2014 PAYMENTS FRAUD SURVEY SUMMARY OF REGIONAL RESULTS

Prepared by: Federal Reserve Bank of Minneapolis' Payments Information and Outreach Office

December 2014

Contents

Executive Summary

During the second quarter of 2014, the Federal Reserve Bank (FRB) of Minneapolis' Payments Information and Outreach office conducted a survey of financial institutions and corporations to gauge their experience with payments fraud.[1] This biennial survey seeks to uncover fraud trends for a variety of payment types, including checks, cash, debit and credit cards, automated clearinghouse (ACH) transactions, and wire transfers. Respondents are asked to describe types and levels of fraud and also to highlight effective fraud mitigation strategies. This survey is the fourth in a series; similar surveys were issued in 2009, 2010, and 2012.

Financial institutions and non-financial firms responding to this survey use different business models and offer or use different mixes of payment products. For example, the majority of non-financial respondents to the 2014 survey make and receive payments primarily from other businesses (59%) and are much less consumer-facing than the banks and credit unions that responded. Financial institutions offer a variety of payment products to end users. Non-financial companies are end users of payment products and select and use products that meet their payment needs. These differences are important to consider when comparing the fraud experiences of responding companies.

Payments fraud remains a significant concern for financial institutions and other corporations in the ninth district and surrounding region. While financial institutions are much more likely to report payment fraud attempts (75% experienced attempted fraud) and losses (70%) than non-financial companies, the proportion of financial institutions reporting fraud attempts and losses has actually decreased since 2012, when most respondents reported fraud attempts (94%) and losses (90%).

At the same time, about half of the financial institutions that experienced payment fraud losses reported increases in those losses, while three quarters of the non-financial firms responded that loss rates had remained about the same over the prior year. In keeping with previous surveys, signature debit transactions are the payment type cited by the largest number of financial institutions as accounting for high levels of payments fraud losses (92% of financial service companies), while checks are cited by 75% of non-financial companies.

Although many respondents experienced fraud attempts and losses, in 2013, one out of five (21%) financial institutions and one out of two (54%) non-financial firms did not incur losses. This suggests that effective measures were in place preventing the successful use of compromised payment instruments and information, or possibly the fraud attempt was relatively unsophisticated.

Indeed, the data shows that companies are investing increasingly in fraud prevention, mitigation, and control. These investments should be taken into consideration when evaluating the overall cost of payment fraud to individual companies and to the economy as a whole. High percentages of surveyed financial institutions report that fraud prevention costs exceed actual losses for many types of payments, especially wire, cash, and ACH payments. This trend is even more striking for non-financial

[1] Questions about the survey may be directed to Claudia Swendseid (claudia.swendseid@mpls.frb.org), Amanda Dorphy (amanda.dorphy@mpls.frb.org) or Katy Jacob (katy.jacob@mpls.frb.org) at the Federal Reserve Bank of Minneapolis.

respondents. In every payment category, a higher percentage of such firms responded that prevention costs exceed fraud losses.

While this finding could suggest that companies are overcompensating in prevention vis-à-vis likely losses, it is also possible that risk mitigation strategies and fraud prevention investments have indeed been effective. Financial institutions are particularly likely to perceive that risk mitigation strategies have led to a decrease in fraud losses; 71% state this belief, compared to only 33% of non-financial firms. Over half of the respondents (60%) whose losses increased or stayed the same report that risk measures taken helped to control the level of losses. Financial institutions are also heavier users of customer authentication methods than non-financial firms. For example, almost all (92%) of surveyed financial institutions use multi-factor authentication, while only 35% of non-financial firms do so. Financial institutions are also more likely to use a variety of transaction screening and risk management methods than non-financial firms, according to survey results.

This might be explained in part by respondents' perspectives on barriers to reducing payment fraud. While both financial institutions and corporations cite a lack of staff resources as a barrier, non-financial firms more often cite the lack of a business case (50% of non-financial firms versus 34% of financial institutions) as a barrier to implementing new fraud reduction strategies. Thus, non-financial firms may be more likely to stick with the status quo and not seek new authentication or prevention strategies because it is difficult for them to produce cost-benefit analyses that make such efforts appear worthwhile.

Finally, survey results indicate that financial and non-financial companies support legal and regulatory changes to strengthen disincentives to committing fraud through stiffer penalties and more certain prosecution. Financial firms also favor assigning liability and/or more responsibility for mitigating fraud to those parties in the best position to do so.

Introduction

During the second quarter of 2014, the Federal Reserve Bank (FRB) of Minneapolis' Payments Information and Outreach office conducted a survey of financial institutions and corporations to gauge their experience with payments fraud[2]. This biennial survey seeks to uncover fraud trends for a variety of payment types, including checks, cash, debit and credit cards, automated clearinghouse (ACH) transactions, and wire transfers. Respondents are asked to describe types and levels of fraud they have experienced and also to highlight effective fraud mitigation strategies. This survey is the fourth in a series; similar surveys were issued in 2009, 2010, and 2012.

Respondent Profile Information

In 2014, FRB Minneapolis and FRB Chicago joined forces to combine responses from their districts into one report. The survey was distributed by various trade associations to their corporate and financial institution members.[3] The survey garnered a total of 226 responses, of which 61% were financial institutions and 39% were corporations, merchants, and other non-financial companies. This is the highest response rate among the four surveys seen from non-financial companies, with the second highest being 29% in 2010. In contrast, the 2012 survey is dominated by financial institutions, which comprised 92% of the total. This difference in the respondent profile should be considered when comparing 2014 results with those of prior years.

Table 1: Respondent Industry Classification
(by % of Respondents and Survey Year)

Respondents by Industry	2014 (N=226)	2012 (N=246)	2010 (N=206)
Financial Service Industry	61%	92%	71%
Non-Financial Service Industry	39%	8%	29%

Of financial institution respondents, about two-thirds, or 67%, were banks, 28% were credit unions, 2% were thrifts, and 4% were service providers, e.g., payment processors, lockbox, card service providers, etc. (Table 2)[4].

[2] The Federal Reserve Banks of Boston, Chicago, Dallas, and Richmond also sponsored concurrent surveys. A consolidated results report is also available on the Federal Reserve Bank of Minneapolis website.

[3] Trade associations that helped to promote participation in this survey include the Upper Midwest Automated Clearing House Association, Wisconsin Automated Clearing House Association, Minnesota Association for Financial Professionals, Financial and Retail Protection Association, Minneapolis chapter of the International Association of Financial Crimes Investigators, Michigan Bankers Association, Community Bankers of Michigan, Minnesota Bankers Association, Montana Bankers Association, Montana Independent Bankers Association, South Dakota Bankers Association, Independent Community Bankers of South Dakota, Independent Bankers Association of America, Credit Research Foundation, National Association of Credit Management, Institute of Financial Operations, Association for Financial Professionals, National Association of Purchasing Card Professionals, Remittance Coalition, and the Small Business Administration.

[4] Throughout the report text the authors use financial institutions to include banks, credit unions, thrifts, and other financial service providers. Figures and tables use financial services to include all four types of financial firms and financial institutions when questions were only asked of banks, credit unions, and thrifts.

Table 2: Financial Service Industry Respondent Type
(by % of Financial Service Respondents and Survey Year)

Financial Service Industry Type	2014 (N=138)	2012 (N=227)
Bank	67%	78%
Credit Union	28%	18%
Thrift	2%	3%
Service Provider	4%	0.4%

Q1b: Please select the type of financial services organization from the list below.

Of non-financial companies, more than one-third of respondents represent manufacturing. Table 3 lists the industry classifications. For the first time, the survey garnered responses from wholesale trade companies and firms in the agriculture industry; both industries represent 9% of non-financial respondents.

Table 3: Non-Financial Service Industry Respondent Industry Classification
(by % of Respondents and Survey Year)

Non-Financial Service Industry Classification	2014 (N=88)	2012 (N=19)	2010 (N=63)
Manufacturing	34%	21%	8%
Wholesale Trade	9%	0%	na[5]
Agriculture	9%	0%	na
Other	8%	11%	29%
Retail Trade	7%	5%	19%
Government	6%	26%	8%
Health Services	5%	16%	2%
Insurance and Pension Funds	5%	5%	6%
Software and Technology	3%	0%	2%
Educational Services	3%	0%	na
Business Services and Consulting	2%	0%	0%
Transportation and Warehousing	2%	0%	2%
Energy	2%	0%	5%
Real Estate, Rental, and Leasing	2%	0%	2%
Construction	1%	5%	0%
Hospitality and Travel	1%	11%	2%
Brokers, Underwriters, and Investment Companies	0%	0%	5%
Telecommunications	0%	0%	2%
Nonprofit	0%	0%	11%

Q1a: How do you classify your organization?

[5] The designation of "na" indicates "not asked" in the prior survey.

Table 4 shows that about half of the respondents meet the definition of a small business (annual revenue under $50 million). This includes over two-thirds, or 72%, of the financial institution and 21% of the non-financial firm respondents. Fourteen percent of respondents have revenue of $1 billion or greater.

Table 4: Annual Revenue
(by % of Respondents)

Annual Revenue	YE 2013			YE 2011			YE 2009		
	FS (N=138)	Non-FS (N=88)	All Org. (N=226)	FS (N=227)	Non-FS (N=19)	All Org. (N=246)	FS (N=143)	Non-FS (N=63)	All Org. (N=206)
Under $10 million	61%	8%	40%	56%	16%	53%	48%	48%	48%
$10 million to $24.9 million	7%	6%	6%						
$25 million to $49.9 million	4%	7%	5%						
$50 – 99.9 million	8%	8%	8%	12%	16%	12%	12%	2%	9%
$100 – 249.9 million	2%	13%	6%	9%	5%	9%	11%	8%	10%
$250 – 499.9 million	1%	19%	8%	5%	11%	6%	5%	6%	5%
$500 – 999.9 million	1%	8%	4%	2%	11%	2%	5%	6%	5%
$1 – 4.9 billion	1%	18%	8%	3%	21%	4%	7%	10%	8%
$5 – 9.9 billion	1%	7%	3%	1%	5%	1%	1%	3%	2%
$10 billion or more	1%	6%	3%	0%	11%	1%	1%	3%	2%
Don't Know	3%	0%	2%	12%	0%	11%	2%	2%	2%
Not applicable	11%	1%	7%	1%	5%	2%	1%	11%	4%

Q6: What do you estimate are your organization's 2013 annual revenues?
(If you don't know, please provide your best estimate.)

Financial institutions were also asked about total assets as it is a common measure of size. Banks and credit unions with under $100 million in assets comprise 50% of survey respondents (Table 5). The higher concentration of smaller financial institutions is consistent with the share of smaller institutions in the region[6].

[6] Fifty five percent of financial institutions (banks, credit unions, and thrifts) in the seventh and ninth Federal Reserve districts are under $100 million in assets.

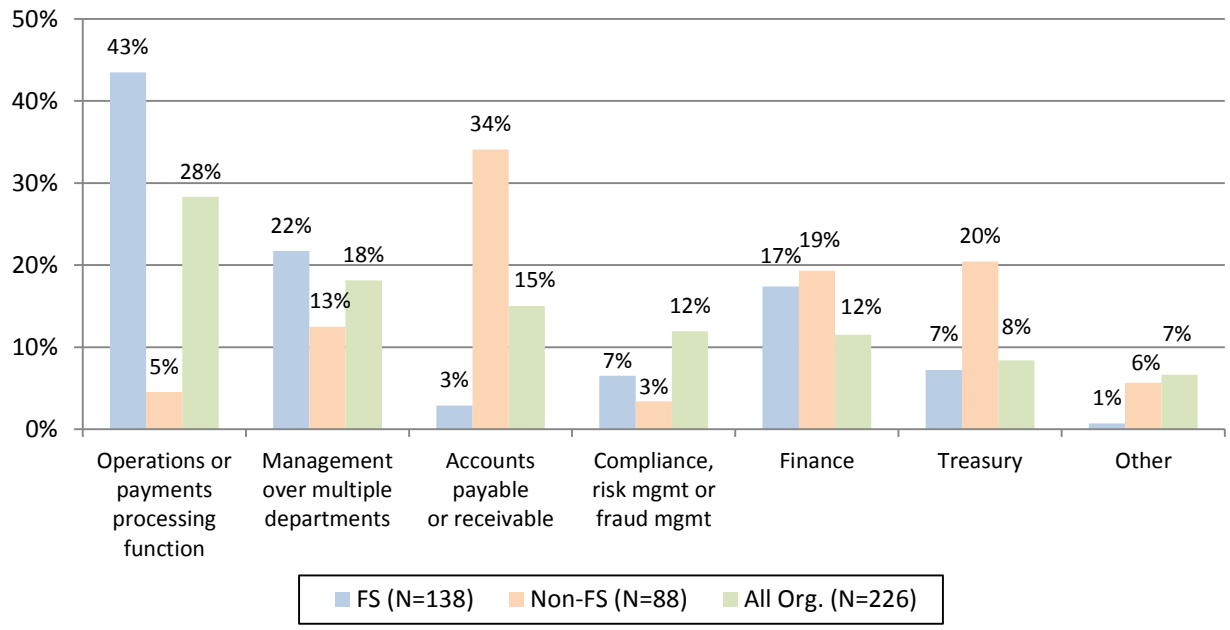
Table 5: Total Assets Year-End
(by % of Financial Institution Respondents)

Financial Institution Total Assets as of Year-End	YE 2013 (N=130)	YE 2011 (N=226)
Under $50 million	28%	24%
$50 – 99.9 million	22%	24%
$100 – 249.9 million	20%	28%
$250 – 499.9 million	12%	12%
$500 – 999.9 million	8%	5%
$1 – 4.9 billion	8%	4%
$5 – 9.9 billion	2%	3%
$10 billion or more	1%	0%

7: What is the size of your financial institution based on year-end 2013 total assets?
(If you don't know, please provide your best estimate.)

Figure 1 shows that operations/payments processing professionals are the most highly represented category of financial institution respondents at 43%. In contrast, more than one-third of non-financial institution respondents work in the accounts payable/receivable area of their firms. Treasury and finance employees are equally represented for non-financial firms (20% and 19% respectively), while managers over multiple departments are the second highest respondent group within financial firms (22%).

Figure 1: Type of Department in which Respondent Works
(by % of Respondents)



5. What best describes the type of department you work in?

In 2014, FRB Minneapolis worked with a variety of trade associations to encourage participation in the survey. As noted in Table 6, over half of financial institution respondents are members of NACHA, the ICBA and/or a regional payments association. Non-financial firms are less likely to belong to an association that focuses on payments; 36% do not belong to any such group. This trend highlights the importance of providing accurate and timely information on payments to non-financial firms that are affected by payments fraud, as alternate sources of information might be lacking.

Table 6: Respondent Membership in Trade Associations that Provide Education on Payments or Payments Risk (by % of Respondents)

Trade Association	FS (N=137)	Non-FS (N=84)	All Org. (N=221)
NACHA The Electronic Payments Association	58%	8%	39%
Independent Community Bankers of America (ICBA)	50%	6%	33%
Regional payments association (e.g., UMACHA, WACHA)	50%	2%	32%
American Bankers Association (ABA)	44%	7%	30%
State banking association	40%	6%	27%
Credit Union National Association (CUNA)	23%	0%	14%
Association for Financial Professionals (AFP)	3%	17%	8%
National Association of Credit Management (NACM)	0%	14%	5%
Credit Research Foundation (CRF)	0%	13%	5%
Financial and Retail Protection Association (FRPA)	7%	2%	5%
State AFP or treasury management association (e.g., MN AFP)	1%	8%	4%
National Association of Federal Credit Unions (NAFCU)	4%	0%	3%
Regional CU League/Network	4%	0%	3%
Other	3%	11%	6%
None	2%	36%	15%

8: Are you or your organization a member of a trade association that provides education on payments and/or payments risk?

Summary of Survey Results by Question

In this section, survey question results are analyzed. Where applicable and relevant, results of financial and non-financial firms are compared. Notable trend variances between this and previous surveys are discussed as well.

Payment Types Used by Non-Financial Institution Respondents

Table 7 shows that most non-financial respondents make and receive payments from other businesses (59%). Only 4% deal primarily with consumers, while more than one-third (37%) exchange payments with both businesses and consumers.

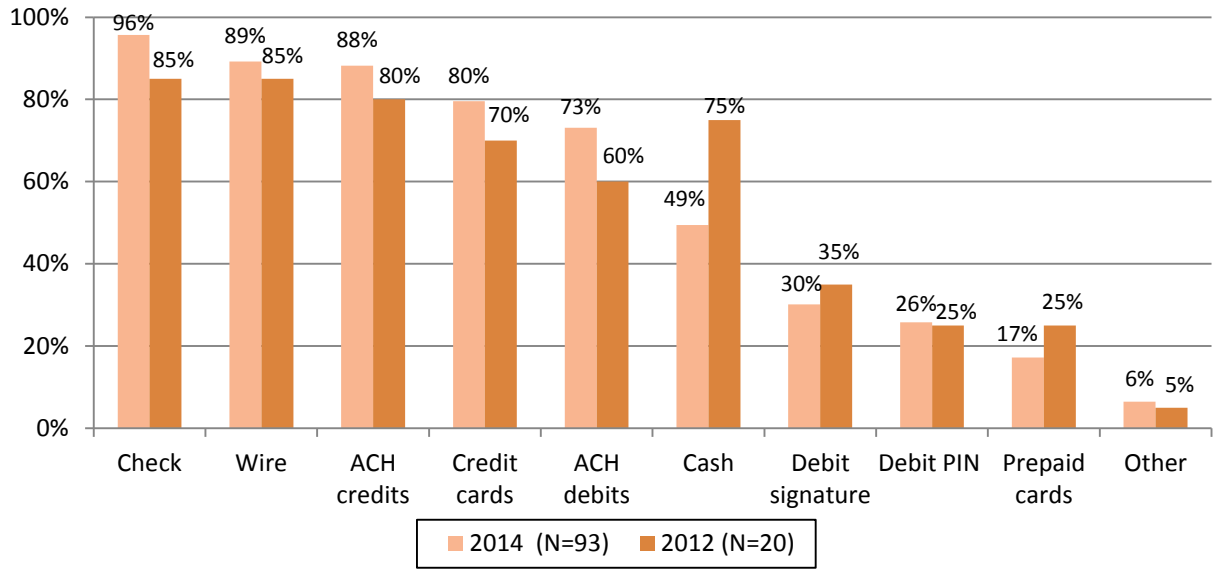
Table 7: Typical Payment Counterparties Associated with Organization's Payments Volume (by % of Non-Financial Institution Respondents (N=92))

Payment Counterparties	(%)
Primarily payments to/from other businesses	59%
Payments to/from both consumers and businesses	37%
Primarily payments to/from consumers	4%

Q9: In terms of your organization's payments volume, who are the typical counterparties?
Note: Businesses includes government entities.

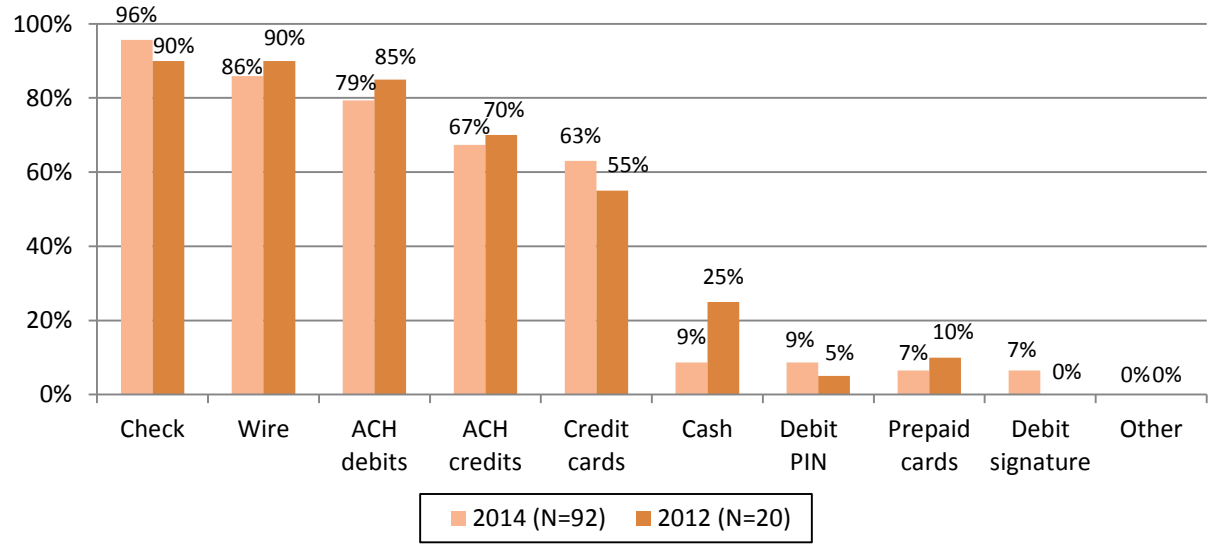
Figure 2 depicts a year-to-year comparison, highlighting the types of payments accepted by non-financial respondents. Almost all companies accept check payments (96%), growing from 85% in 2012. This change may be due to the higher number of non-financial respondents in the 2014 survey (93), compared to the number in 2012 (20). Nonetheless, general trends remain fairly constant, with one notable exception. Generally, checks, wires, ACH payments, and credit cards are widely accepted by non-financial firms; debit and prepaid cards are accepted at much lower level. Curiously, cash is accepted by 49% of non-financial firms in 2014 versus 75% just two years ago. The payment types used for disbursement (Figure 3) show similar trends to the payment types accepted (Figure 2): checks, wires, and ACH payments are used much more often than debit and prepaid cards. ACH credits and credit cards are used for disbursements fairly equally at 67% and 63% respectively. Again, 2014 shows a decrease in cash usage for payment disbursement over 2012, declining from 25% to 9% of firms.

