

2014 Payments Fraud Survey Summary of Results

Federal Reserve Bank of Dallas
FIRM–Financial Institution Relationship Management
November 5, 2014

Contents

Introduction 2

Respondent Profile 3

Summary of Survey Results by Questions 5

 Payment Types Used by NonFinancial Institution Respondents 5

 Payment Products Offered by Financial Institution Respondents 6

 Payment Fraud Attempts and Financial Losses 8

 Perpetrators Involved in Successful Payments Fraud 17

 Most Common Fraud Schemes 17

 Payments Fraud Mitigation Strategies 21

 Customer Authentication Methods 22

 Transaction Screening and Risk Management Methods 25

 Internal Controls and Procedures 28

 Risk Mitigation Services Offered by Financial Services Organizations 30

Barriers to Reducing Payments Fraud 33

Opportunities to Reduce Payments Fraud 34

 New or Improved Methods Most Needed 34

 Authentication Methods 35

 Legal or Regulatory Changes 36

Conclusions 38

Introduction

During the second quarter of 2014, the Federal Reserve Bank of Dallas' FIRM—Financial Institution Relationship Management—conducted a survey on payments-related fraud experienced by financial institutions and corporations within the Dallas Fed District.¹ This was part of a broader initiative conducted in conjunction with the Federal Reserve Banks of Minneapolis, Chicago, Boston and Richmond and was the second time the Dallas Fed has participated in this survey.

The survey respondents answered questions about their experiences in 2013 with fraud trends and fraud mitigation strategies used for payment types such as cash, check, debit and credit cards, automated clearinghouse (ACH) and wire transfers. A variety of mobile and online payments questions were also included in the survey.

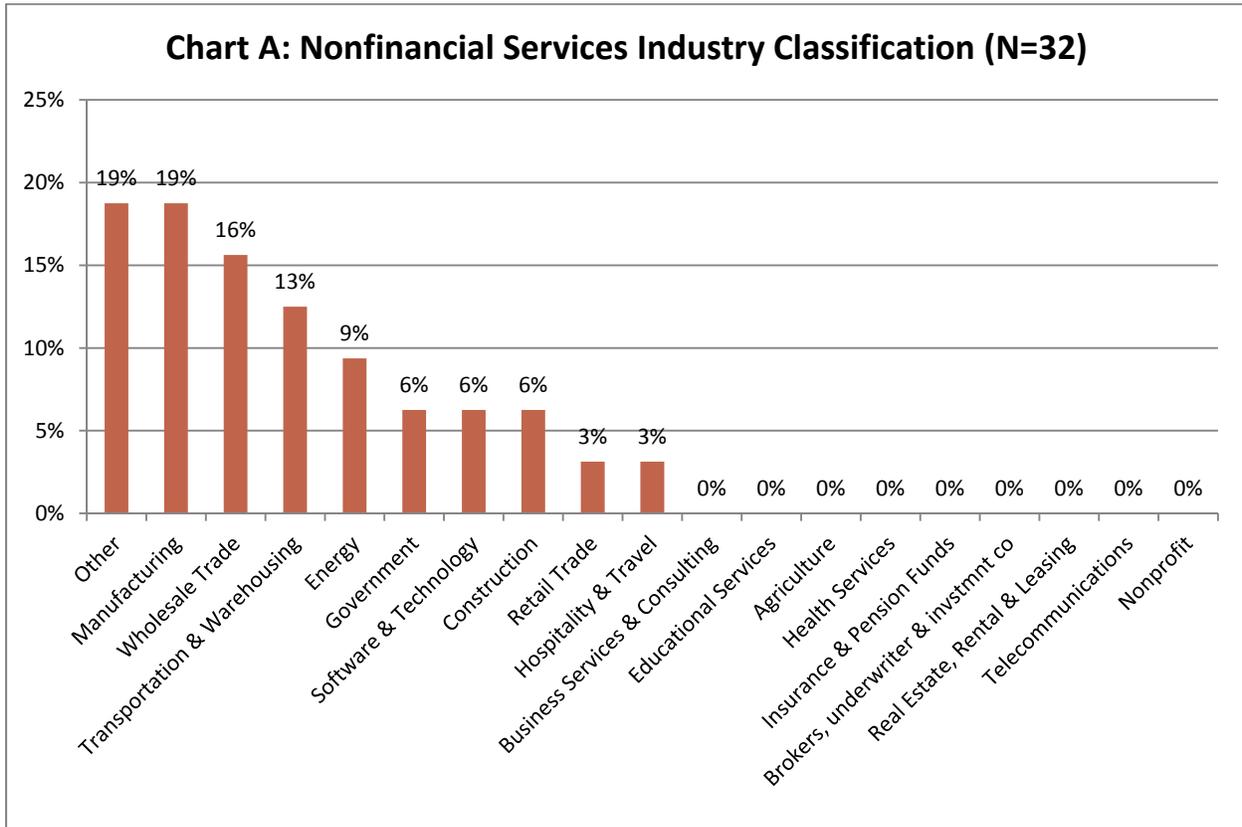
The survey audience was expanded with the help of the following organizations that sent the survey directly to their members: SWACHA—The Electronic Payments Resource®, the Austin, Dallas, Fort Worth and San Antonio chapters of the Association for Financial Professionals, the Houston Treasury Management Association, the Dallas, Central Texas and Houston chapters of the Association of Certified Anti Money-Laundering Specialists, the Fort Worth and Rio Grande Valley chapters of the Association of Certified Fraud Examiners, Central Texas, Rio Grande Valley and San Antonio chapters of the Risk Management Association, and the Dallas Area Compliance Association. We thank these organizations for their help in obtaining responses.² In addition, we thank members of the Federal Reserve Bank of Dallas Corporate Payments Council who also participated in the survey.

