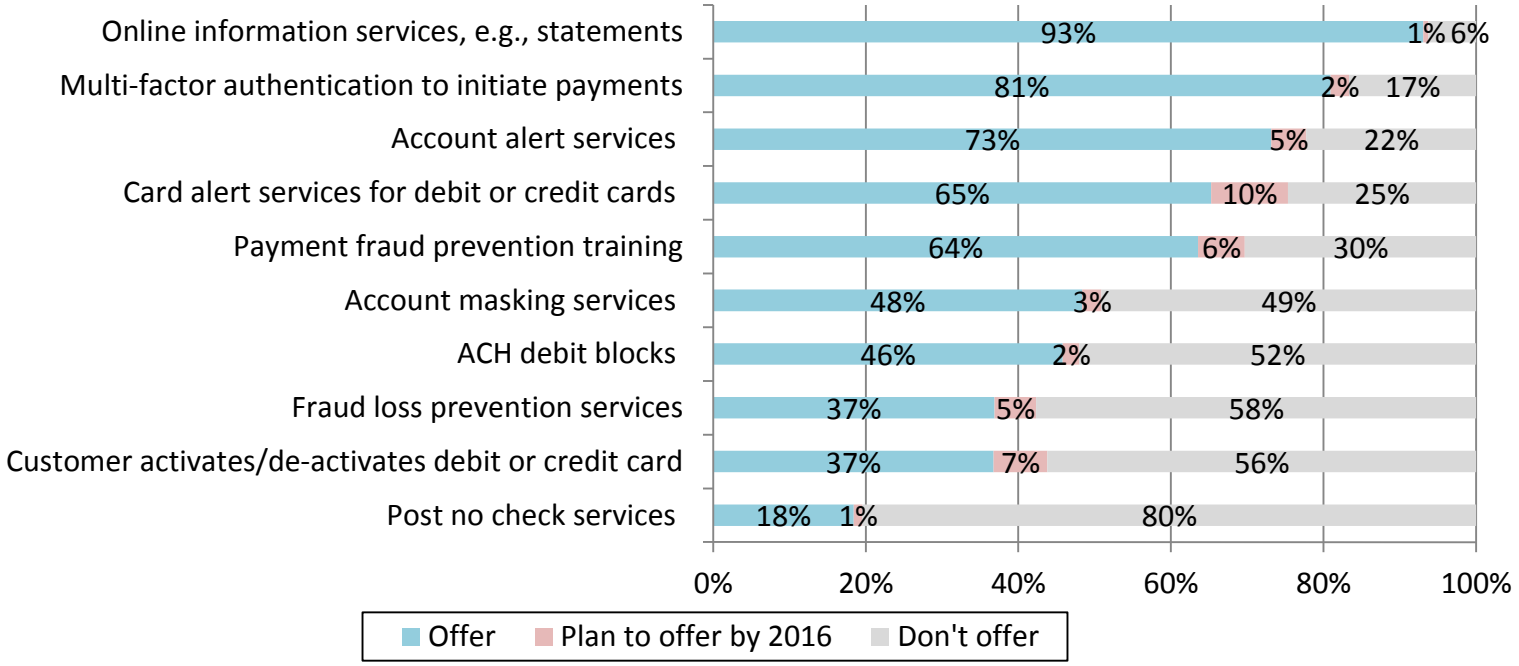
- Users of FS risk services are highly satisfied