Figure 2: Payment Types Accepted
(by % of Non-Financial Institution Respondents)



Q10: What types of payments does your organization accept?

Figure 3: Payment Types Used for Disbursements
(by % of Non-Financial Institution Respondents)



Q11: What types of payments does your organization use to disburse payments?

Payment Products Offered by Financial Institution Respondents

The majority of financial institution respondents (73%) offer payment services to both businesses and consumers. About a quarter (26%) focus on the consumer segment and only a few (2%) serve mainly business or commercial customers (Table 8).

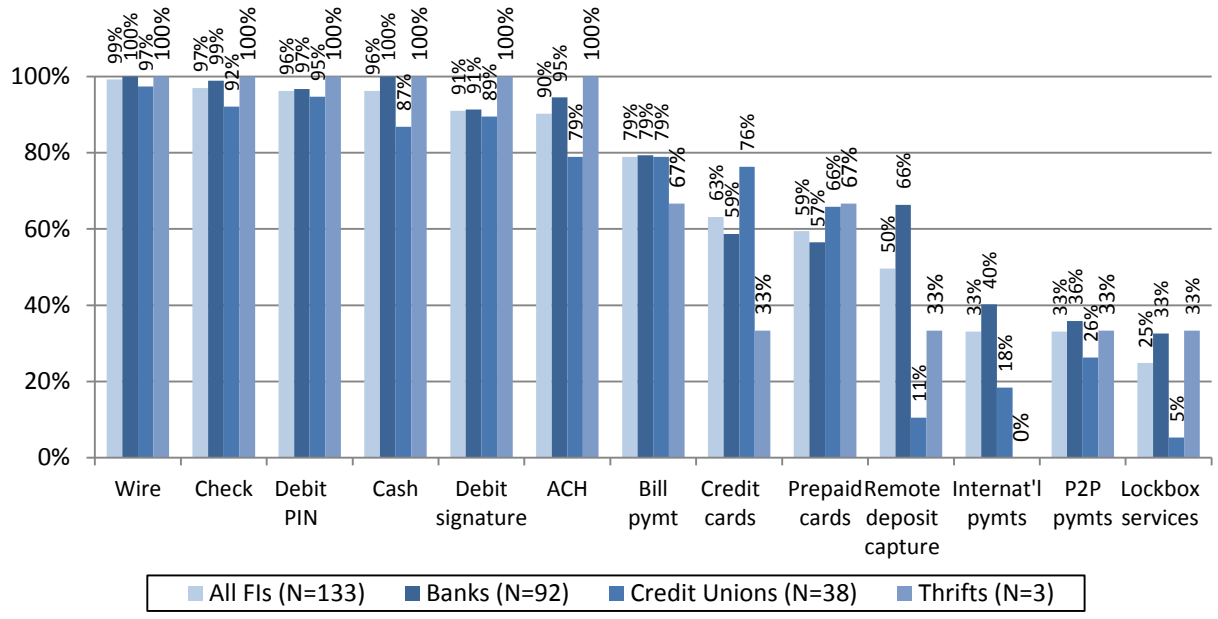
Table 8: Type of Customers to Whom Financial Institution Typically Offers Its Payment Products and Services
(by % of Financial Institution Respondents)

FI Customers	Banks (N=90)	Credit Unions (N=38)	Thrifts (N=3)	All FIs (N=131)
Both consumers and business or commercial clients	87%	37%	100%	73%
Primarily to consumers	11%	63%	0%	26%
Primarily business or commercial clients	2%	0%	0%	2%

Q12: To what type of customers does your financial institution typically offer payment products and services?

Figure 4 shows the breakdown of financial institution types and the payment products and services they provide. More than 90% offer wire, check, debit card, ACH, and cash payment services to customers. Interestingly, credit unions are more likely to offer credit card services (76%) than banks (59%). This is most likely due to credit unions' focus on consumer payments rather than commercial payments, and is consistent with findings from past surveys. Bill payment, prepaid cards, and remote deposit capture (RDC) are also offered by more than 50% of financial institutions. Financial institutions focus their risk management strategies on payment services they offer, which should be considered when interpreting the survey results.

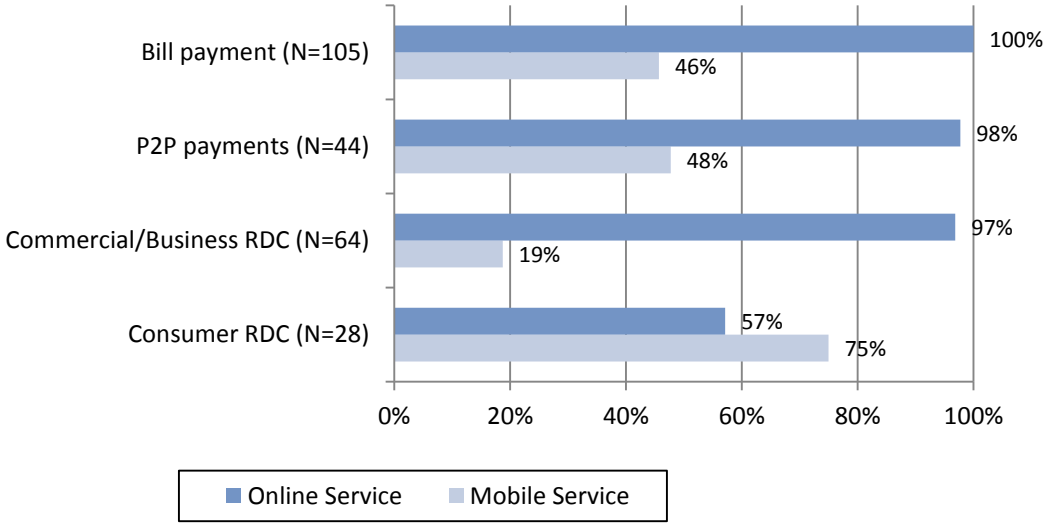
Figure 4: Payment Products and Services Offered
(by % of Financial Institution Respondents)



Q13: Which of the following payments products does your financial institution offer?

For a few payment products, the survey explored whether the service is offered online or via a mobile device (Figure 5). RDC services were also broken down between commercial/business RDC products and consumer RDC products. Online options are used more than mobile services for bill payment, commercial RDC services, and P2P payments, whereas mobile devices are more often used for consumer RDC. The industry's interest has heightened in the security features of online and mobile payments, so it is important to assess payment fraud associated with these forms.

Figure 5: Online and Mobile Services Offered
(by % of Financial Institutions that Offer the Payment Product)

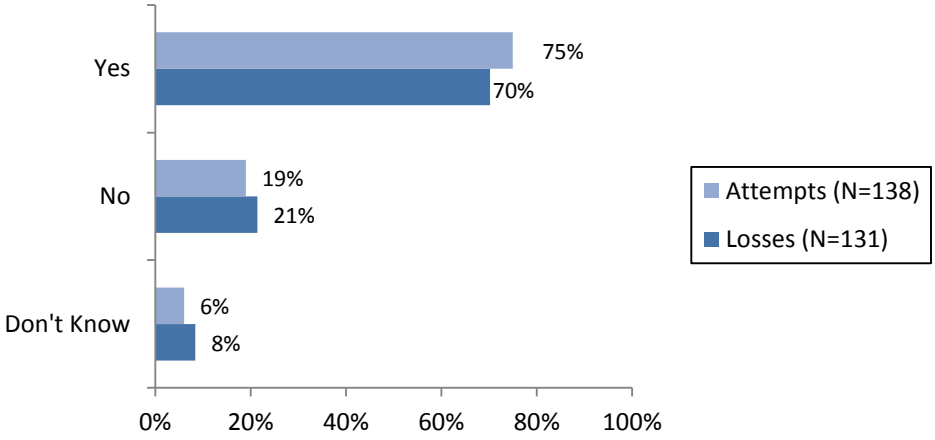


Q13 analysis: For select products offered by the financial institution, is the service offered online and/or via mobile device?

Payment Fraud Attempts and Financial Losses

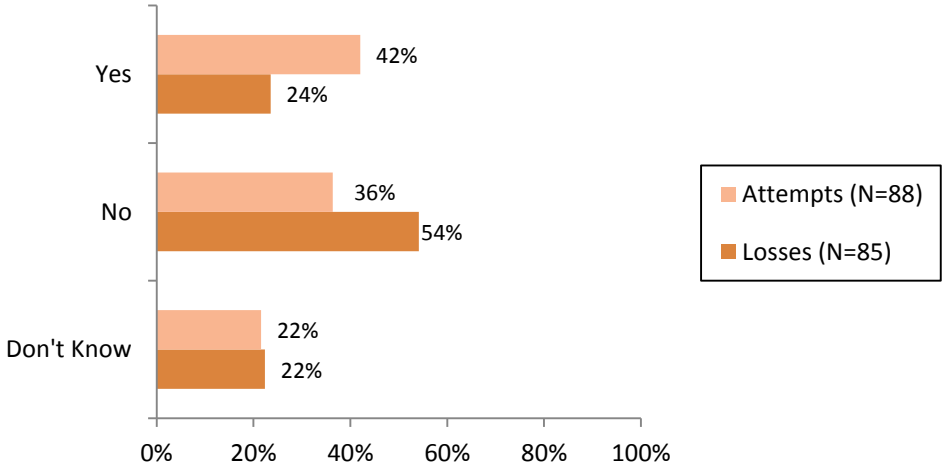
Sixty-two percent of those surveyed report fraud attempts against their organization with 52% actually experiencing losses. Figure 6 shows that 75% of financial institution respondents experienced attempted payments fraud in 2013, and 70% report losses. Figure 7 demonstrates the experience of non-financial firms—i.e., only 42% encountered payments fraud attempts and about a quarter (24%) reported losses from payments fraud. Thus, financial institution respondents are more likely to be the subject of payment fraud attempts and to suffer monetary loss as a result. The percentage of organizations that did not know whether they experienced fraud attempts or losses is notable, especially among non-financial firms where one out of five respondents did not know.

Figure 6: Payment Fraud Attempts and Fraud Losses Experienced in 2013
(by % of Financial Services Respondents)



Q14: Did your organization experience any payment fraud attempts in 2013?
Q18: Did your organization experience any payment fraud losses in 2013?

Figure 7: Payment Fraud Attempts and Fraud Losses Experienced in 2013
(by % of Non-Financial Services Respondents)



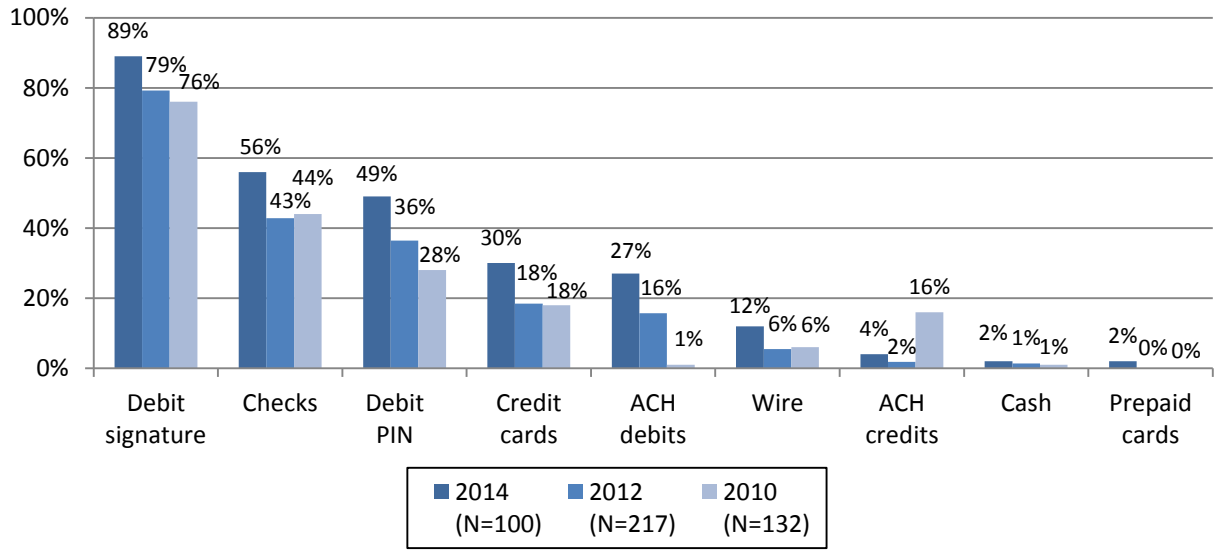
Q14: Did your organization experience any payment fraud attempts in 2013?
Q18: Did your organization experience any payment fraud losses in 2013?

In 2014, respondents who said they experienced fraud attempts were asked to choose and also rank the top three payment types with the highest number of fraud attempts at their organization. For financial institutions, responses to this question remain fairly constant over the past three surveys. Figure 8 shows that a large majority (89%) of financial institutions that experienced fraud attempts, report signature debit as one of the top three payment types with high levels of fraud attempts. Roughly half, or 49%, of financial institutions list PIN debit transactions as among the top three payment types most prone to fraud attempts, which is only slightly lower than the 56% of institutions that include checks in the top three. Interestingly, in terms of ranking, 95% of financial institution respondents specify some type of card as the payment type most prone to fraud attempts (73% cite signature-based debit, 13%

cite PIN-based debit, 8% cite credit cards, and 1% cite prepaid). Only 2% or these respondents identify checks as most prone to fraud attempts.

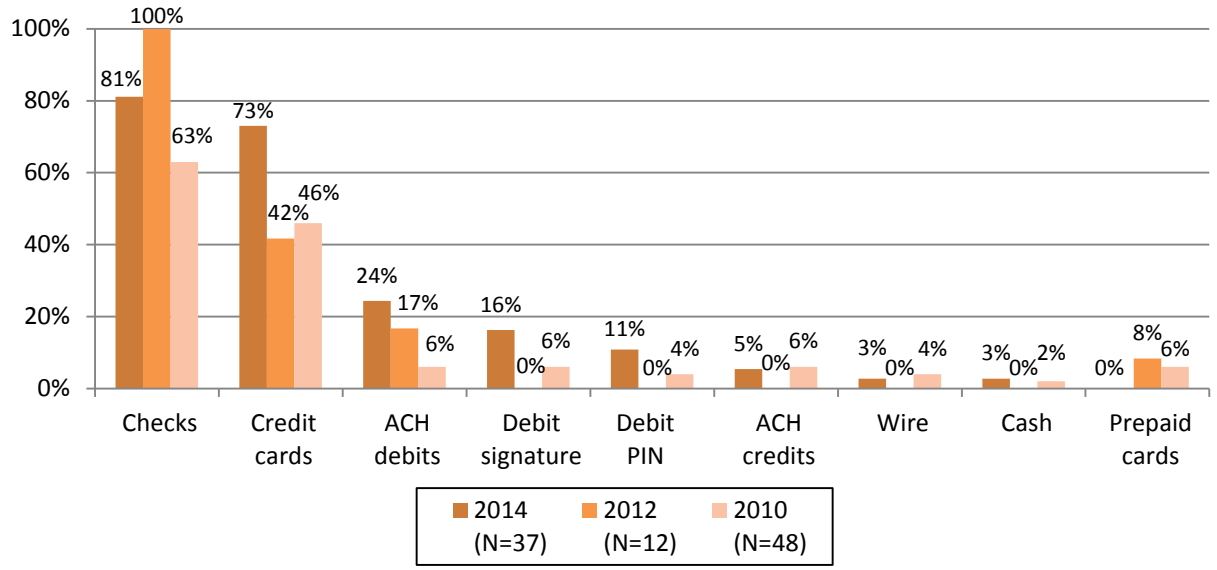
As shown in Figure 9, non-financial firms identify different payment types than financial institutions with the highest number of fraud. More than 80% of non-financial firms include checks in the top three payment types experiencing the highest number of fraud attempts. Credit cards are cited by 73% of non-financial firms as among the top three payment methods prone to fraud attempts. This is a large increase from 2012 and 2010 when 42% and 40% respectively identified credit cards in this category. A greater share of firms also include ACH debits, signature debit card, and PIN debit card in the top three for fraud attempts than in the past, with 24%, 16% and 11% respectively. In terms of ranking, credit card has the greatest share of non-financial firms ranking it as highest in terms of fraud attempts (49%) compared to 38% ranking checks as the highest. Five percent of firms rate ACH debits and signature-based debit cards as having the highest number of fraud attempts.

Figure 8: Top 3 Payment Types with Highest Number of Fraud Attempts
(by % of Financial Services Respondents)



Q15: Indicate the payment types where your organization experienced the highest number of fraud attempts (regardless of actual financial losses) in 2013. (Select and rank up to three that are highest.)

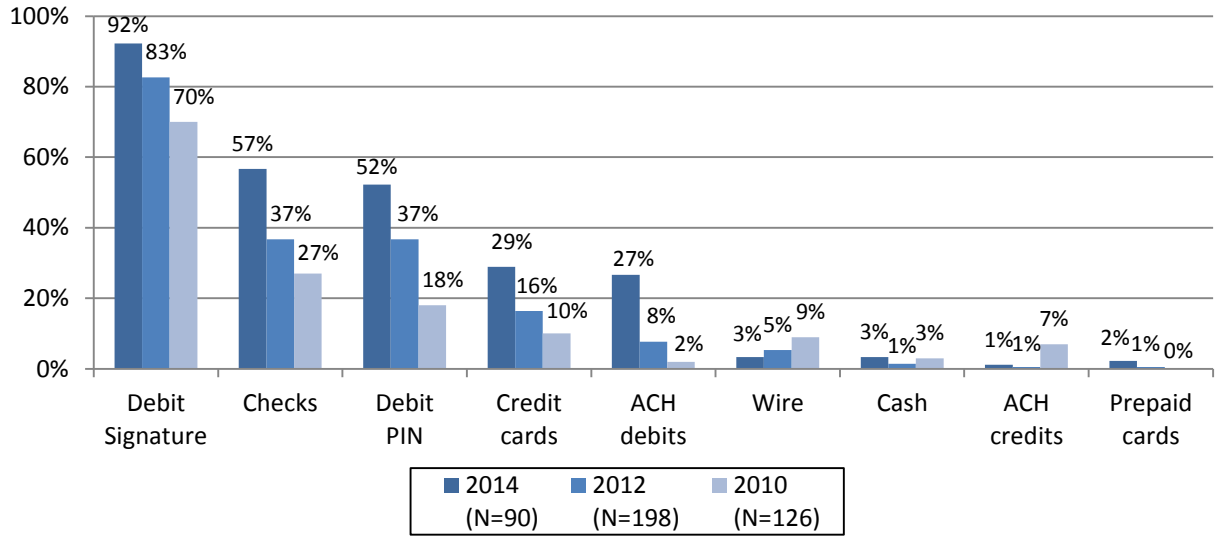
Figure 9: Top 3 Payment Types with Highest Number of Fraud Attempts (by % of Non-Financial Services Respondents)



Q15: Indicate the payment types where your organization experienced the highest number of fraud attempts (regardless of actual financial losses) in 2013. (Select and rank up to three that are highest.)

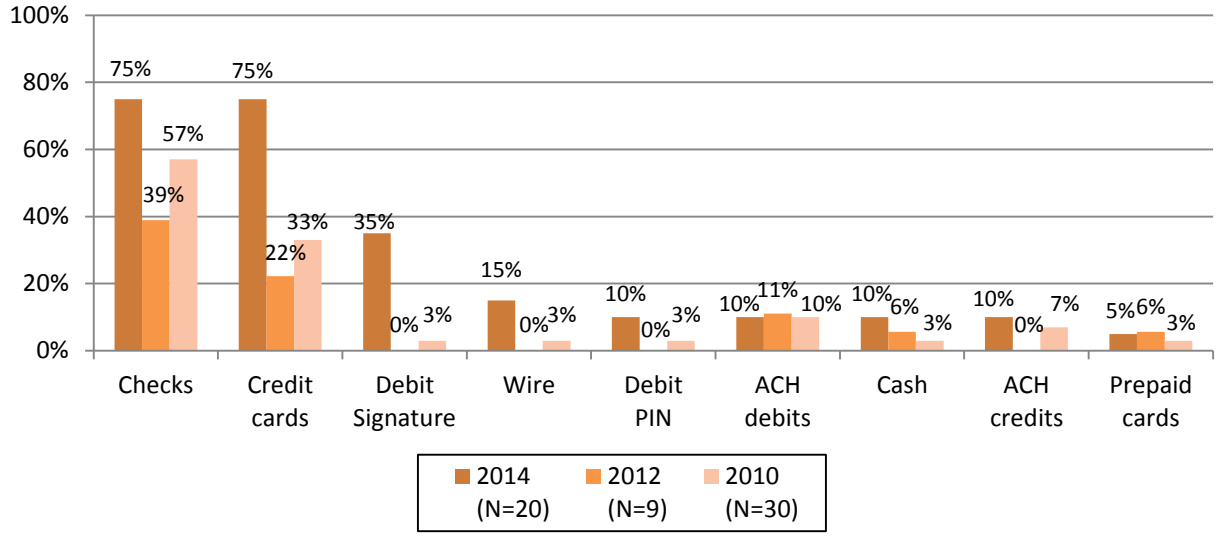
Not surprisingly, the top three payment types with the highest dollar losses (Figures 10 and 11) are mostly the same as the payments with the highest number of attempts (Figures 8 and 9). For financial institution respondents, 92% identify signature debit card among the top three payments with the highest losses and 75% rank it as the highest. Three-quarters of non-financial firms identify checks and credit cards and about a third indicate signature-based debit. Checks and credit cards are both ranked highest in terms of losses by 40% of non-financial firms.

Figure 10: Top 3 Payment Types with Highest Dollar Losses Due to Fraud (by % of Financial Services Respondents)



Q19: Indicate the payment types where your organization has experienced the highest dollar losses due to fraud in 2013. (Select and rank up to three that are highest.)

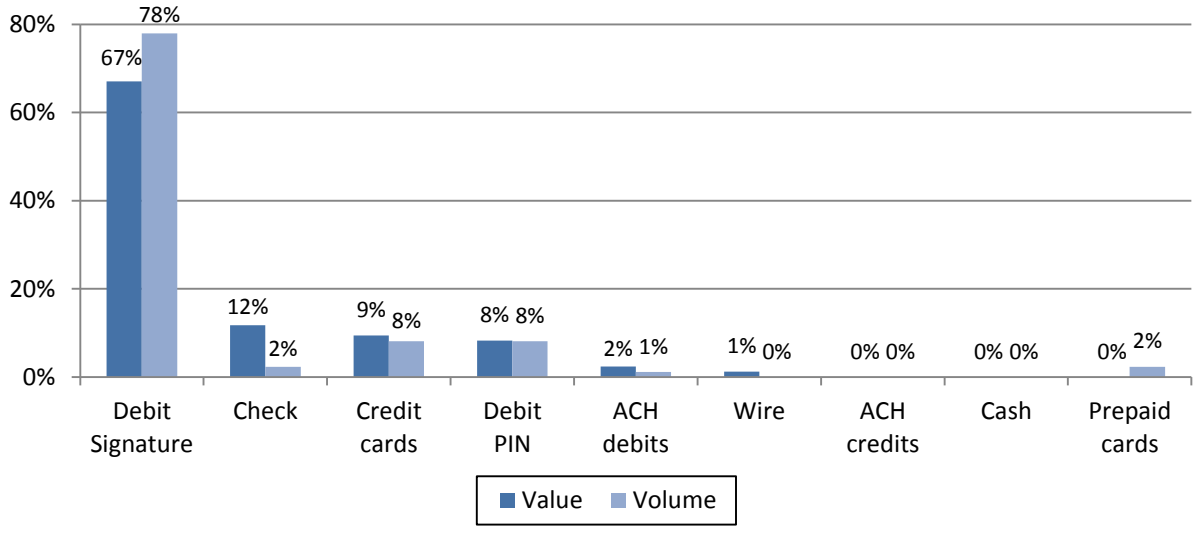
Figure 11: Top 3 Payment Types with Highest Dollar Losses Due to Fraud
(by % of Non-Financial Services Respondents)



Q19: Indicate the payment types where your organization has experienced the highest dollar losses due to fraud in 2013. (Select and rank up to three that are highest.)

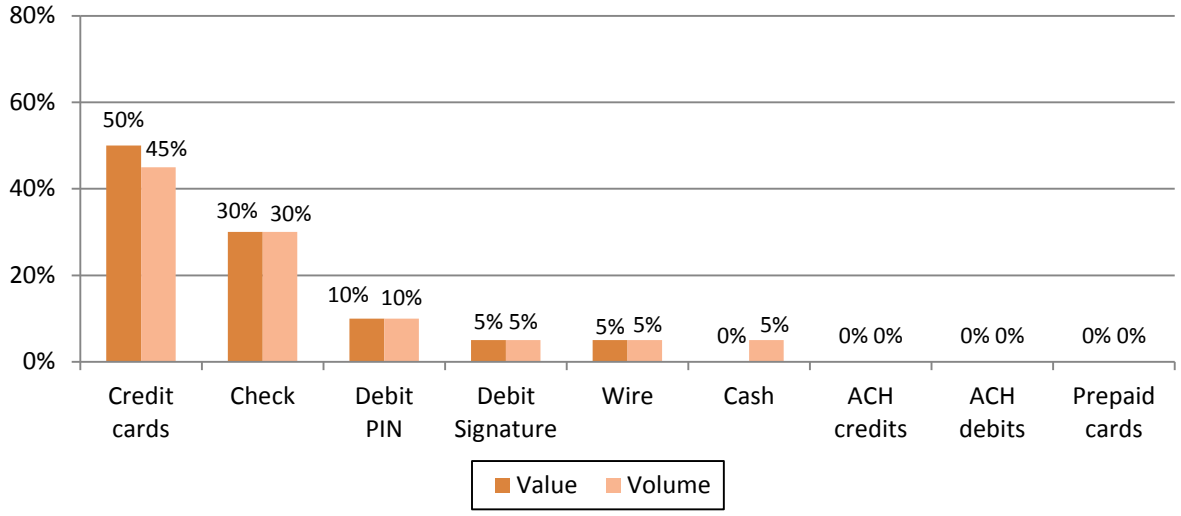
In order to assess risk from another perspective, the survey asked respondents to consider the volume and value of each payment type that they offer or use and identify which payment has the highest rate of loss based on the value or volume of that payment. Over two-thirds of financial institution respondents identify signature debit card as having the highest rate of fraud (Figure 12). About half of non-financial firms identify credit cards as having the highest loss rate based on the value and volume of credit card transactions. Thirty percent identify check transactions.

Figure 12: Payment Type with the Highest Loss Rate Based on Volume and Value of Transactions for Each Payment Type
(by % of Financial Services Respondents (N=85 to 86))



Q20a: Please indicate which payment type has the highest loss rate based on the volume of transactions for that payment type.
Q20b: Please indicate which payment type has the highest loss rate based on the value of transactions for that payment type.

Figure 13: Payment Type with the Highest Loss Rate Based on Volume and Value of Transactions for Each Payment Type
(by % of Non-Financial Services Respondents (N=20))



Q20a: Please indicate which payment type has the highest loss rate based on the volume of transactions for that payment type.
Q20b: Please indicate which payment type has the highest loss rate based on the value of transactions for that payment type.

Notably, fraud *attempts* do not equal successful fraud *events*. Further, even when firms do experience fraud, they do not necessarily incur significant losses. As seen in Figures 6 and 7, 21% of financial institutions and more than half (54%) of non-financial firms report no losses from payments fraud in 2013. This is an improvement over the 2012 survey, when only 6% of financial institutions and 50% of non-financial firms reported no losses in 2011. Table 9 also shows that in 2013, only 6% of financial institution firms report losses that amount to above 0.5% of annual revenues. Only 3% of non-financial firms report losses greater than 0.3% of annual revenues. While any fraud loss is undesirable, these data suggest that in aggregate fraud losses experienced by survey respondents are relatively low.

Table 9: Payments Fraud Financial Losses
(by % of Respondents Data)

Loss Range as a Percent of Annual Revenue	Financial Service Respondents (N=122)[7]	Non-Financial Service Respondents (N=85)	All Respondents (N=207)
No losses	23%	54%	36%
Over 0% -.3%	47%	20%	36%
.3% - .5%	15%	1%	9%
.6% - 1%	4%	0%	2%
1.1% - 5%	2%	2%	2%
Over 5%	0%	0%	0%
Don't know	9%	22%	14%

Q21: For your organization, please estimate the financial losses experienced due to payments fraud during 2013 as a percent of the company's total revenue.

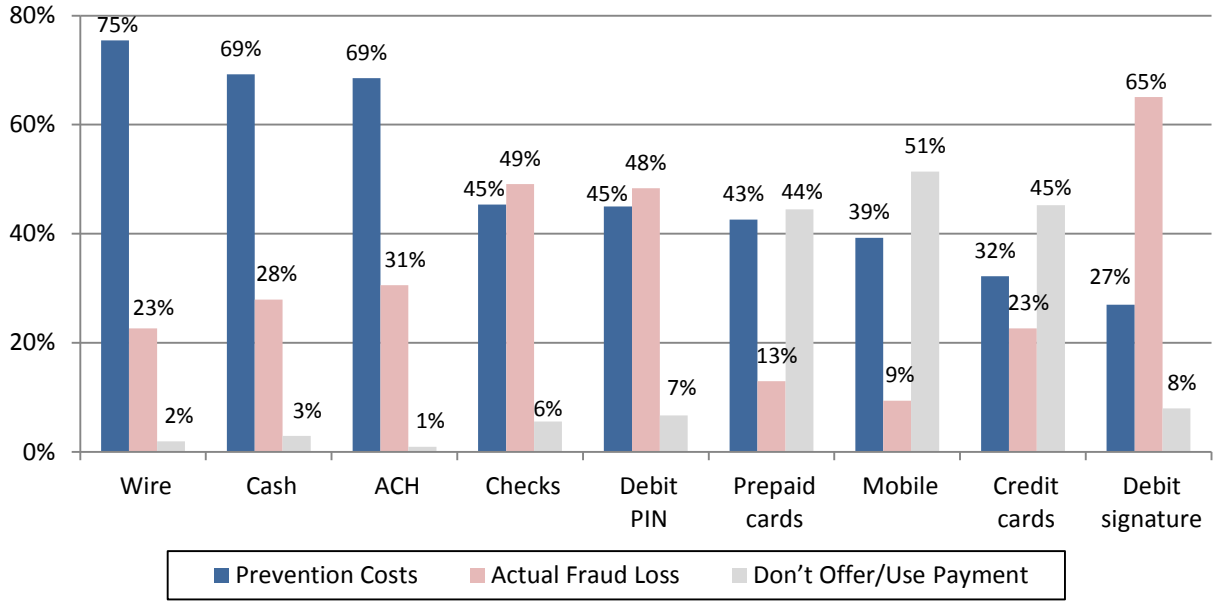
[7] Figure 6 and Table 9 differ in the percent of financial service respondent percentages for "no losses" and "don't know because N=138 in Figure 6 and N=122 in Table 9.

One of the limitations of payment fraud data is that the data often focus solely on losses in the event of actual fraud. In order to understand the true cost of payments fraud to the economy, other factors must be considered. For example, both financial and non-financial firms must invest in infrastructure improvements, fraud mitigation strategies, and loss resolution programs regardless of whether payments fraud has already occurred. For this reason, respondents were asked to report whether fraud prevention costs or actual fraud losses were a greater expense for their organization for each payment type listed—shown in Figures 14 through 17.

Figure 14 uncovers two different ways of looking at fraud costs by payment type within financial institutions. More financial institutions report actual fraud losses exceeding prevention costs in three areas: checks (49%), debit PIN (48%), and debit signature (65%). For all other categories of payments, a higher percentage of financial institutions report that prevention costs are greater than actual losses. This is particularly striking for wire, cash, and ACH payments. More than two-thirds of financial institution respondents report that prevention costs outweigh actual fraud losses for these types of payments.

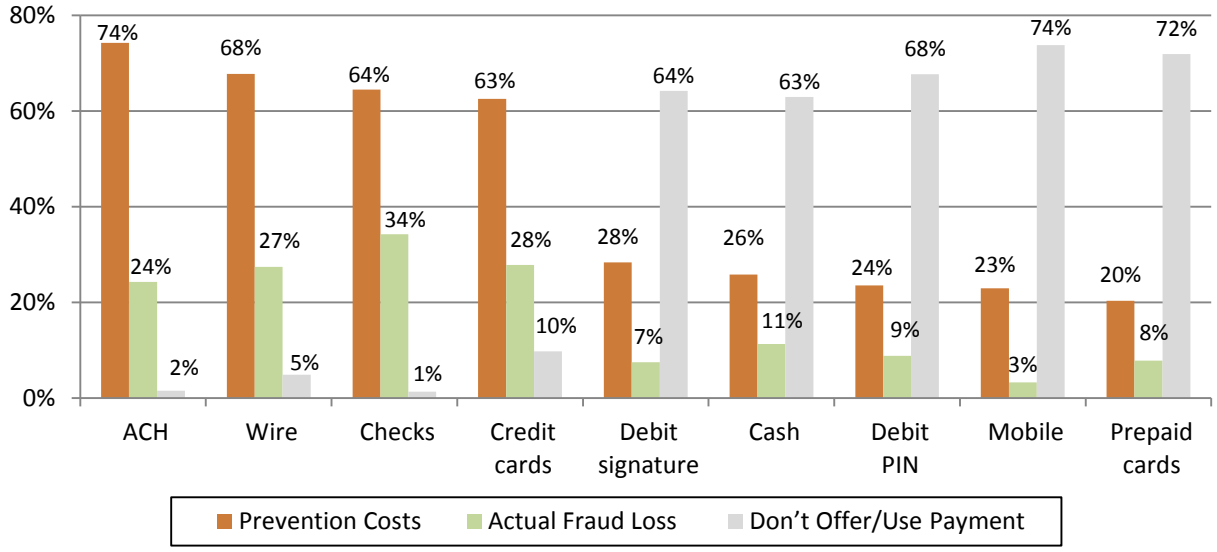
Figure 15 provides insight into how fraud costs impact non-financial firms. For every payment type, a higher percentage of firms respond that prevention costs exceed actual losses. Importantly, high percentages of respondents do not offer nor use signature debit, PIN debit, cash, mobile, and prepaid card payments. This could be due to the fact that primary payment counter-parties are other businesses rather than consumers as discussed earlier (Table 7).

Figure 14: Fraud Prevention Costs versus Actual Fraud Losses
(by % of Financial Services Respondents (N=104 to 126))



Q16: For these payment types, which is a greater expense for your organization–fraud prevention costs or actual dollar losses?

Figure 15: Fraud Prevention Costs versus Actual Fraud Losses
(by % of Non-Financial Services Respondents (N=61 to 76))

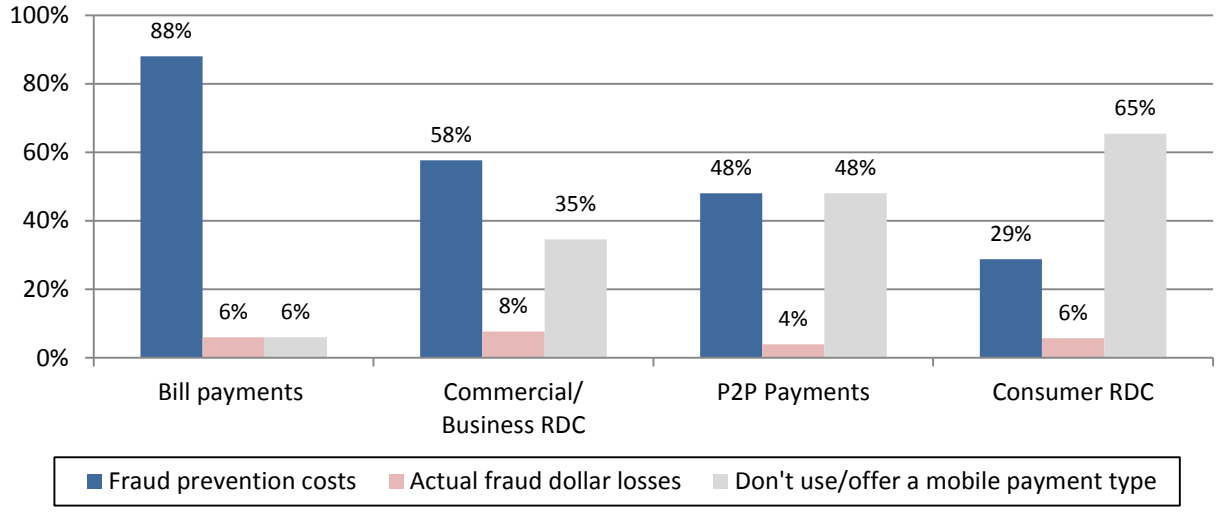


Q16: For these payment types, which is a greater expense for your organization–fraud prevention costs or actual dollar losses?

The relative security of mobile payments is often a topic of debate. Some argue that mobile payments carry high risk, especially if multiple third parties are involved in the transaction, while others contend that mobile devices provide the possibility of higher levels of security. For those organizations that use or offer mobile payment products, the respondents identify which are greater—fraud prevention costs or actual losses caused by fraud. Figures 16 and 17 show that more financial and non-financial firms report higher prevention costs than actual losses for all subtypes of mobile payment services. For financial institutions, 8% or fewer report actual losses as higher than prevention costs for any type of mobile payment service. Non-financial firms are more likely to report higher losses than prevention costs in two categories: mobile bill payments (20% of firms) and commercial/business remote deposit capture products (21%).[8] However, note that the number of non-financial firms actually using these products is low among survey respondents.

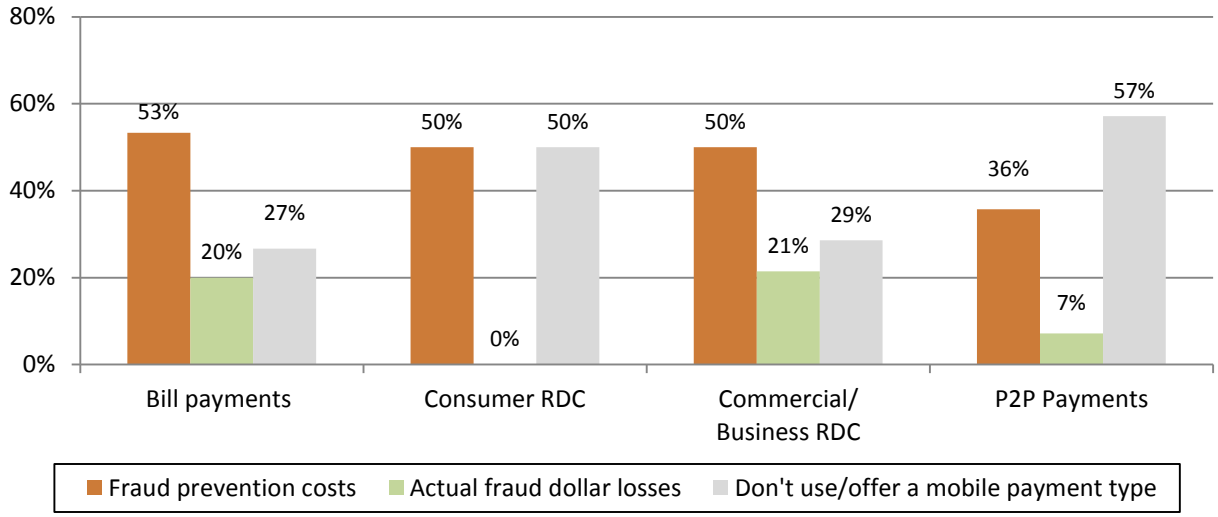
[8] Remote deposit is the ability to deposit a check into a banking account from a remote location, such as an office or home, without having to physically deliver the paper check to the bank. This is accomplished by capturing or scanning a digital image of a check into a computer, then transmitting that image along with additional data to the bank.

Figure 16: Fraud Prevention Costs versus Actual Fraud Losses
(by % of Financial Services Respondents that Offer or Use a Mobile Payment Product (N=50 to 52))



Q17: For mobile payment products, which is a greater expense for your organization– fraud prevention costs or actual fraud dollar losses?

Figure 17: Fraud Prevention Costs versus Actual Fraud Losses
(by % of Non-Financial Services Respondents that Offer or Use a Mobile Payment Product (N=14 to 15))



Q17: For mobile payment products, which is a greater expense for your organization– fraud prevention costs or actual fraud dollar losses?

Finally, for both financial and non-financial firms, it is important to correctly interpret these data. Even if a very high percentage of companies respond that prevention costs are significantly higher than losses, this survey did not ask how much higher those costs are or the value of losses avoided; this question does not get to the underlying issue of proportion. Importantly, the result of higher prevention costs may be much higher potential monetary losses that would have occurred had payments fraud not been prevented. In other words, without those preventive measures in place, the real dollars lost to fraud could have been significantly higher. So while prevention and mitigation efforts should be weighed from a cost/benefit perspective, part of the "cost" assessment is an estimate of fraud losses that are avoided.

Because fraud prevention costs are ongoing and require constant upgrades to infrastructure, it is important to understand fraud loss trends over time. Respondents were asked to gauge whether or not fraud losses had increased, decreased, or stayed the same in 2013 compared to 2012. The vast majority, 74%, of non-financial firms responded that losses remain about the same when considering both years, as depicted in Table 10. The financial institution picture is quite different with only about a quarter experiencing the same level of fraud losses and over half, 51%, reporting increases in the amount of loss experienced. Fifteen percent of those financial institutions classified their loss rate as having increased substantially (10%) or very substantially (5%) (Figure 18). On a positive note, those responding with a very substantial increase are down from 9% reported in the 2012 and 2010 surveys. Further, despite the increases noted here, the total losses estimated as a percentage of revenues remains quite low for most respondents, as shown in Table 9 above.

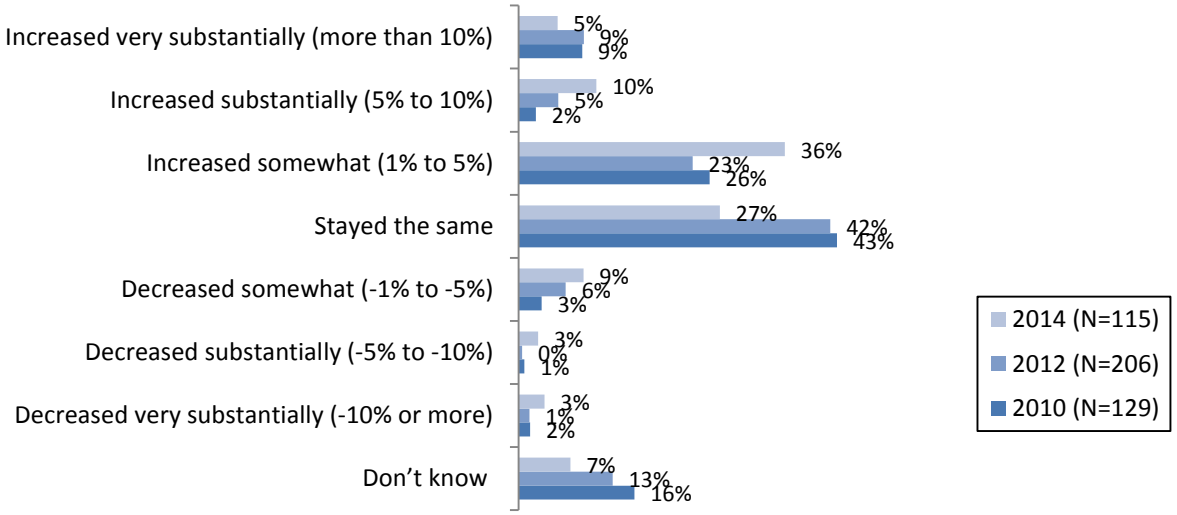
Most non-financial firms continue to report that their fraud loss rate stayed the same (Figure 19). Six percent of the non-financial firms report a very substantial decline in their loss rate in 2013 compared to 2012 while 5% of non-financial firms report a substantial increase in their loss rate.