Risk Services Offered to Consumer Account Holders by FS Respondents

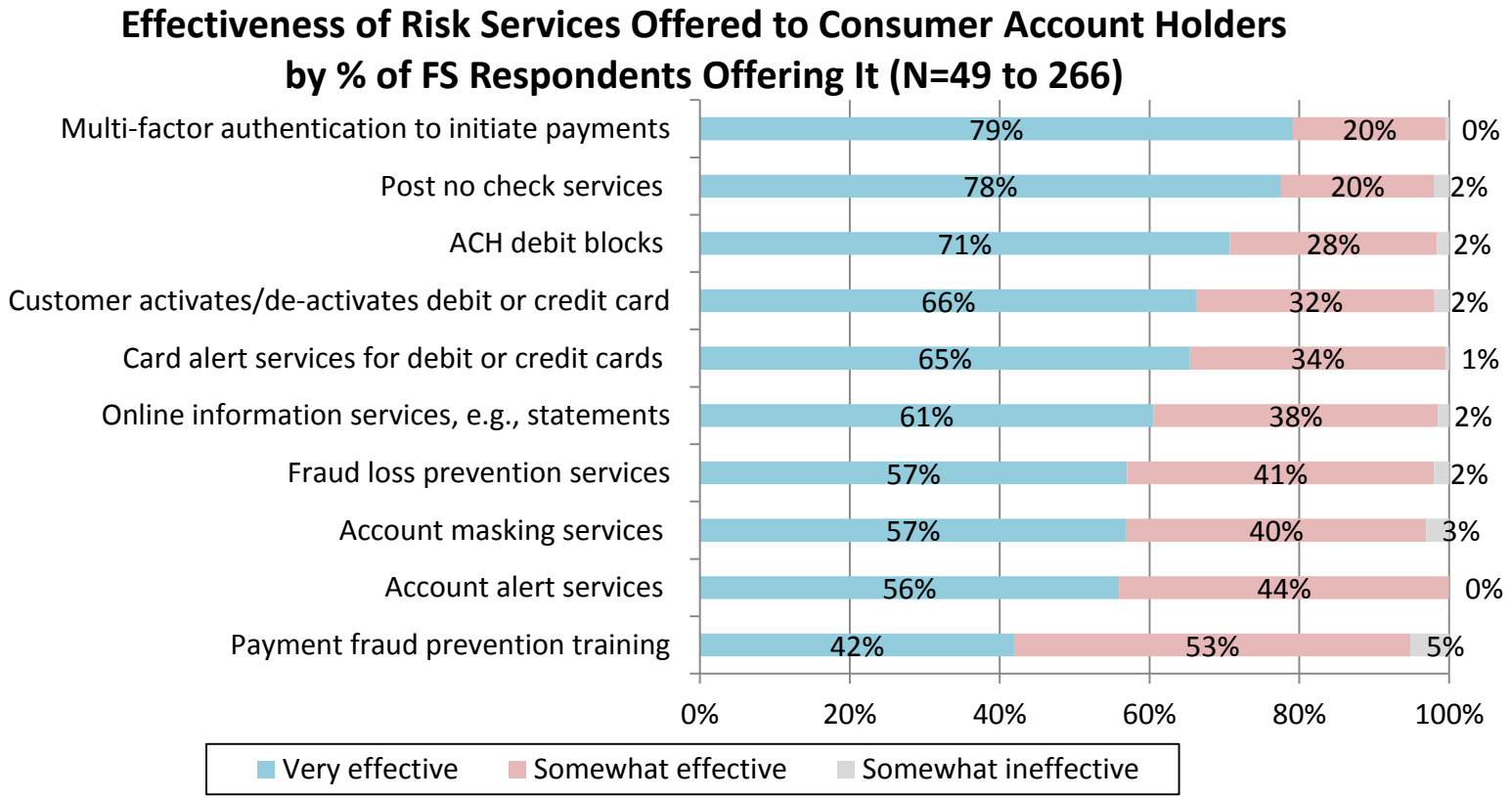
- 5 of the 10 risk-services for consumer accounts are offered by over half of the FS respondents
- More FS respondents offer card alert services to consumers (65%) than commercial account holders (39%); this may reflect the smaller share of FS respondents that offer credit cards & smaller share of businesses that use of debit cards for disbursements

Risk Services Offered to Consumer Account Holders by FS Respondents (N=266 to 289)



Effectiveness of FS Risk Services Offered to Consumer Accounts Rated by FS Respondents

- Consistent with services offered to commercial accounts holders, FS respondents are also confident in the services they offer to consumers



Opportunities to Reduce Payments Fraud

Most Needed Improvements

- Replacement of card magnetic stripe with EMV chip technology & improvements over Internet payments are reported as most needed improvements by over half of the respondents

Most Needed New or Improved Methods to Reduce Payments Fraud	FS (N=297)	Non-FS (N=185)	All Orgs (N=482)
Replacement of card/magnetic stripe with EMV chip technology	75%	50%	65%
Controls over Internet payments	62%	44%	55%
More aggressive law enforcement	48%	45%	47%
Consumer education on fraud prevention	49%	27%	40%
Controls over mobile payments	44%	30%	39%
Information sharing on emerging fraud tactics conducted by criminal rings	35%	45%	39%
Industry specific education on best prevention practices for fraud	26%	37%	30%
Industry alert services	26%	36%	30%
Tokenization of sensitive information	27%	35%	30%
Image survivable check security features for business checks	11%	19%	14%

Preferences in Adoption of Authentication Methods

- Majority favor a "Chip & PIN" requirement
- Smart chip cards/devices contain embedded microprocessors that provide strong security features against counterfeit fraud in card-present transactions
- Dynamic data authentication is an authentication technique used in chip transactions & protects against card skimming, counterfeiting & replay fraud
- "Chip & PIN" authentication is more secure because it requires two factors for authentication—what you have, the chip (in a card or a mobile device) & what you know, the PIN

Authentication Method Preferences	FS (N=295)	Non-FS (N=151)	All Orgs (N=436)
Chip & PIN requirement	80%	27%	70%
Chip for dynamic authentication	68%	18%	56%
Multi-factor authentication	48%	20%	44%
PIN requirement	30%	18%	31%
Token	27%	18%	29%
Mobile device to authenticate person	32%	12%	28%
Out-of-band/channel authentication to authorize payment	33%	6%	25%
Biometrics	18%	7%	16%