Table 10: Change in Payment Fraud Losses in 2013 compared to 2012 (by % of Respondents)

Change	Financial Service Respondents (N=115)	Non-Financial Service Respondents (N=66)	All Respondents (N=181)
Increased	51%	11%	36%
Stayed the same	27%	74%	44%
Decreased	15%	9%	13%
Don't know	7%	6%	7%

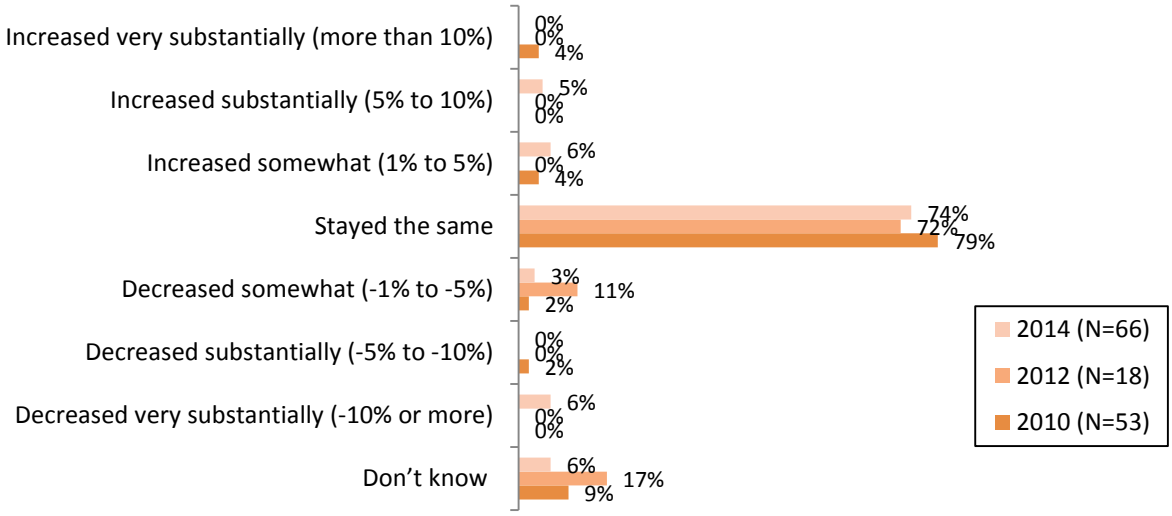
Q22: For your organization, how has the percentage of financial losses due to payments fraud changed in 2013 compared to 2012?

Figure 18: Percent Change in Loss Rate (by % of Financial Services Respondents)



Q22: For your organization, how has the percentage of financial losses due to payments fraud changed in 2013 compared to 2012?

Figure 19: Percent Change in Loss Rate
(by % of Non-Financial Services Respondents)



Q22: For your organization, how has the percentage of financial losses due to payments fraud changed in 2013 compared to 2012?

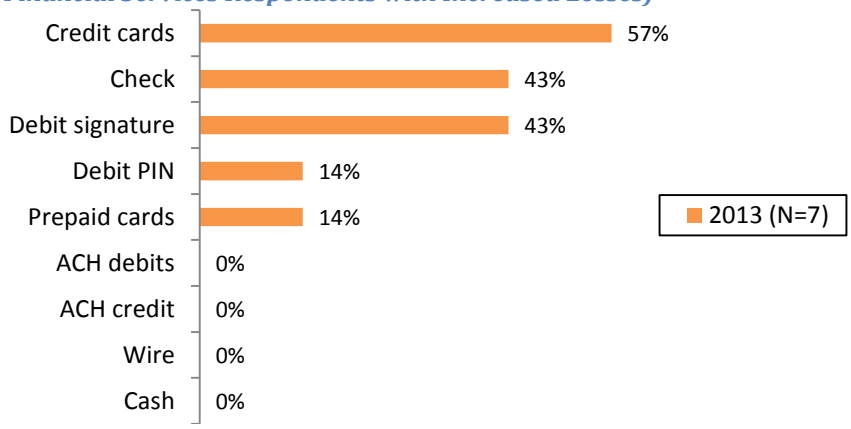
Respondents with an increase in fraud losses were asked to identify one or more payment types associated with the increased loss. Figure 20 provides the results for non-financial firms.[9] More than half, or 57%, of such firms attribute the increase in fraud losses to credit card payments. Checks and signature debit transactions are tied at 43%, while both debit and prepaid cards are noted as a cause of increased loss by 14% of non-financial firms.[10]

Figure 21, which describes payment types responsible for higher losses for financial institutions, tells a much different story. First, the vast majority of financial institutions (89%) attribute some of their increases in losses to signature debit payments. This percentage far eclipses the proportion of financial institutions claiming an increase in losses due to any other payment type, including PIN debit, which comes in at second place with 32% of institutions attributing increased losses to such transactions. Second, the data allows a time series analysis of which payment types are responsible for increases in fraud losses for financial institutions. Trends remain constant year over year.

[9] In the 2012 survey, none of the non-financial firms reported an increase in their loss rate in 2011 compared to 2010. As a result, no comparative data is provided in Figure 20.

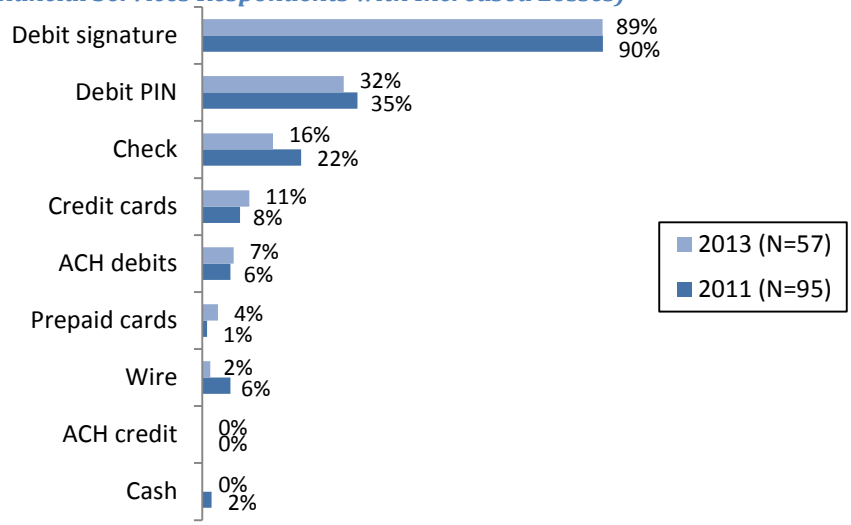
[10] These percentages add up to greater than 100% because respondents were allowed to pick multiple payment types that were responsible for increased losses. We do not know which payment type is associated with the highest increase in losses for any given respondent, as they were not asked to rank order their responses.

Figure 20: Payment Types Attributed to Fraud Loss Increase (by % of Non-Financial Services Respondents with Increased Losses)



Q23: To which payment types do you attribute the 2013 increase in your organization's actual dollar losses?

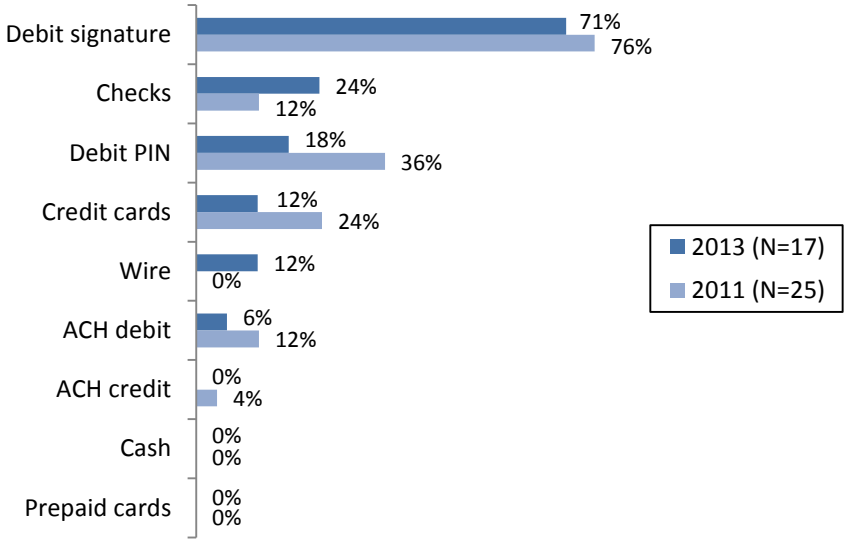
Figure 21: Payment Types Attributed to Fraud Loss Increase (by % of Financial Services Respondents with Increased Losses)



Q23: To which payment types do you attribute the 2013 increase in your organization's actual dollar losses?

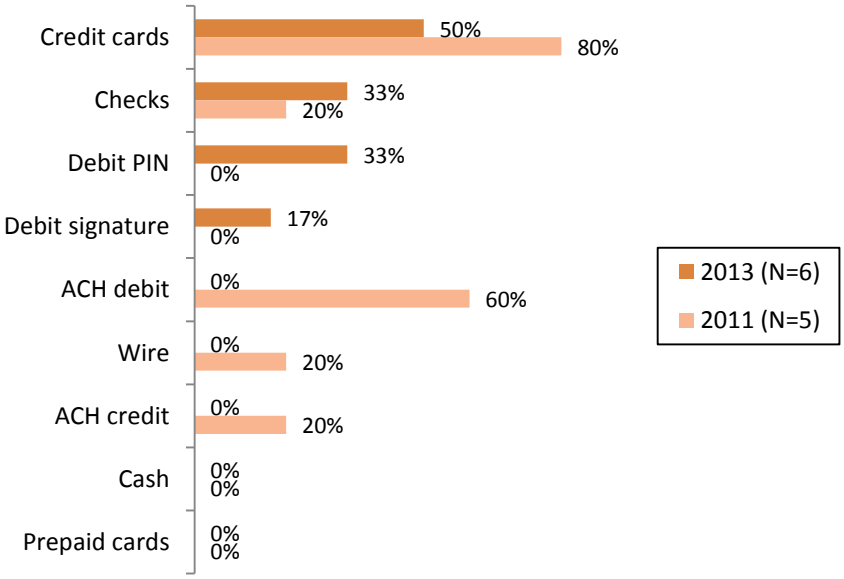
Figures 22 and 23 highlight similar trends for those firms experiencing a decrease in fraud losses. Financial institutions overwhelmingly attribute fraud loss decreases to signature debit, data which suggests that institutions can be successful in reducing card fraud losses. Some of the non-financial firms also report reductions in the same payments that are identified by others as causing an increase in losses. Specifically, these firms report decreased losses in credit cards and checks (Figure 23).

Figure 22: Payment Types Attributed to Fraud Loss Decrease (by % of Financial Services Respondents with Decreased Losses)



Q24: To which payment types do you attribute the 2013 decrease in your organization's actual dollar losses?

Figure 23: Payment Types Attributed to Fraud Loss Decrease (by % of Non-Financial Services Respondents with Decreased Losses)



Q24: To which payment types do you attribute the 2013 decrease in your organization's actual dollar losses?

While important to pinpoint trends related to fraud increases, equally important is to understand why and how firms experienced *decreases* in fraud losses. When financial institutions and non-financial firms were asked whether they had implemented changes to payment risk management that led to a decrease in losses, in the 2012 survey 62% of financial institutions and 60% of non-financial firms responded "yes." However, in 2014, while most financial institutions that reduced losses (71%) responded that they implemented successful risk management practices, only 33% of non-financial firms with reduced losses claimed that such changes led to a decrease in fraud losses (Table 11). The latter

suggests that something else was responsible for the decrease in losses for most firms, or that previously implemented strategies are continuing to work effectively for these firms.

Table 11 also shows that the majority of respondents whose losses stayed the same or increased report they also made key changes that helped control the level of losses. This indicates that these respondents believe their losses would have been greater without changes in risk management practices.

Table 11: Implemented Changes to Payments Risk Management Practices (by % of Respondents)

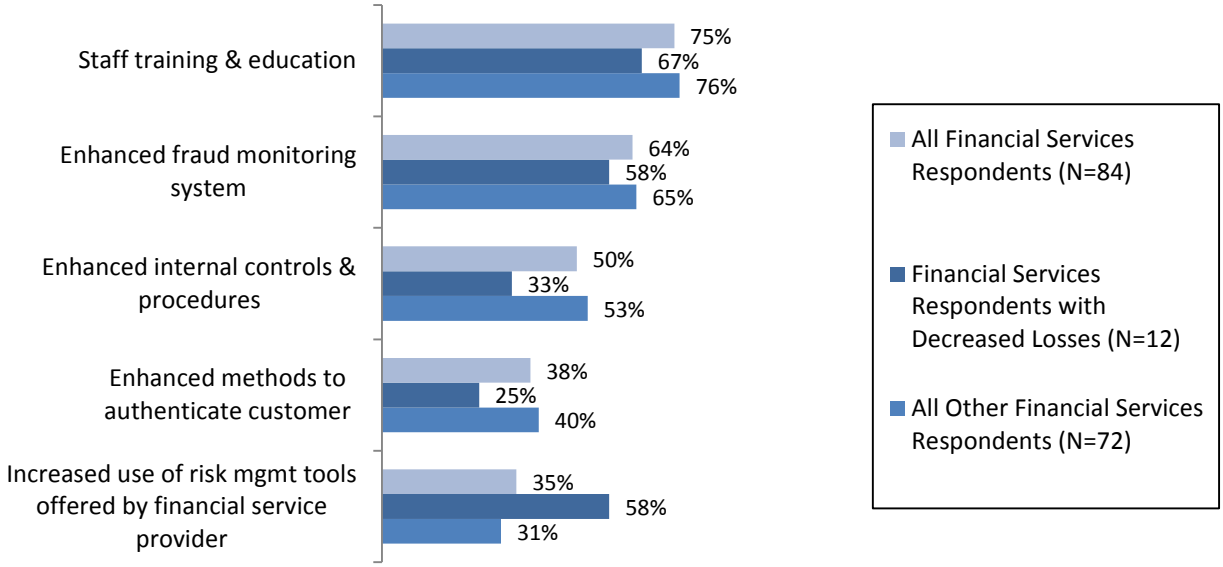
Made Key Changes to Risk Management Practices	Percent of Organizations w/ Decreased Losses		Percent of All Other Organizations		Percent of All Respondents
	Financial Services (N=17)	Non-Financial Services (N=6)	Financial Services (N=111)	Non-Financial Services (N=82)	All Respondents (N=216)
Yes	71%	33%	65%	54%	60%
No	24%	50%	35%	46%	39%
Don't Know	6%	17%	na	na	1%

Q25: Did your organization make changes to its payments risk management practices that led to the decrease in 2013 payments fraud losses?
Q27: Did your organization make changes that helped to control your organization's payments fraud losses?

Figure 24 shows that financial institutions made multiple changes to help control or reduce fraud losses. Over half of the financial institutions reported enhanced staff training and education, enhanced fraud monitoring systems and enhanced internal controls and procedures. Nearly all of the financial institutions that implemented enhanced fraud monitoring systems applied them to debit card transactions (Figure 25).

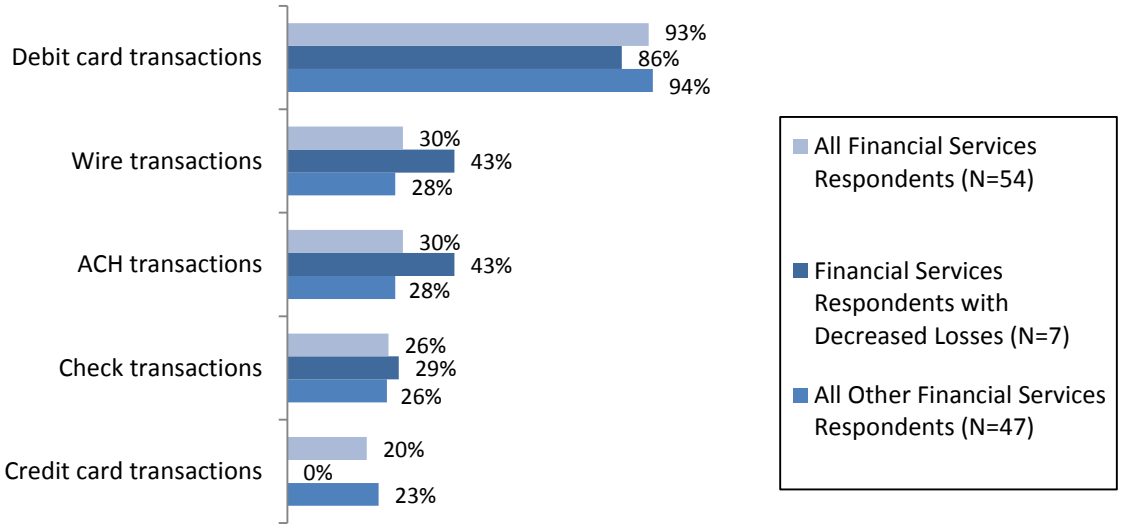
Two-thirds of the non-financial firms also reported changes to staff training and education and enhanced internal controls and procedures. About half of the firms identified changes to enhance methods to authenticate their customers (Figure 26). Keep in mind that three-quarters of the non-financial firms stated that fraud loss rates year-to-year stayed the same. Although a smaller share of non-financial firms (22%) indicated that they enhanced fraud monitoring systems, those that did, apply them to multiple transaction types. Over 50% of firms that made such enhancements applied them to ACH, credit card, and check transactions.

Figure 24: Key Changes Made to Payments Risk Management Practices (by % of Financial Services Respondents that Made Changes)



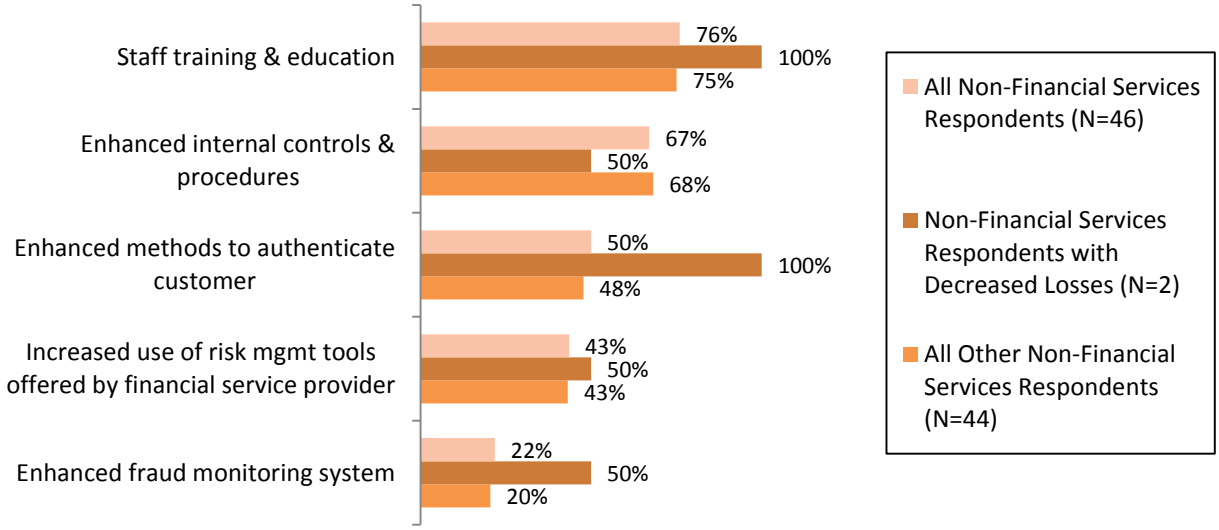
Q26: What are the key changes made by your organization that you think have contributed to the decrease in your organization's payments fraud losses?
Q27a: Which of the following changes did your organization make that helped to control your organization's payments fraud losses?

Figure 25: Payments to Which Enhanced Fraud Monitoring Applies (by % of Financial Services Respondents)



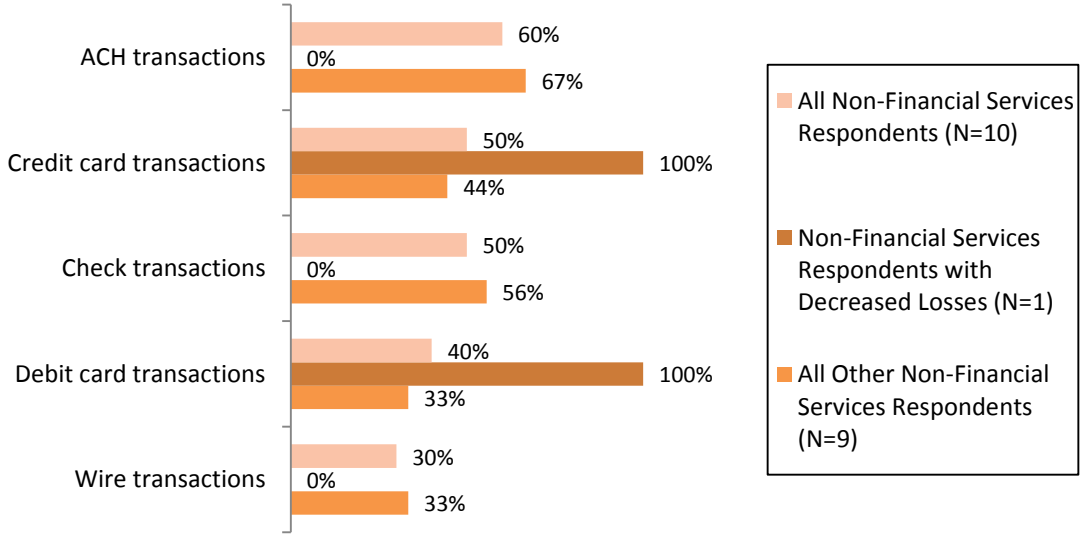
Q26 and Q27a: To which payments does enhanced monitoring apply?

Figure 26: Key Changes Made to Payments Risk Management Practices
(by % of Non-Financial Services Respondents that Made Changes)



Q26: What are the key changes made by your organization that you think have contributed to the decrease in your organization's payments fraud losses?
Q27a: Which of the following changes did your organization make that helped to control your organization's payments fraud losses?

Figure 27: Payments to Which Enhanced Fraud Monitoring Applies
(by % of Non-Financial Services Respondents)



Q26 and Q27a: To which payments does enhanced monitoring apply?

Perpetrators Involved in Successful Payments Fraud

Consistent with past surveys, respondents continue to report external parties as the main perpetrators of successful payments fraud. In the 2014 survey, 77% of respondents report that external parties are responsible for 100% of the payments fraud against their organization. Three percent of respondents report that internal parties are responsible for all successful payments fraud and the same share of respondents are unable to determine the parties involved (Figure 12).

Table 12: Successful Fraud by Perpetrators Involved
(by % of Respondents with Payment Fraud Losses (N=79))

Perpetrator Category	Portion of Successful Fraud by Perpetrators Involved				
	100%	76% - 99%	51% - 75%	26% - 50%	1% - 25%
Internal Only	3%	3%	0%	1%	4%
Internal w/External Parties	1%	0%	0%	1%	4%
External Only	77%	3%	5%	1%	0%
Could Not Determine	3%	0%	0%	1%	5%

Q29: For payment fraud that was successful, please estimate the percentage that involved: only internal staff; internal staff collaborating with external parties; only external parties; unknown – could not determine. (Answers should total 100%.)

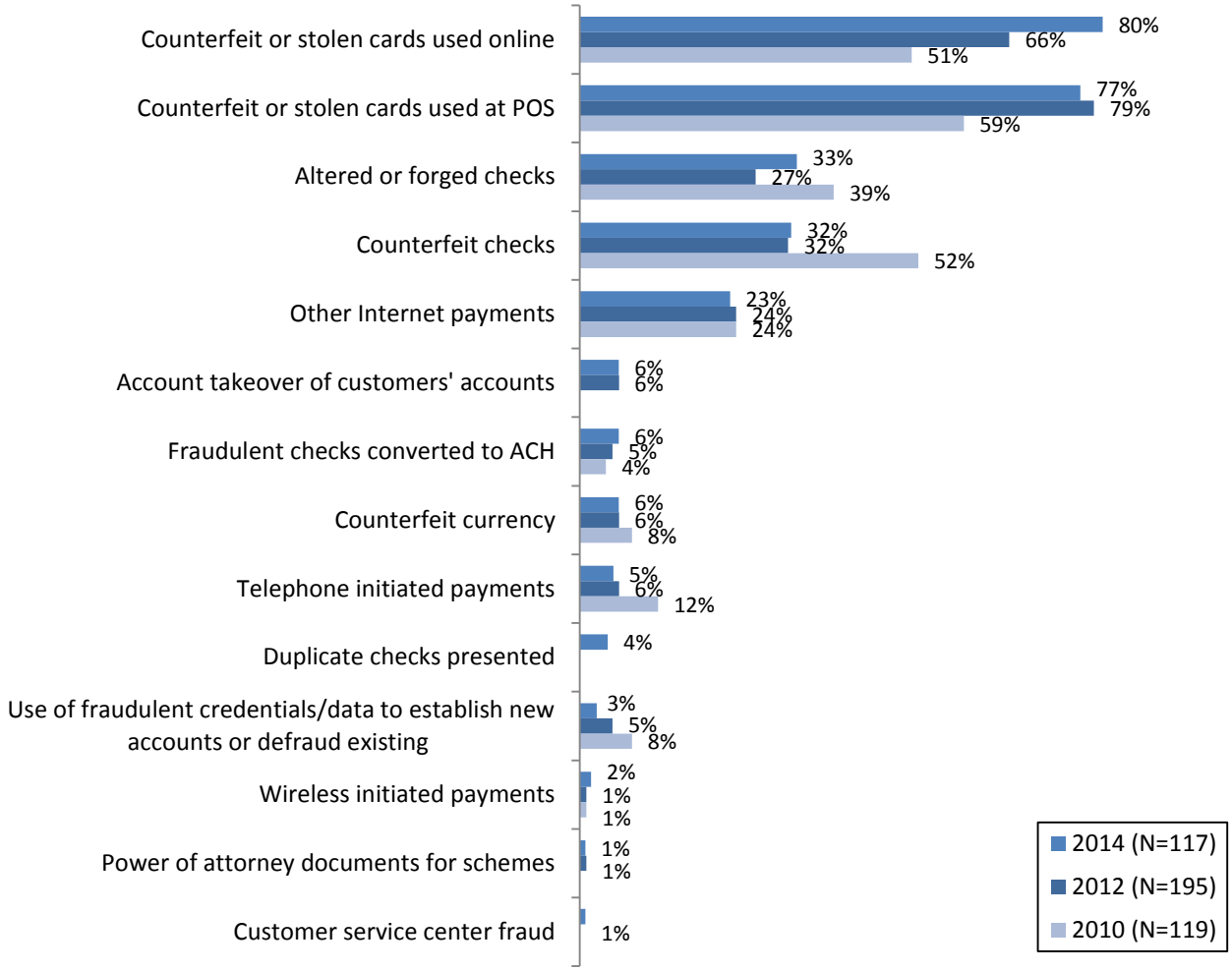
Most Common Fraud Schemes

Respondents were asked to list and rank the top three schemes used most often to initiate payments fraud in the following areas:

- Payments by or on behalf of financial institutions' customers (Figure 28)
- Payments against the respondent's own bank accounts (Figure 29 and 30)
- Payments received or accepted by non-financial firms (Figure 31)

For the fourth consecutive survey, a higher percentage of financial institutions identify counterfeit and stolen cards used online and counterfeit or stolen cards used at the point of sale as being in the top three most used fraud schemes involving payments by or on behalf of the financial institutions' customers. Notable is growth in the share of financial institutions that identify counterfeit or stolen cards used online—from about 50% in 2010 to 80% in the 2014 survey. Over two-thirds of the financial institutions rank the counterfeit/stolen card schemes described above as the most common and the second most common scheme. A third of financial institutions list altered or forged checks (33%) and counterfeit checks (32%) in the top three fraud schemes involving their customers' accounts. The vast majority of those selecting altered/forged and counterfeit checks rank it as the third most commonly used scheme involving payments by or on behalf of their customers.

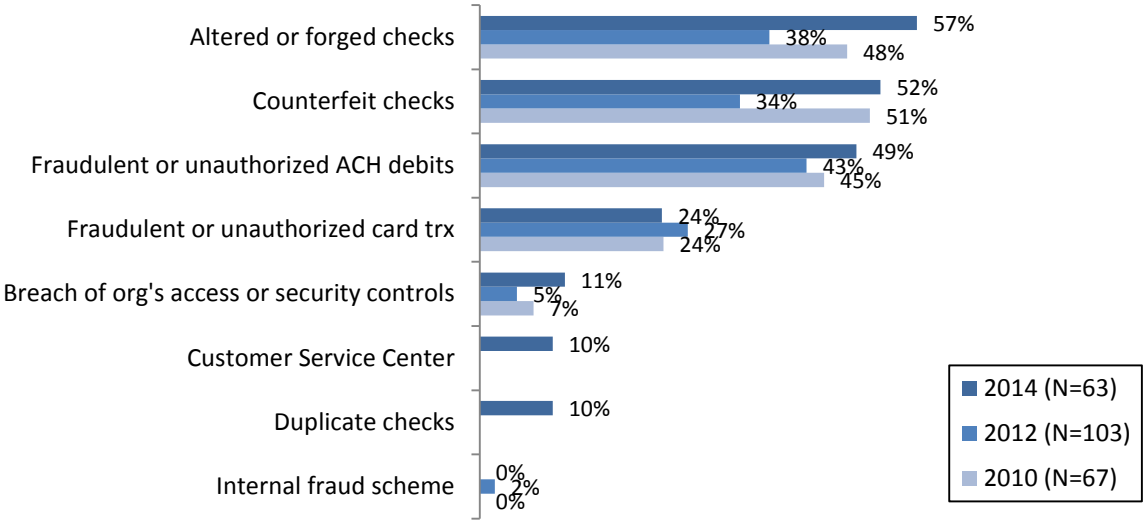
Figure 28: Top 3 Current Fraud Schemes Most Often Used Involving Payments by or on Behalf of Financial Services' Customers
(by % of Financial Services Respondents)



Q31: For payments by or on behalf of your customers, what are the three current fraud schemes that fraudsters are using most often to initiate payments fraud? (Select and rank up to three that are most common.)

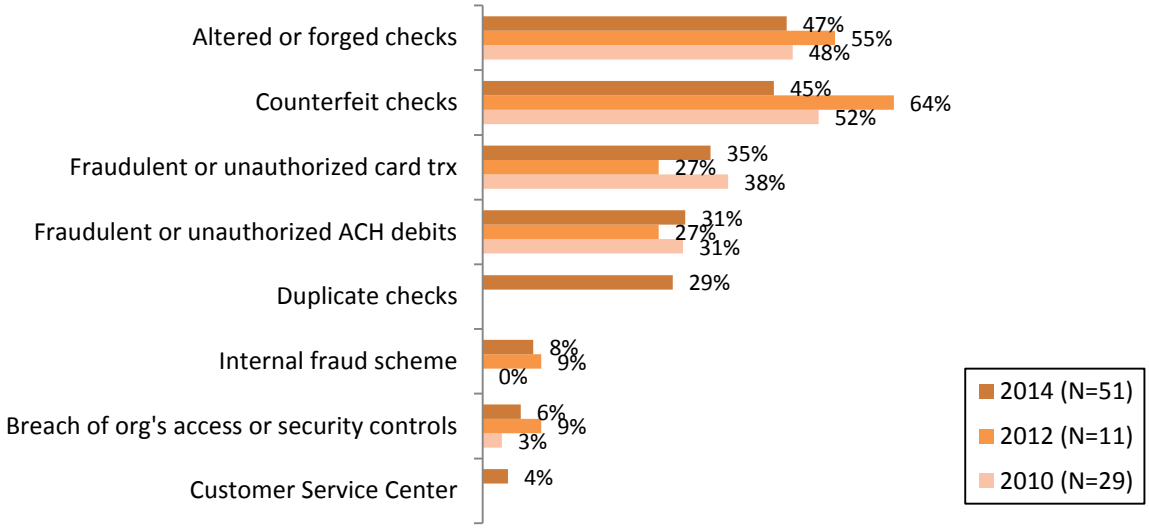
Both financial and non-financial firms were asked about the most common fraud schemes against their own banking accounts. For a non-financial firm, this would be accounts that it holds at financial institutions such as checking accounts or credit card accounts. For all organizations that experienced attempts against their own accounts, altered and forged checks followed by counterfeit checks are among the top three schemes for financial institutions (Figure 29) and non-financial firms (Figure 30). In terms of ranking, these two schemes are also ranked as the most common scheme by respondents.

Figure 29: Top 3 Current Fraud Schemes Most Often Used Involving Organization's Own Accounts (by % of Financial Services Respondents)



Q32: Against your organization's own bank accounts, what are the three current fraud schemes that fraudsters are using most often to initiate payments fraud? (Select and rank up to three that are most common.)

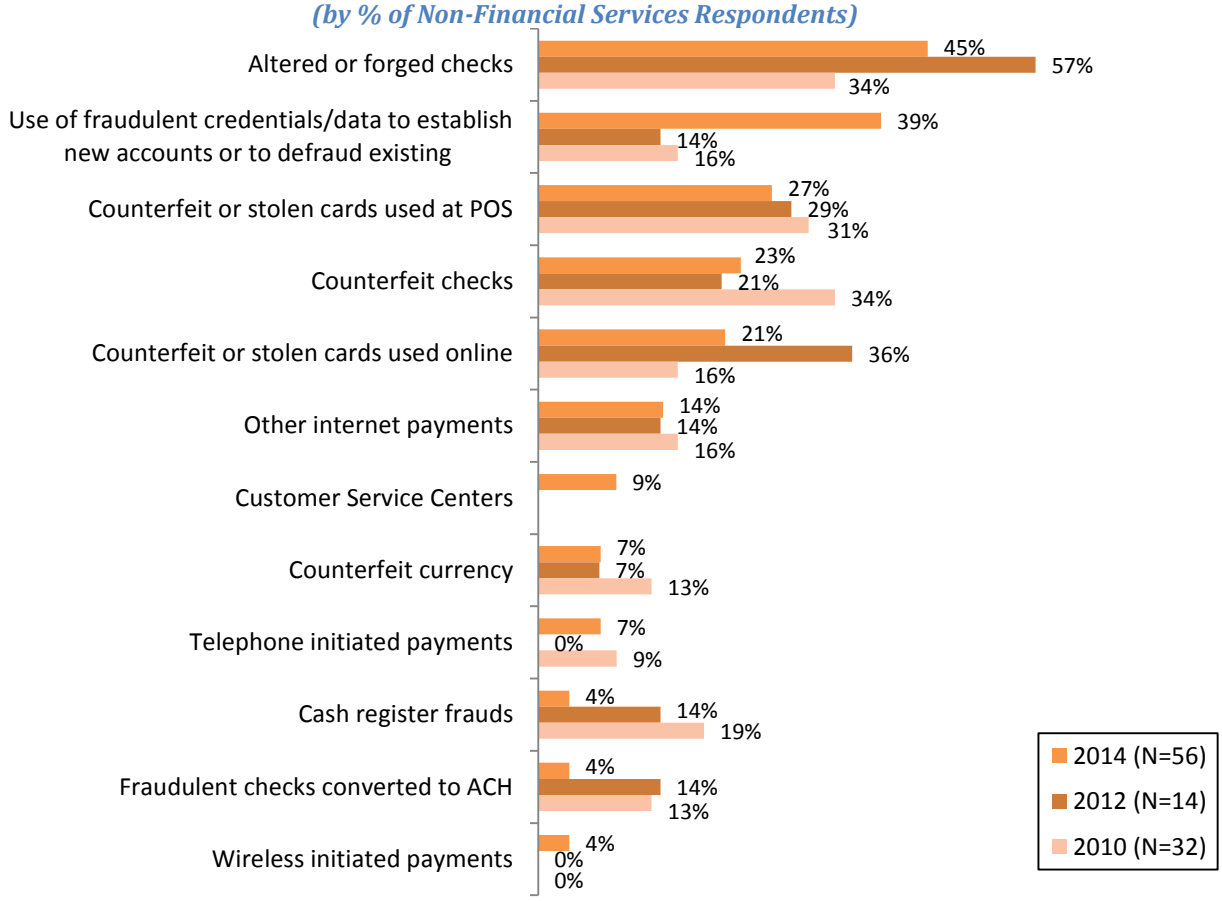
Figure 30: Top 3 Current Fraud Schemes Most Often Used Involving Organization's Own Accounts (by % of Non-Financial Services Respondents)



Q32: Against your organization's own bank accounts, what are the three current fraud schemes that fraudsters are using most often to initiate payments fraud? (Select and rank up to three that are most common.)

Non-financial firms were asked about payments fraud schemes involving payments that they receive. Figure 31 shows that 39% of non-financial firms list fraudulent credentials or data used to establish new accounts or defraud existing accounts as among the top three fraud schemes in 2014, compared to 14% in 2012 and 16% in 2010. Altered/forged checks are cited as a top fraud scheme by 45% of non-financial firms and also ranked as the most common scheme by 32% of the firms. Counterfeit or stolen cards used at the POS are cited by 27% of these firms as being one of the top fraud schemes.

Figure 31: Top 3 Current Fraud Schemes Involving Payments Received (by % of Non-Financial Services Respondents)



Q30: For payments received by your organization, what are the three current fraud schemes that fraudsters are using most often to initiate payments fraud? (Select and rank up to three that are most common.)

Criminals find creative ways to perpetrate payments fraud. Firms that are seeking to combat or prevent fraud must contend with an array of tactics that can lead to attempted or real data compromise and payments fraud. Table 13 outlines the top three information sources used in fraud schemes for both financial institutions and non-financial firms.

The 2014 survey reveals that a top source of information used by fraudsters is compromised sensitive information obtained from lost or stolen cards, checks, or other physical documents or devices while in the consumer's control, as reported by 46% of financial institutions and 31% of non-financial firms. Although higher than any other, this information source declined significantly from the previous survey (60% of financial institutions and 62% of non-financial companies). A slight increase in email and webpage cyber-attacks along with data breaches due to computer hacking are cited by an increased share of financial institutions over 2012 responses. Other notable trends include the substantial reduction in the share of non-financial firms that list their organization's information being obtained from a legitimate check issued by the organization as a top source of information for payments fraud (29% in 2014 compared to 69% in 2012).

Moreover, for the first time, in 2014, respondents were allowed to choose "unknown" as a top information source used to commit fraud. Importantly, this category is listed by the highest percentage of non-financial firms (49%), and by the second-highest percentage of financial institutions (39%). While comparisons to previous years' responses cannot be made, these results indicate that organizations often remain unaware of the nature of the compromise that led to successful payments fraud. "Social engineering" was also added as a potential data compromise source in 2014; 15% of financial institutions and 12% of non-financial firms see this as one of the most significant ways that criminals were able to obtain information to perpetrate payments fraud.[11]

Table 13: Top 3 Information Sources Used in Fraud Schemes

Information Sources	2014			2012			2010		
	FS (N=110)	Non-FS (N=59)	All Orgs (N=169)	FS (N=181)	Non-FS (N=13)	All Orgs (N=194)	FS (N=107)	Non-FS (N=30)	All Orgs (N=137)
Unknown	39%	49%	43%	na	na	na	na	na	na
"Sensitive" information obtained from lost or stolen card, check, physical document or device while in consumer's control	46%	31%	41%	60%	62%	62%	54%	30%	49%
Email and webpage cyber-attacks to obtain "sensitive" customer information, e.g., phishing, spoofing	38%	22%	33%	31%	31%	32%	49%	17%	42%
Data breach due to computer hacking	35%	10%	26%	23%	0%	22%	6%	3%	5%
Physical device tampering, e.g., use of skimmer on POS terminal to obtain magnetic stripe information	29%	14%	24%	35%	8%	34%	41%	3%	33%
Organization's information obtained from a legitimate check issued by your organization	18%	29%	22%	15%	69%	19%	22%	53%	29%
Information about customer obtained by family or friend	23%	8%	18%	27%	0%	26%	19%	20%	19%
Social engineering	15%	12%	14%	na	na	na	na	na	na
Employee with legitimate access to organization or customer information	2%	5%	3%	1%	8%	2%	1%	23%	6%
Lost or stolen physical documentation or electronic devices while in control of the organization	1%	7%	3%	4%	8%	5%	8%	0%	7%

Q33: In your response to the last two questions, you identified the most often used fraud schemes in payments fraud attempts experienced by your organization. What are the top three sources of information fraudsters used for these attempts? (Select and rank up to three that are most common.)

[11] Social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures.

Payments Fraud Mitigation Strategies

In order to keep up with the constantly evolving strategies that criminals use to commit payments fraud, firms must be vigilant in developing and implementing a variety of strategies to prevent fraud from occurring and lessen its impact in cases when it is successful. For the purposes of this survey, fraud mitigation strategies were broken down into four categories and the relative effectiveness is captured and examined from the respondents' experience. These categories were:

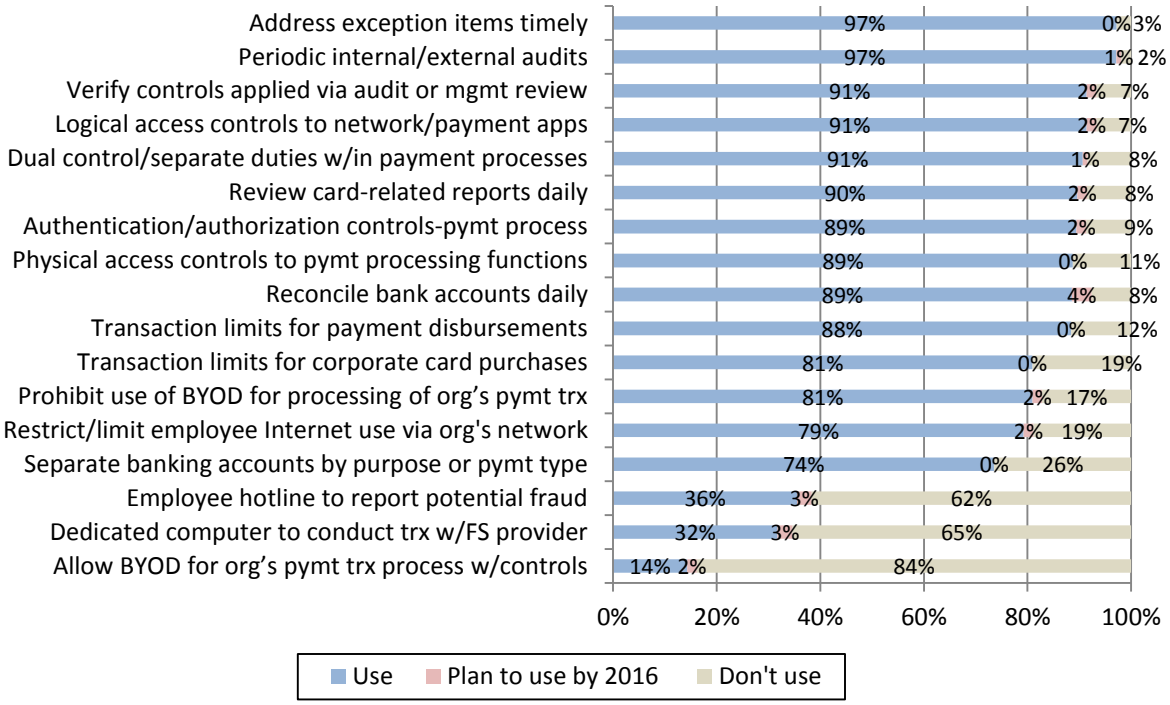
1. Internal controls[12] and procedures
2. Customer authentication methods
3. Transaction screening and risk management methods
4. Risk mitigation services provided by financial institutions

Internal Controls and Procedures

Internal controls and procedures are the fraud mitigation tools that are most likely to be used by both financial institutions and non-financial firms. More than 80% of financial institution respondents use 12 or more of the internal controls listed on Figure 32 and believe they are highly effective. Almost 100% of firms list these top 12 internal control procedures as very or somewhat effective (Figure 34). These trends are similar to survey year 2012 results. While non-financial firms are somewhat less likely to utilize these internal controls, usage rates are still high. More than 80% of non-financial firms use seven or more internal control procedures, as highlighted in Figure 33. All of these top seven procedures are rated very or somewhat effective by 100% of non-financial firms in 2014 (Figure 35).