Legal or Regulatory Change

- FS & non-FS firms differ on ideas for legal & regulatory change that would help to reduce payments fraud

Legal & Regulatory Changes that Would Help Reduce Payments Fraud	FS (N=292)	Non-FS (N=176)	All Orgs (N=468)
Strengthen disincentives to committing fraud through stiffer penalties & more likely prosecution	60%	65%	62%
Place responsibility to mitigate fraud & shift liability for fraudulent card payments to the entity that initially accepts the card payment	73%	24%	55%
Place more responsibility on consumers & customers to reconcile & protect their payment data	72%	24%	54%
Improve law enforcement cooperation on domestic & international payments fraud & fraud rings	50%	60%	54%
Assign liability for fraud losses to the party most responsible for not acting to reduce the risk of payment fraud	65%	25%	50%
Focus future legal or regulatory changes on data breaches to where breaches occur	47%	30%	40%
Assign responsibility for mitigating fraud risk to the party best positioned to take action against fraud	40%	24%	34%
Align Regulation E & Regulation CC to reflect changes in check collection systems' use of check images & conversion of checks to ACH	40%	22%	34%
Establish new laws/regulation or change existing ones in order to strengthen the management of payments fraud risk	27%	38%	31%
Establish new laws/regulations to require data sharing to strengthen the management of payments fraud risk	22%	32%	25%

Cost & Privacy Are Main Barriers

- More FS & non-FS firms list “lack of staff resources” than any other barrier to fraud mitigation

Main Barriers	FS (N=250)	Non-FS (N=154)	All Orgs (N=404)
Lack of staff resources	60%	55%	58%
Lack of compelling business case (cost vs. benefit) to adopt new or change existing methods	36%	53%	42%
Consumer data privacy issues/concerns	37%	25%	32%
Corporate reluctance to share information due to competitive issues	24%	36%	28%
Cost of implementing commercially available fraud detection tool/service	21%	8%	16%
Cost of implementing in-house fraud detection tool/service	17%	12%	15%
Unable to combine payment information for review due to operating with multiple business areas, states or banks	16%	12%	15%

Conclusions

Conclusions

- In survey year 2014, payments fraud remains a significant concern for FS & non-FS firms that responded to this survey. FS respondents are significantly more likely to report payment fraud attempts (82%) & losses (76%) than non-FS companies.
- FS & non-FS firms have different experiences with loss rates, though overall losses remain quite low for both groups measured as a percentage of revenues. In 2014, 50% of the FS respondents that experienced payment fraud losses report increases in those losses, while 63% of non-FS firms respond that loss rates remain about the same over the prior year.
- Consistent with the 2012 survey, signature debit transactions are the payment type cited by the largest percent of FS respondents as accounting for high levels of payments fraud attempts & losses, while checks & credit cards are cited by the largest percent of non-FS companies.
- High percentages of surveyed FS organizations report that fraud prevention costs exceed actual losses for many types of payments, especially wire, cash, & ACH payments. This trend is even more striking for non-FS respondents. In every payment category, a higher percentage of such firms respond that prevention costs exceed actual losses. This may indicate that investments in fraud mitigation are working.

Conclusions

- For the 2014 survey, compromised sensitive information obtained from lost or stolen cards, checks, or other physical documents or devices while in the consumer's control is listed as a top source of information used in payments fraud by 45% of the FS respondents; & organization's information obtained from a legitimate check is listed as a top source of information by 35% of non-FS firms. These are higher than any other information source.
- Non-FS firms exhibit a very different usage pattern than FS firms in the category of customer authentication. There are only two authentication methods (verify CVV/CID codes on payment card & customer authentication for online transactions) that are used by more than 50% of firms surveyed. While 90% of FS firms use multi-factor authentication, only 33% of non-FS firms use multi-factor authentication for customer verification purposes.
- When asked about their authentication preferences, 80% of the FS respondents prefer chip & PIN requirements & 68% prefer chip for dynamic authentication; non-FS firms preferred these authentication methods at 27% & 18% respectively.
- Lack of staff resources is cited by respondents as the main barrier to reducing payments fraud.
- The most needed new or improved fraud mitigation methods cited by the highest percentage of FS respondents remained constant between 2012 & 2014. These methods are replacement of card magnetic stripe with EMV chip technology (75%); controls over Internet payments (62%); & consumer education of fraud prevention (49%). The top three methods seen as most needed by non-FS firms are replacement of card magnetic stripe with EMV chip technology (50%), information sharing on emerging fraud tactics being conducted by criminal rings (45%) & more aggressive law enforcement (45%).