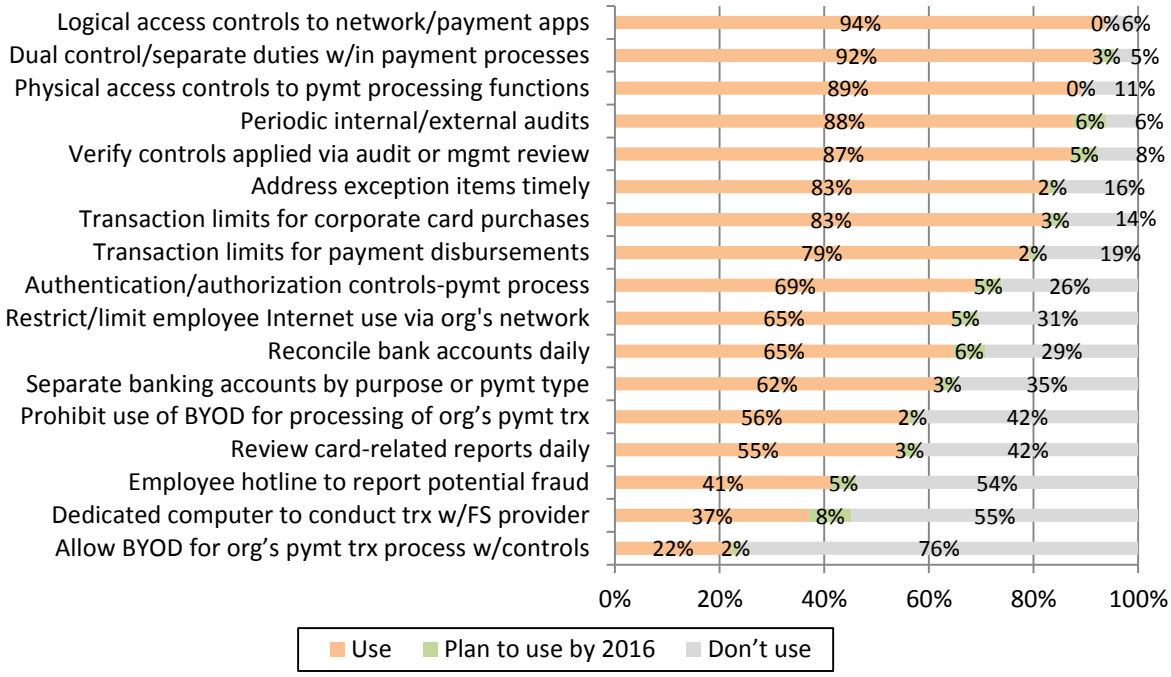
[12] Internal controls are systematic measures (such as reviews, checks and balances, methods and procedures) instituted by an organization to conduct its business in an orderly and efficient manner, safeguard its assets and resources, deter and detect errors, fraud, and theft, ensure accuracy and completeness of its accounting data, produce reliable and timely financial and management information, and ensure adherence to its policies and plans.

Figure 32: Use of Internal Controls and Procedures
(by % of Financial Services Respondents (N=104 to 107))



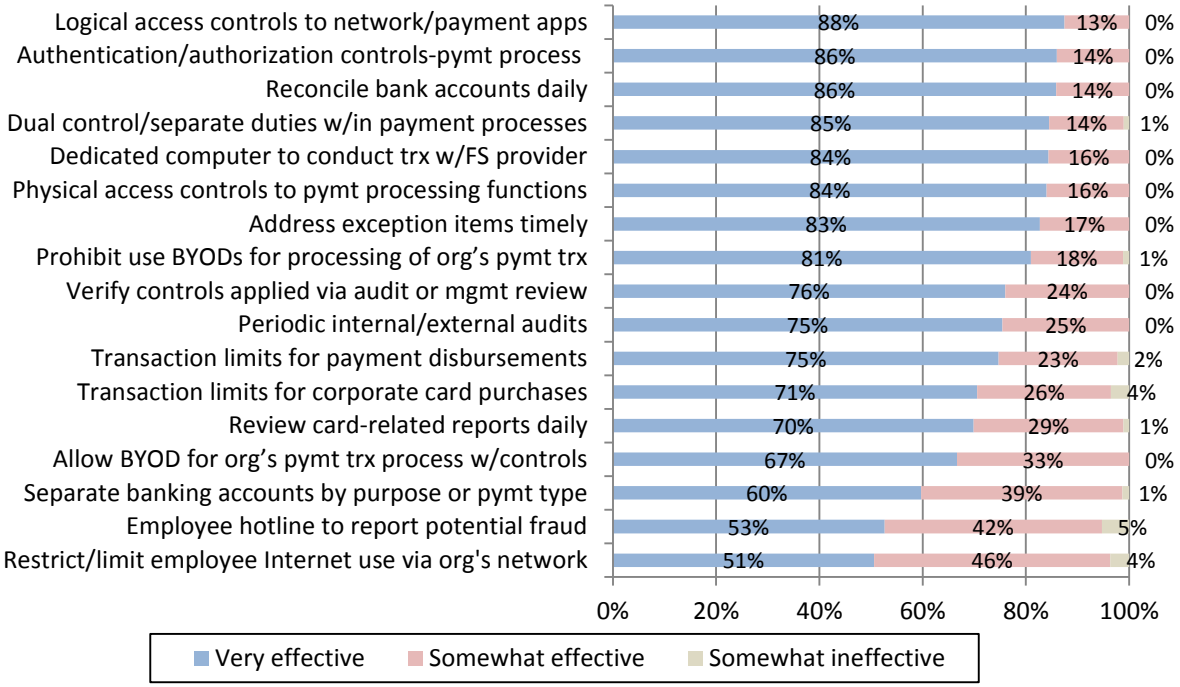
Q38: Which of the following internal controls and procedures does your organization currently use or plan to use?

Figure 33: Use of Internal Controls and Procedures
(by % of Non-Financial Services Respondents (N=62 to 66))



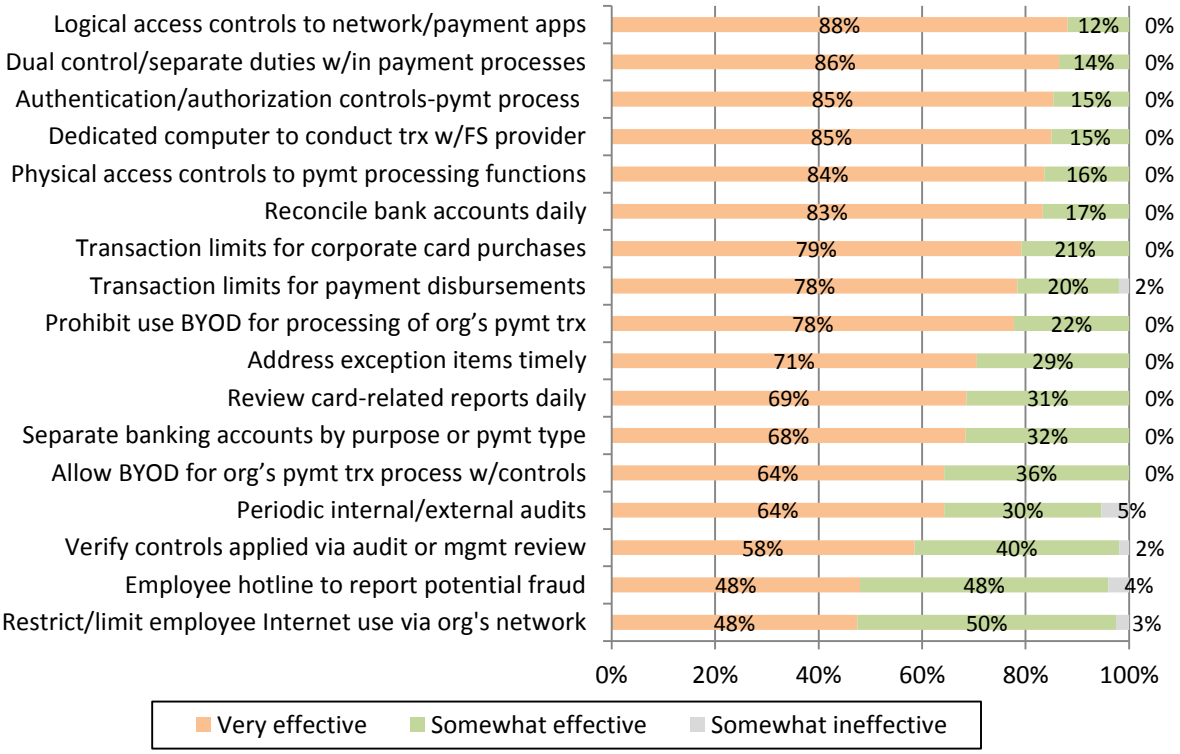
Q38: Which of the following internal controls and procedures does your organization currently use or plan to use?

Figure 34: Effectiveness of Internal Controls and Procedures
(by % of Financial Services Respondents Using It (N=15 to 102))



Q39: Please rate the effectiveness of the internal controls and procedures currently used by your organization.

Figure 35: Effectiveness of Internal Controls and Procedures
(by % of Non-Financial Services Respondents Using It (N=20 to 59))



Q39: Please rate the effectiveness of the internal controls and procedures currently used by your organization.

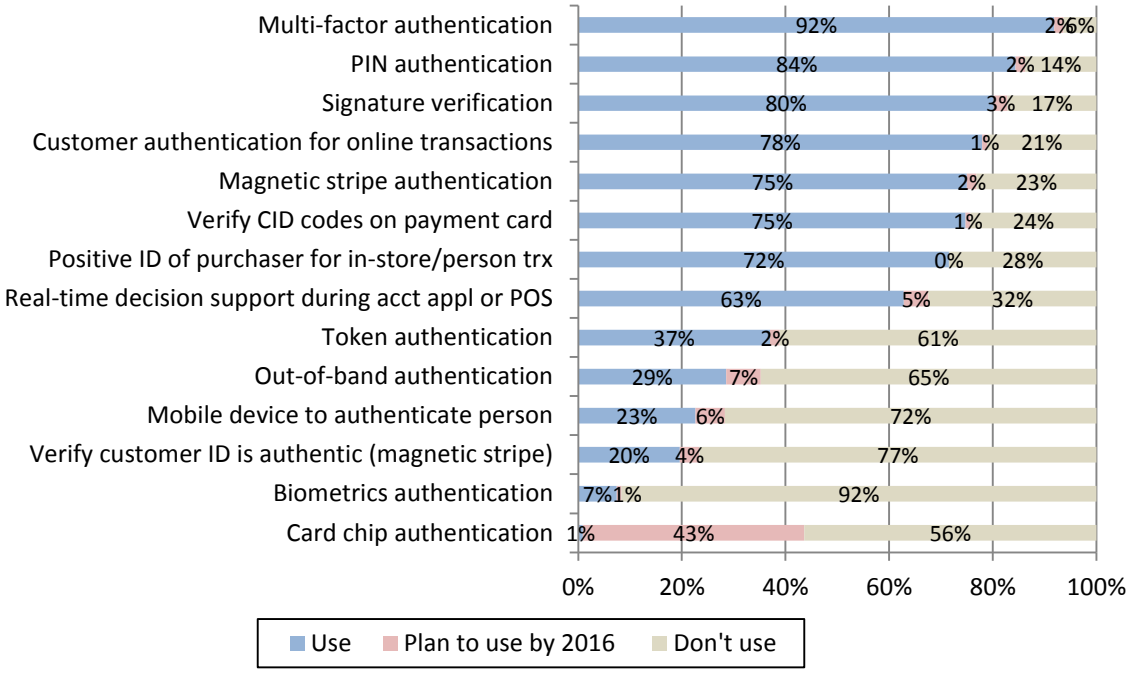
Customer Authentication Methods

This year, the survey included fourteen different authentication methods, compared to ten in the 2012 survey. The following methods were new to the survey this year: token authentication (USB or fob); out-of-band authentication; mobile device to authenticate person; and multi-factor authentication.[13] These additions reflect changes in the marketplace.

Financial institutions rely on many of the authentication methods listed, as shown in Figure 36. Seven authentication methods are used by more than 70% of financial services companies. Lower levels of usage are seen across alternative factors that could be used in multi-factor authentication, such as physical tokens (37%), out of band authentication (29%), using a mobile device to authenticate a customer (20%), and biometrics (7%). Card chip authentication is used by only 1% of financial institutions surveyed, but 43% expect to use chip authentication by 2016. This likely is related directly to the timelines set forth by major card networks' to migrate magnetic stripe cards in the U.S. towards a chip-enabled environment. Customer authentication methods are seen as highly effective by financial institutions. For every method listed except for two, 94% or more of the surveyed institutions rate them as very or somewhat effective (Figure 38). Notably, magnetic stripe authentication is seen as somewhat ineffective for the purpose of consumer authentication by 21% of financial institutions surveyed; 13% also find biometric authentication to be somewhat ineffective.

[13] *Token authentication* as used here refers to a physical token such as a USB token or "fob."
Out-of-band authentication includes any technique that allows the identity of the individual originating a transaction to be verified through a channel different from the one the customer is using to initiate the transaction (e.g., a phone call, an email, or a text message).
Mobile device to authenticate person is often used as one of the authentication factors in multi-factor authentication. Fingerprint readers or facial recognition software on a mobile device (biometrics), receiving SMS or email messages are examples of authentication methods on a mobile device.
Multi-factor authentication uses two or more factors for authentication: something only the user knows (the PIN), something only the user has (physical token, a card or mobile device) and/or something only the user is (a fingerprint). Authentication occurs only if each factor is validated by the other party.

Figure 36: Use of Customer Authentication Methods
(by % of Financial Services Respondents (N=105 to 111))

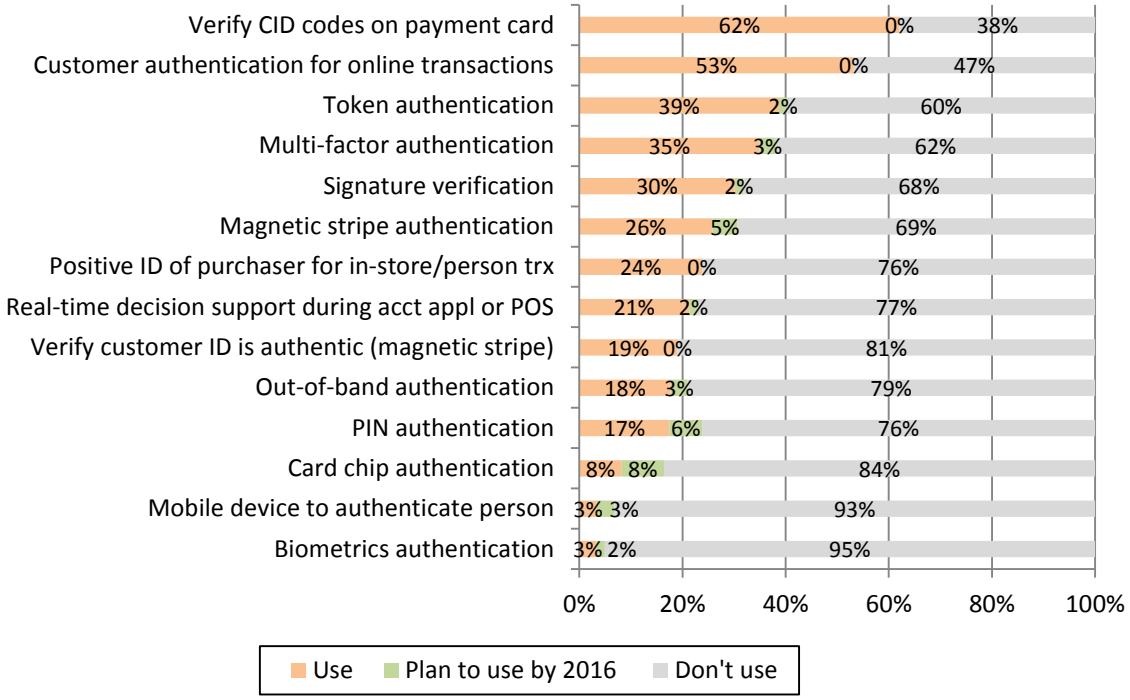


Q34: Which of the following authentication methods does your organization currently use or plan to use to mitigate payment risk?

Non-financial firms exhibit a different usage pattern than financial institutions in the category of customer authentication. There are only two authentication methods that are used by more than 50% of firms surveyed (verify CID codes[14] on payment card and customer authentication for online transactions). While 92% of financial institutions use multi-factor authentication, only 35% of non-financial firms use this method for customer verification purposes. Further, Figure 37 shows that most non-financial firms do not have plans to adopt customer authentication methods in the next few years that they are not already using. This is perhaps not surprising, as the vast majority of non-financial respondents do not focus on consumer payments. Business to business payments will naturally require different authentication tactics and consider the payments used for disbursement or accepted by the company. Non-financial firms appear to be mostly satisfied with the authentication methods they use, as shown in Figure 39. More than 90% of firms that use these methods find all but two of them to be very or somewhat effective. Signature verification stands out, as 22% of non-financial companies that use signature verification find it to be a somewhat ineffective authentication tool. Similarly, 15% of non-financial companies believe that real time decision support during account application or at the point of sale is a somewhat ineffective authentication method.

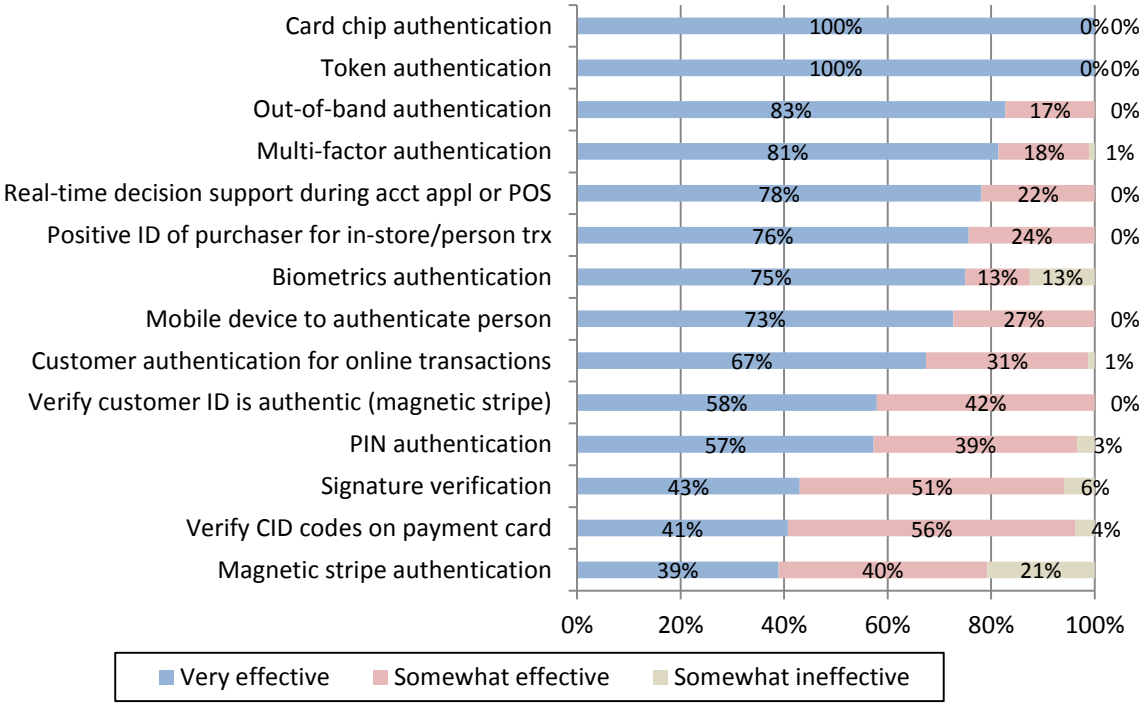
[14] CID (card identification number), CVV (card verification value), CVC (card verification code) are different terms for a 3- or 4-digit security code that is found on either the front or the back of a payment card. It is used to verify that the cardholder is in possession of the card during a card-not-present transaction.

Figure 37: Use of Customer Authentication Methods
(by % of Non-Financial Services Respondents (N=54 to 66))



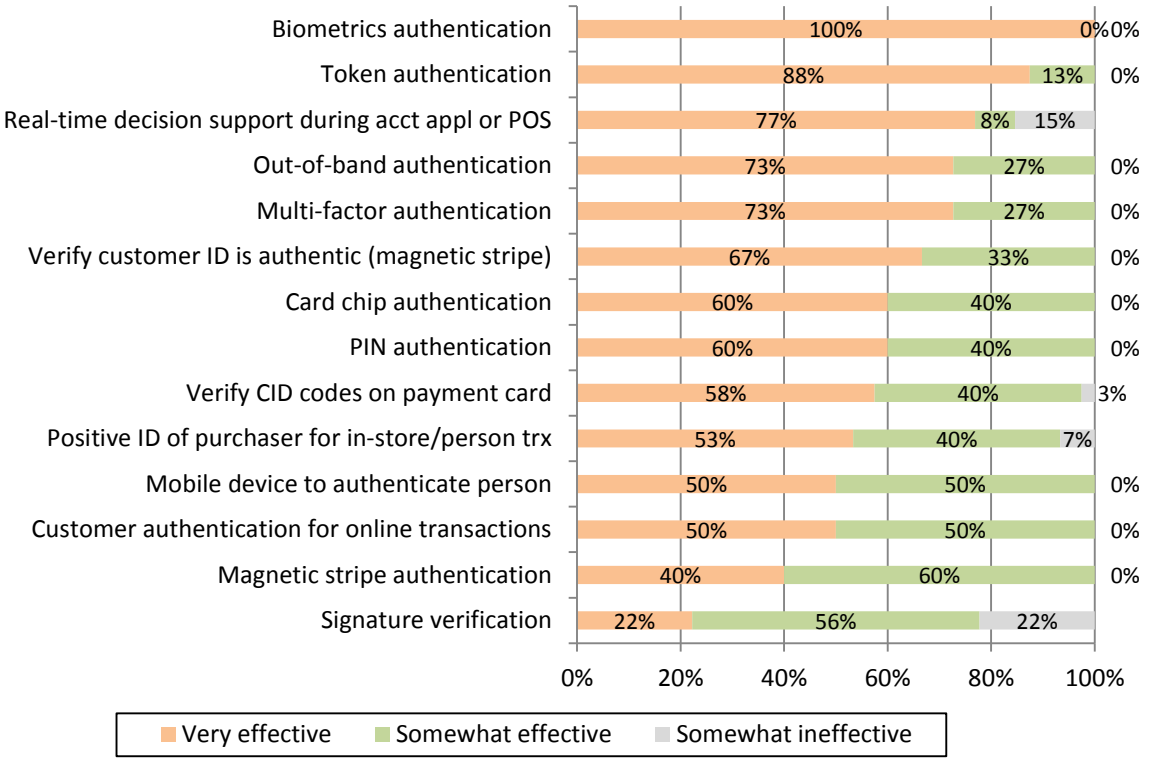
Q34: Which of the following authentication methods does your organization currently use or plan to use to mitigate payment risk?

Figure 38: Effectiveness of Customer Authentication Methods
(by % of Financial Services Respondents Using It (N=1 to 97))



Q35: Please rate the effectiveness of authentication methods currently used by your organization.

Figure 39: Effectiveness of Customer Authentication Methods
(by % of Non-Financial Services Respondents Using It (N=1 to 40))



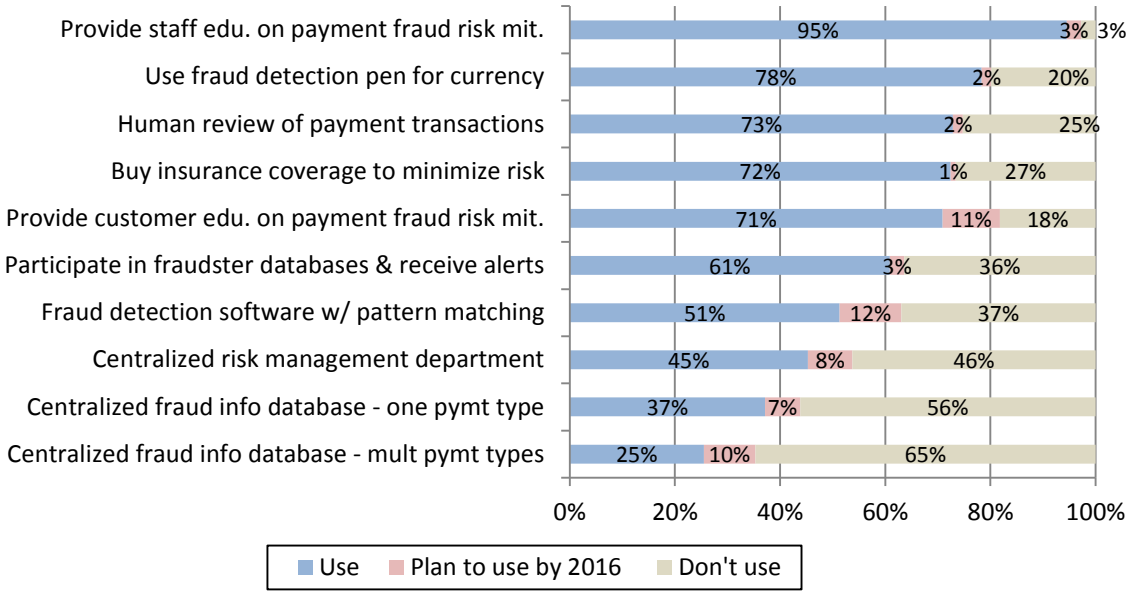
Q35: Please rate the effectiveness of authentication methods currently used by your organization.

Transaction Screening and Risk Management Methods

Also included in the survey were the transaction screening and management methods used by both financial institutions and non-financial firms. These results can be seen in Figures 40 and 41. Respondents were asked about ten different screening tools; in 2014, the survey included "buy insurance coverage to minimize risk" for the first time. Overall, the 2014 survey shows similar usage patterns for financial institutions compared to the 2012 survey year. The two methods most used by financial institutions remained the same: provide staff education on payment fraud risk mitigation and use fraud detection pen for currency.

Overall, financial institutions use a variety of screening and risk management tools. There are five categories of tools in use by more than 70% of surveyed institutions. Although most financial institutions do not appear to be planning to adopt screening tools that they do not currently use, there are a few areas where institutions expressed interest in incorporating new tools. Eleven percent of financial institutions plan to provide customer education on payment fraud risk by 2016, 12% plan to institute fraud detection software with pattern matching and 10% plan to use a centralized fraud information database for multiple payment types in that timeframe. Figure 42 shows that financial institutions believe that these screening and risk management tools are highly effective. There is only one category, "buy insurance coverage to minimize risk," that is not rated as effective by 90% or more of the firms that utilize it.

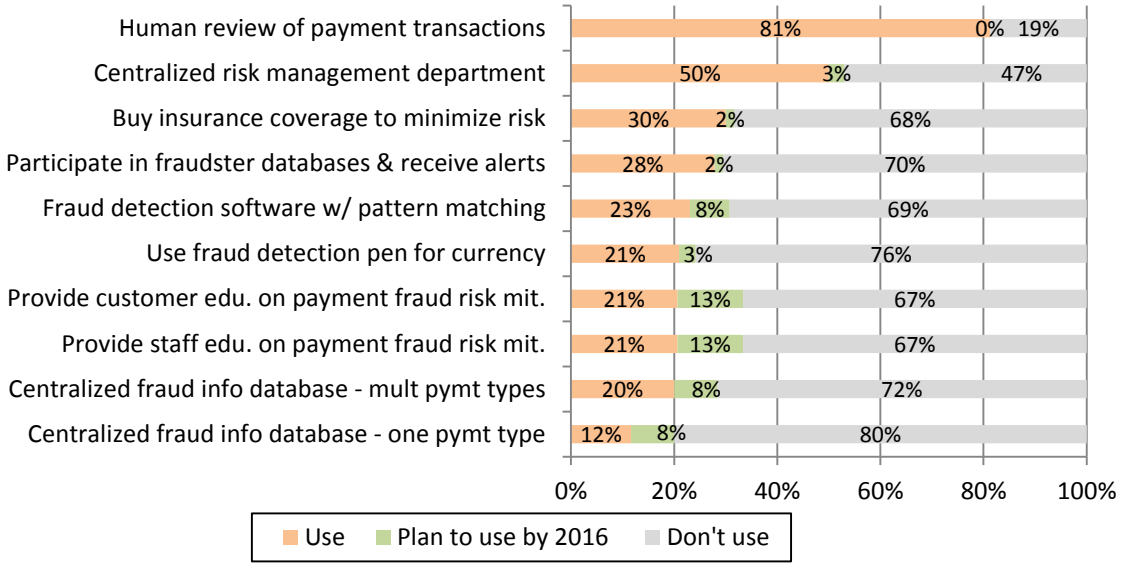
Figure 40: Use of Transaction Screening and Risk Management Methods (by % of Financial Services Respondents (N=102 to 111))



Q36: Which of the following transaction screening and risk management methods does your organization currently use or plan to use to mitigate payment risk?

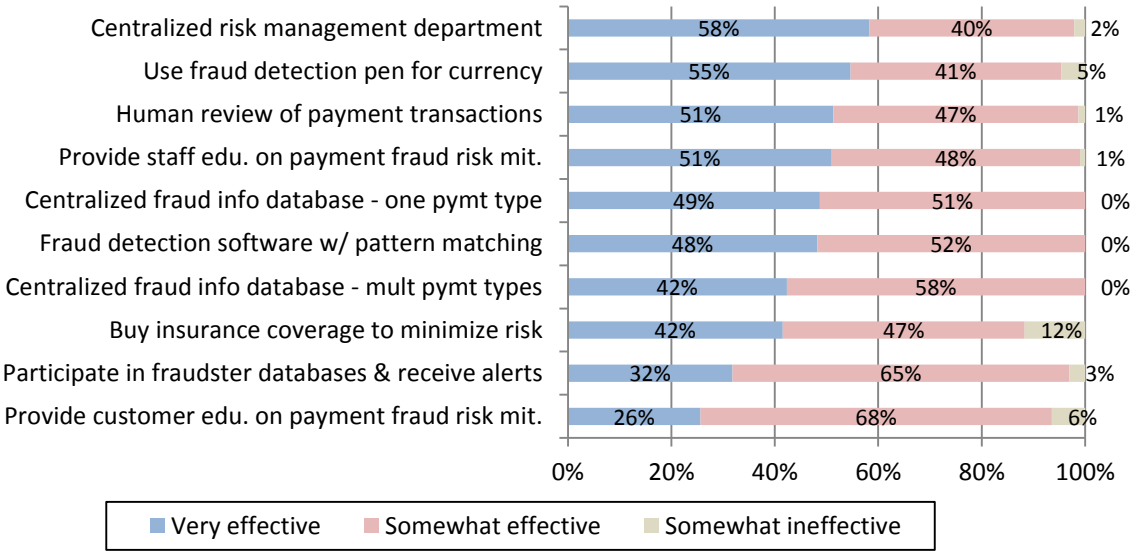
Non-financial firms are much less likely to use the screening and risk management tools listed. Only two tools are being used by at least half of firms surveyed: 81% of non-financial firms take advantage of human review of payment transactions and 50% have implemented a centralized risk management department (Figure 41). These same methods were also found to be most prevalent in the 2012 survey. All other tools are used by less than one third of firms. Most do not plan to adopt new screening and risk management tools, though education efforts (for both customers and staff) are being considered by 13% of non-financial firms by the year 2016. Non-financial firms also seem highly satisfied with the tools they are currently using. All firms that use a specific screening or risk management method found all but three tools listed to be very or somewhat effective (Figure 43). The exceptions are fraud detection pen for currency, insurance coverage, and human review of payment transactions, which are seen as somewhat ineffective by 8%, 6%, and 4% of firms respectively.

Figure 41: Use of Transaction Screening and Risk Management Methods
(by % of Non-Financial Services Respondents (N=1 to 66))



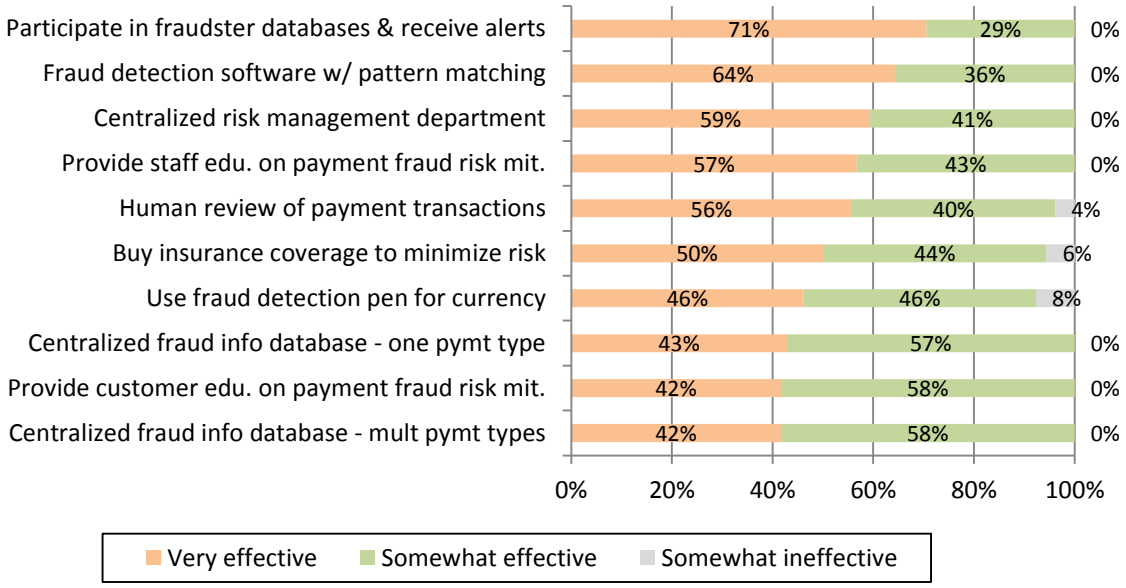
Q36: Which of the following transaction screening and risk management methods does your organization currently use or plan to use to mitigate payment risk?

Figure 42: Effectiveness of Transaction Screening and Risk Management Methods
(by % of Financial Services Respondents Using It (N=26 to 102))



Q37: Please rate the effectiveness of the transaction screening and risk management methods currently used by your organization.

Figure 43: Effectiveness of Transaction Screening and Risk Management Methods
(by % of Non-Financial Services Respondents Using It (N=7 to 52))

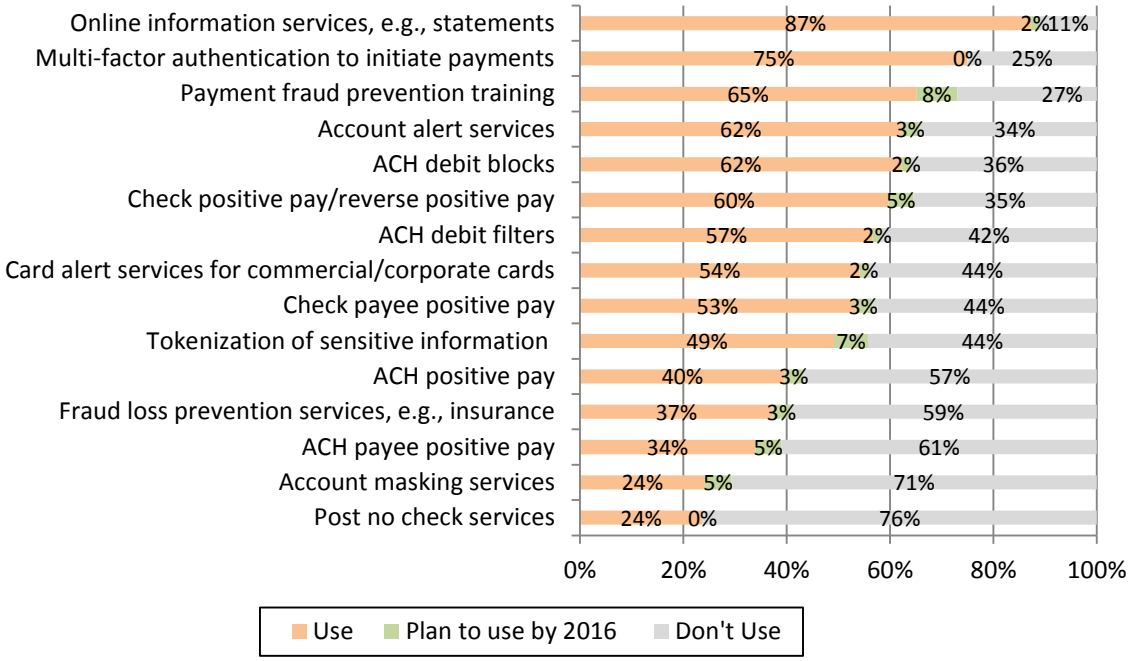


Q37: Please rate the effectiveness of the transaction screening and risk management methods currently used by your organization.

Risk Mitigation Services Offered by Financial Service Organizations

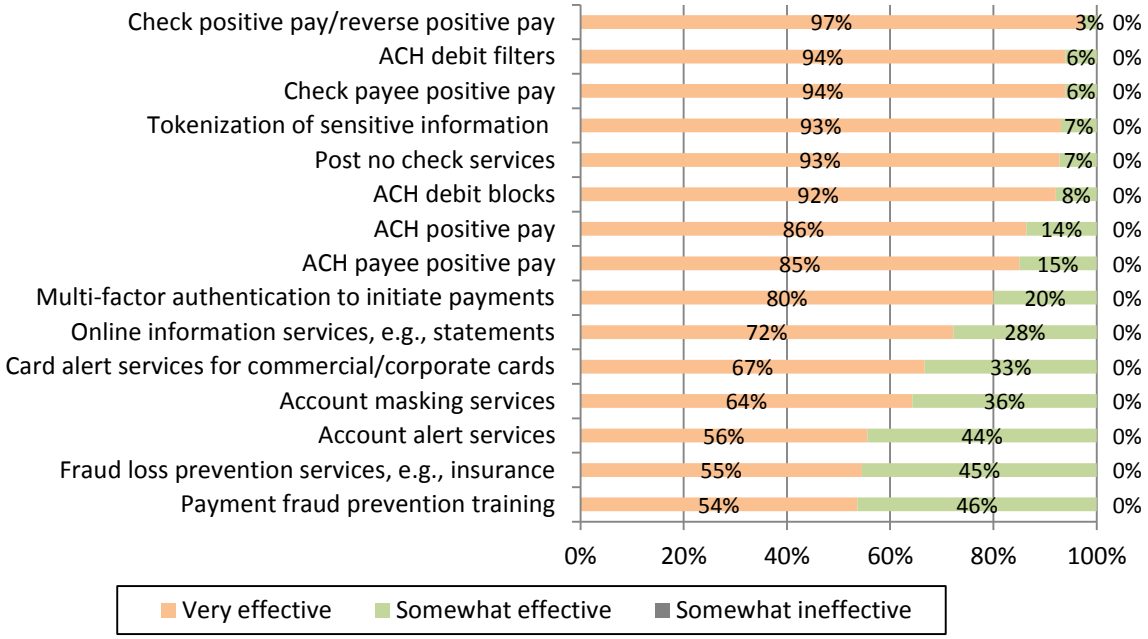
Non-financial firms were asked to elaborate on the risk mitigation services offered by financial institutions and service providers. Figure 44 provides these results. The top five services being used are: online information services; multi-factor authentication to initiate payments; payment fraud prevention training; account alert services, and ACH debit blocks. Overall results compared with the 2012 survey show that usage is down in most categories. However, many more non-financial firms responded to the survey in 2014 than in 2012. Companies remain overwhelmingly satisfied with the risk mitigation services offered to them by financial services firms and service providers. None of the respondents rate any of the services used as somewhat ineffective (Figure 45).

Figure 44: Use of Risk Mitigation Services Offered by Financial Institutions and Service Providers (by % of Non-Financial Services Respondents (N=58 to 63))



Q40: What risk mitigation services offered by your financial institution/service provider does your organization currently use or plan to use?

Figure 45: Effectiveness of Risk Mitigation Services Offered by Financial Institutions and Service Providers (by % of Non-Financial Services Respondents Using It (N=14 to 54))



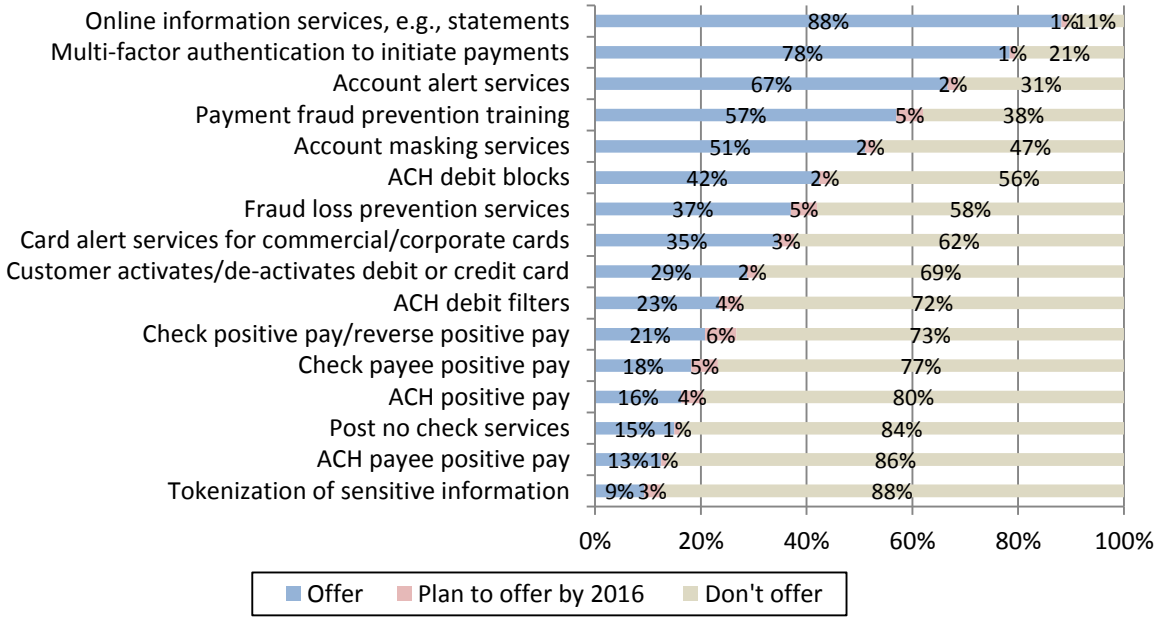
Q41: Please rate the effectiveness of risk mitigation services currently used by your organization.

The 2014 survey breaks out services that financial institutions and service providers offer to business customers and those they offer to consumers. The results are found in Figures 46 and 48. Notably, results show similar levels of offerings for those categories that apply to both consumer and business transactions. Figure 48 lists ten types of risk mitigation services offered to consumers. Nine of those services are similar for business customer transactions; however, one stands apart. Card alert services for debit or credit cards are offered for consumer transactions by 63% of respondents; such alerts are only offered by 35% for business transactions. This difference in card alert service offerings may be a reflection of payment products offered and customers served as shown earlier in Table 8 and Figure 4.

Financial service providers are highly confident in the services offered for both consumer and business transactions, as seen in Figures 47 and 49.

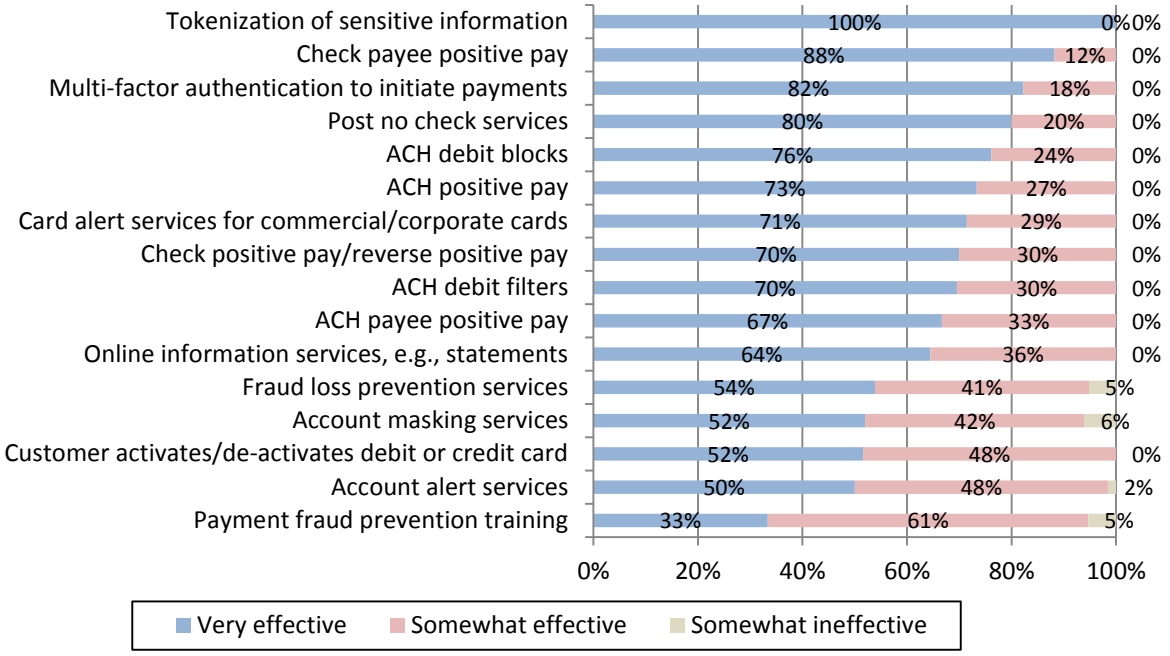
Notably, at least half of the businesses surveyed use the six risk services that are also rated as "very effective" by 90% of the companies using them (Figures 44 and 45). However, less than 25 percent of the financial service respondents offer the services that received the highest effectiveness rating by businesses. These services focus on fraud related to check (check positive pay and payee positive pay services, post no check), ACH filters, and tokenization of sensitive payments information which can be used to protect card account numbers as well as other data (Figure 46). Only a small share of financial institutions plan to offer these services by 2016.

Figure 46: Risk Mitigation Services Offered to Business Customers by Financial Institutions and Service Providers (by % of Financial Services Respondents (N = 96 to 102))



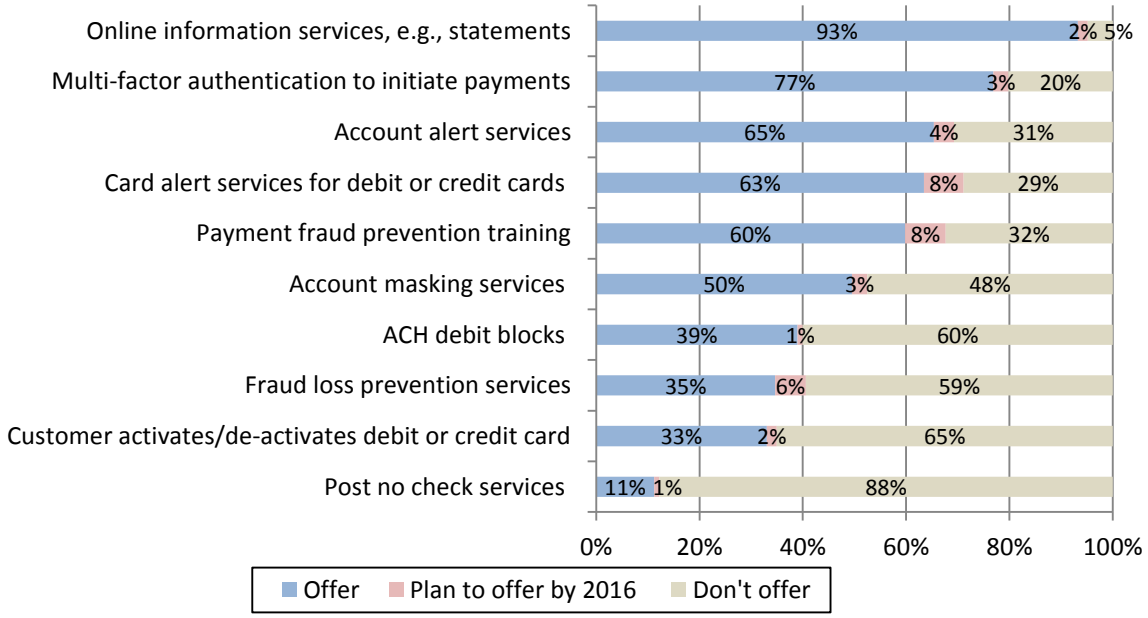
Q42: What risk mitigation services/products does your organization currently offer or plan to offer to your business customers?

Figure 47: Effectiveness of Risk Mitigation Services Offered to Business Customers Rated by Financial Institutions and Service Providers
(by % of Financial Services Respondents Offering It (N = 9 to 90))



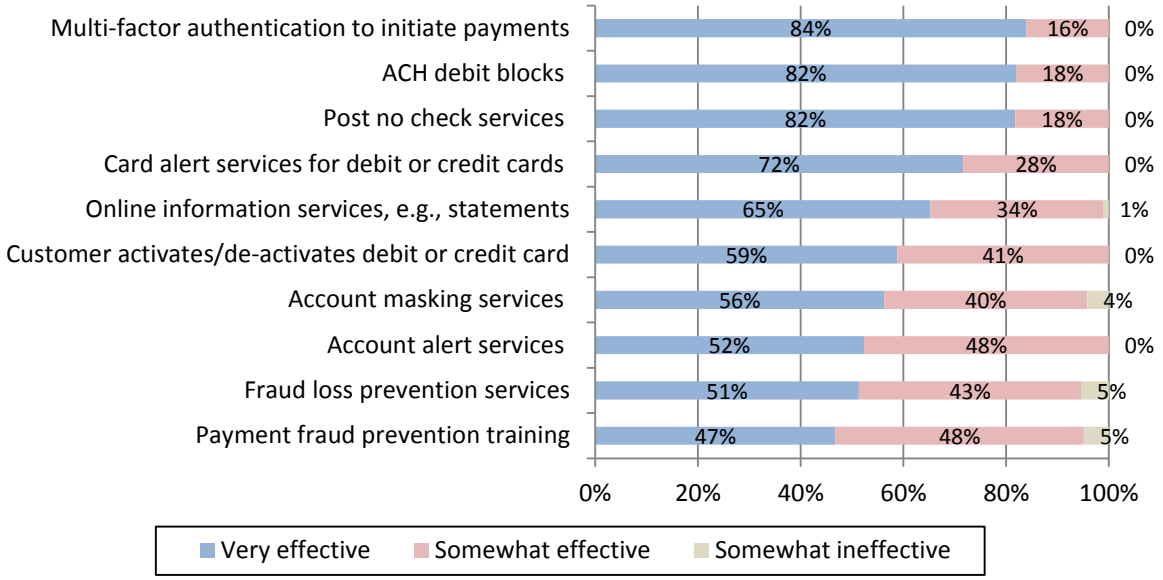
Q43: Please rate the effectiveness of risk mitigation services currently offered by your organization to your business customers.

Figure 48: Risk Mitigation Services Offered to Consumer Customers by Financial Institutions and Service Providers
(by % of Financial Services Respondents (N = 98 to 104))



Q44: What risk mitigation services/products does your organization currently offer or plan to offer to your consumer customers?

Figure 49: Effectiveness of Risk Mitigation Services Offered to Consumer Customers Rated by Financial Institutions and Service Providers
(by % of Financial Services Respondents Offering it (N = 11 to 98))



Q45: Please rate the effectiveness of risk mitigation services currently offered by your organization to your consumer customers.

Barriers to Reduce Payments Fraud

In order to get a handle on payments fraud, it is important to understand current risks and to evaluate whether current risk mitigation efforts are effective. However, it is also crucial to recognize that fighting payments fraud is an uphill battle. Criminals exhibit increasingly sophisticated ways of perpetrating payments fraud, and as consumer and business payments preferences evolve, firms must ensure that new forms of payment are secure and reliable. While large, established banks and merchants are likely to have extensive resources in place to devote to reducing payments fraud, smaller organizations might find this more challenging.

Table 14 displays information about barriers that firms experience when attempting to mitigate payments fraud. Interestingly, more financial and non-financial firms list "lack of staff resources" than any other barrier. In 2014, 59% of financial institutions and 63% of non-financial firms cite this as a barrier. More than a third of financial institutions also list consumer data privacy issues (38%) and lack of a compelling business case to adopt new or change existing methods (34%). Surprisingly, the 2014 survey shows a sharp decline in the percentage of financial institutions that cite cost as a barrier to payments fraud mitigation. In 2012, 38% of financial institutions attributed the cost of implementing commercially available fraud detection tools and services as a barrier, compared to only 15% in 2014. Similarly, almost half, or 49%, of financial institutions cited the cost of implementing in-house fraud detection tools and services as a barrier in 2012, compared to just 14% this year. The most common barriers identified by non-financial companies in 2014 are lack of staff resources (63%), lack of a compelling business case (50%), and corporate reluctance to share information due to competitive issues (35%). While there are slight differences in responses between 2012 and 2014, there were so few non-financial firms responding in 2012 (n=12) that it is challenging to draw conclusions from the data.

Table 14: Main Barriers to Payments Fraud Mitigation
(by % of Respondents)

Barrier	2014			2012		
	FS (N=92)	Non-FS (N=52)	All Org. (N=144)	FS (N=164)	Non-FS (N=12)	All Org. (N=176)
Lack of staff resources	59%	63%	60%	55%	75%	69%
Lack of compelling business case (cost vs. benefit) to adopt new or change existing methods	34%	50%	40%	38%	75%	49%
Consumer data privacy issues/concerns	38%	21%	32%	33%	33%	40%
Corporate reluctance to share information due to competitive issues	17%	35%	24%	11%	25%	15%
Cost of implementing commercially available fraud detection tool/service	15%	10%	13%	38%	17%	45%
Cost of implementing in-house fraud detection tool/service	14%	12%	13%	49%	8%	57%
Unable to combine payment information for review due to operating w/ multiple business areas, states or banks	10%	10%	10%	12%	17%	15%
Other	8%	6%	7%	5%	0%	6%

Q48: What are the main barriers to mitigate payments fraud that your organization experiences?

Opportunities to Reduce Payments Fraud

This section of the report looks at opportunities to reduce payments fraud for both financial and non-financial service organizations in three areas: new or improved methods most needed, authentication methods, and legal and regulatory changes.

New or Improved Methods Most Needed

Table 15 shows which new or improved fraud mitigation methods are deemed most needed by respondents. The top three methods cited by the highest percentage of financial institutions remain constant between 2012 and 2014. These methods are replacement of card magnetic stripe with EMV or smart chip technology; controls over Internet payments; and consumer education of fraud prevention. Responses vary for non-financial firms since 2012; however, remarks in this report focus on the 2014 survey due to the small number of such firms that responded in 2012. In 2014, the top three methods seen as most needed by non-financial firms are replacement of card magnetic stripe with EMV chip technology (55%), controls over Internet payments (47%) and tokenization of sensitive information (47%). A much smaller percentage of financial institutions cite tokenization as a most needed method for fraud mitigation (23%). This may be due to the fact that a major benefit of tokenization for merchants is personal and account information normally stored at the merchant location is removed through the tokenization process so that this information is never stored by the merchant.

Table 15: New or Improved Methods Needed
(by % of Respondents)

New or Improved Methods Needed	2014			2012		
	FS (N=106)	Non-FS (N=58)	All Org. (N=164)	FS (N=173)	Non-FS (N=14)	All Org. (N=187)
Replacement of card magnetic stripe with EMV chip technology	69%	55%	64%	58%	29%	46%
Controls over Internet payments	65%	47%	59%	66%	57%	65%
More aggressive law enforcement	40%	40%	40%	47%	36%	46%
Consumer education of fraud prevention	45%	28%	39%	61%	71%	62%
Controls over mobile payments	42%	22%	35%	40%	36%	40%
Information sharing on emerging fraud tactics being conducted by criminal rings	28%	43%	34%	40%	79%	43%
Tokenization of sensitive information[15]	23%	47%	31%	na	na	na
Industry specific education on best prevention practices for fraud	28%	34%	30%	36%	21%	35%
Industry alert services	22%	33%	26%	23%	29%	24%
Image survivable check security features for business checks	8%	14%	10%	10%	14%	11%
Other	4%	3%	4%	5%	7%	5%

Q46: From your organization's perspective, what new or improved methods are most needed to reduce payments fraud?

[15] Tokenization is defined as the process of randomly generating a substitute value to replace sensitive information. When used in financial transactions, tokens can replace payment credentials—such as a bank account or credit/debit card numbers. Removing these sensitive credentials from the transaction flow improves the security of the payment. (See "Mobile Payments Industry Workgroup Meeting: Discussion on Tokenization Landscape in the U.S.," Federal Reserve Banks of Boston and Atlanta, June 2-3, 2014.)

Authentication Methods

Table 16 details respondents' preferences for adoption of authentication methods. As reported already, most of the survey's non-financial respondents do not focus on consumer-facing payments but rather on business to business payments, while the financial institutions provide payments to both constituents. A high percentage of financial institutions choose chip and PIN requirements[16] (79%) and chip for dynamic authentication (62%), while only 46% and 40% of non-financial firms respectively cite those options as the preferred authentication methods.

Table 16: Preferences for Adoption of Authentication Methods
(by % of Respondents)

Method	2014			2012		
	FS (N=103)	Non-FS (N=48)	All Org. (N=151)	FS (N=161)	Non-FS (N=12)	All Org. (N=173)
Chip and PIN requirement	79%	46%	68%	55%	25%	53%
Chip for dynamic authentication	62%	40%	55%	34%	25%	34%
Multi-factor authentication	43%	29%	38%	49%	42%	49%
PIN requirement	24%	29%	26%	43%	42%	43%
Token	23%	44%	30%	29%	67%	31%
Mobile device to authenticate person	28%	29%	28%	22%	25%	22%
Out-of-band/channel authentication to authorize payment	21%	10%	18%	29%	17%	28%
Biometrics	17%	10%	15%	23%	17%	23%
Other	1%	2%	1%	4%	0%	3%

Q46: What authentication methods would your organization prefer or consider adopting to help reduce payments fraud?

[16] "Chip" as used in the two choices is not specific to cards, but is expanded to include an EMV smart chip in a card and/or mobile device. 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 that calculates a cryptogram for each transaction that is unique to the specific card/device and transaction. Dynamic data authentication protects against card skimming, counterfeiting and replay fraud, since dynamic data can be used for purchases only once.

"Chip and PIN" authentication is more secure because it requires two factors for authentication—what you have, the chip (in a card or a mobile device) and what you know, the PIN. In this case, if the card is lost or stolen, it will be useless if used in a transaction when a PIN is required.

Legal or Regulatory Changes

Finally, the survey asked respondents to consider how the public sector might help the industry combat payments fraud and whether or not a variety of legal and regulatory considerations would be most useful in this regard. The results are in Table 17. In general, financial institutions are more supportive of a variety of legal and regulatory changes than are non-financial companies. More than half of financial institutions cite the following specific considerations as useful:

- Place responsibility to mitigate fraud and shift liability for fraudulent card payments to the entity that initially accepts the card payment.
- Place more responsibility on consumers and customers to reconcile and protect their payment data.
- Assign liability for fraud losses to the party most responsible for not acting to reduce the risk of payment fraud.
- Strengthen disincentives to committing fraud through stiffer penalties and more likely prosecution.

Three of the above strategies focus on shifting or reassigning liability and/or responsibility for payments fraud. Private rules and contracts can and do assign liability for a variety of transaction types and situations. However, there is a sense among industry participants that incentives are not always correctly aligned so as to most efficiently and effectively reduce payment fraud.[17] While almost two-thirds of non-financial firms (65%) agree that strengthening disincentives to committing fraud through stiffer penalties and more likely prosecution is a favorable solution, only one other category is cited by more than half of such firms: 56% support the improvement of law enforcement cooperation on domestic and international payments fraud and fraud rings. Non-financial firms do not appear to be very supportive of liability shifts or reassigning responsibility for payments fraud, perhaps in part because they fear that such changes would move more of the burden of paying for such fraud to businesses.

[17] See Federal Reserve Bank of Chicago 3Q/2013, Economic Perspectives, "Clarifying liability for twenty-first-century payment fraud" by Sandeep Dhameja, Katy Jacob, and Richard D. Porter

Table 17: Legal and Regulatory Considerations
(by % of Respondents)

Legal and Regulatory Changes	FS (N=105)	Non-FS (N=54)	Total (N=159)
Strengthen disincentives to committing fraud through stiffer penalties and more likely prosecution	55%	65%	58%
Place responsibility to mitigate fraud and shift liability for fraudulent card payments to the entity that initially accepts the card payment	70%	31%	57%
Place more responsibility on consumers and customers to reconcile and protect their payment data	70%	19%	52%
Assign liability for fraud losses to the party most responsible for not acting to reduce the risk of payment fraud	59%	26%	48%
Improve law enforcement cooperation on domestic and international payments fraud and fraud rings	40%	56%	45%
Focus future legal or regulatory changes on data breaches to where breaches occur	41%	26%	36%
Assign responsibility for mitigating fraud risk to the party best positioned to take action against fraud	42%	22%	35%
Establish new laws/regulations or change existing ones in order to strengthen the management of payments fraud risk	26%	33%	28%
Align Regulation E and Regulation CC to reflect changes in check collection systems' use of check images and conversion of checks to ACH	32%	17%	27%
Establish new laws/regulations to require data sharing to strengthen the management of payments fraud risk	17%	30%	21%

Q49: Please indicate what types of legal or regulatory changes you think would help reduce payments fraud.

Conclusions

- In survey year 2014, payments fraud remains a significant concern for financial institutions and other corporations in the ninth district and surrounding region. While financial institutions are significantly more likely to report payment fraud attempts (75%) and losses (70%) than non-financial companies, the proportion of financial institutions reporting fraud attempts and losses has actually decreased since survey year 2012.
- Financial institutions and corporations have different experiences with loss rates, though overall losses remain quite low for both groups measured as a percentage of revenues. In 2014, more than half of financial institutions that experienced payment fraud losses report increases in those losses, while three quarters of non-financial firms respond that loss rates remain about the same over the prior year.
- In keeping with previous surveys, signature debit transactions are the payment type cited by the largest percent of financial institutions as accounting for high levels of payments fraud attempts and losses, while checks and credit cards are cited by the largest percent of non-financial companies.
- High percentages of surveyed financial institutions report that fraud prevention costs exceed actual losses for many types of payments, especially wire, cash, and ACH payments. This trend is even more striking for non-financial 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.
- 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 46% of financial institutions and 31% of non-financial firms, higher than any other information source.
- Non-financial firms exhibit a very different usage pattern than financial institutions in the category of customer authentication. There are only two authentication methods (verify CID codes on payment card and customer authentication for online transactions) that are used by more than 50% of firms surveyed. While 92% of financial institutions use multi-factor authentication, only 35% of non-financial firms use multi-factor authentication for customer verification purposes.
- When asked about their authentication preferences, 79% of financial services respondents prefer chip and PIN requirements and 62% prefer chip for dynamic authentication; non-financial firms preferred these authentication methods at 46% and 42% respectively.
- Lack of staff resources is cited by respondents as the main barrier to reducing payments fraud. The 2014 survey shows a sharp decline in the percentage of financial institutions that cite cost of implementing in-house or commercially available fraud detection tools and services as a barrier to payments fraud mitigation. In 2012, 38% of financial institutions cited the cost of implementing commercially available fraud detection tools and services as a barrier, compared to only 15% in 2014. Similarly, almost half, or 49%, of financial institutions cited the cost of implementing in-house fraud detection tools and services as a barrier in 2012, compared to just 14% this year.

- The most needed fraud mitigation methods cited by the highest percentage of financial institutions remained constant between 2012 and 2014. These methods are replacement of card magnetic stripe with EMV chip technology (69%); controls over Internet payments (65%); and consumer education of fraud prevention (45%). The top three methods seen as most needed by non-financial firms are replacement of card magnetic stripe with EMV chip technology (55%), controls over Internet payments (47%) and tokenization of sensitive information (47%). A much smaller percentage of financial institutions cited tokenization as a needed method for fraud mitigation (23%).