¹ Questions about the survey should be directed to Donna Raedeke, Payments Outreach Analyst, Federal Reserve Bank of Dallas, at donna.raedeke@dal.frb.org or 214-922-6042.

² In addition, the following national organizations helped to expand our survey audience by reaching out to their regional groups: 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 and the Small Business Administration.

Respondent Profile

There were a total of 149 respondents to the survey based in the Dallas Federal Reserve District; 117 were from the financial services industries and 32 were from nonfinancial services industries, corporations and merchants. Financial services industry respondents consisted of 80 banks, 33 credit unions, one thrift and three service providers.³ The nonfinancial services respondents classified their organizations in one of 19 industry categories, as shown in Chart A.



³ For the purposes of this survey, the term “financial institutions” includes banks, credit unions and thrifts. The term “service providers” includes payments processors. For some of the questions in the survey, service providers were included with banks, credit unions and thrifts, and the group is called “financial services industry.”

Respondents were also categorized by annual revenues, as shown in Chart B. Fifty-eight percent of the respondents, or 87 by number, were small businesses, with annual revenues under \$50 million.

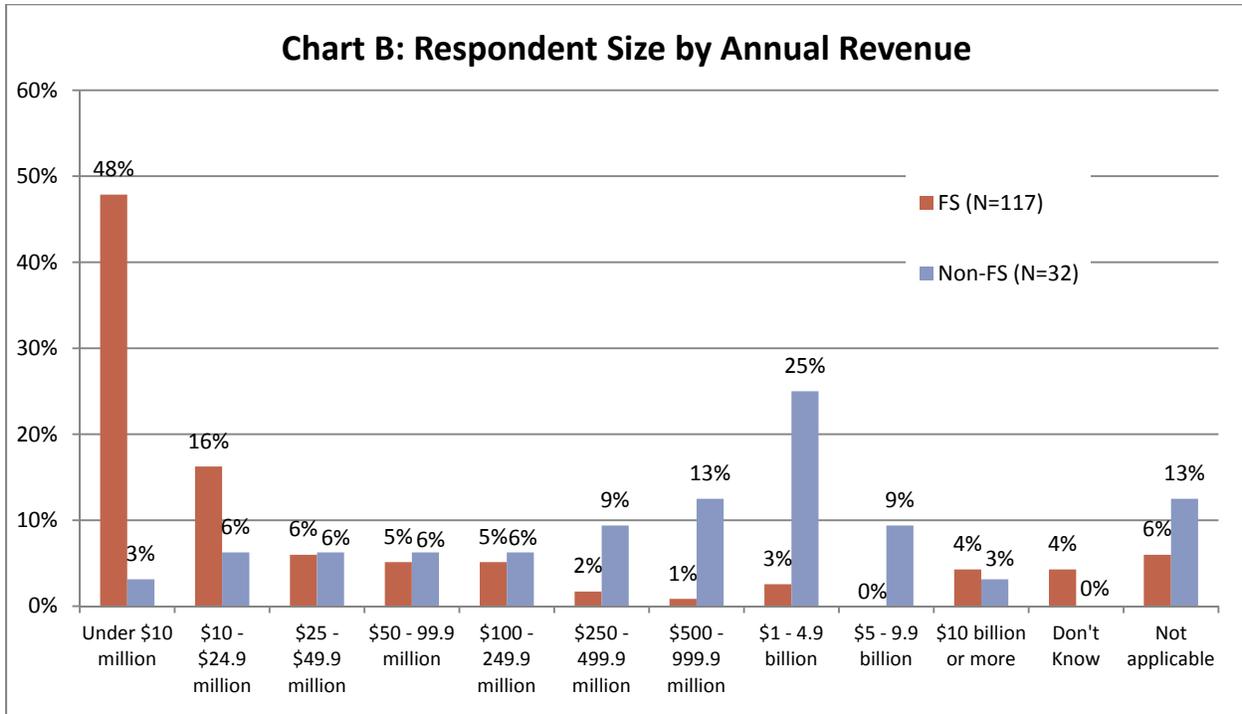
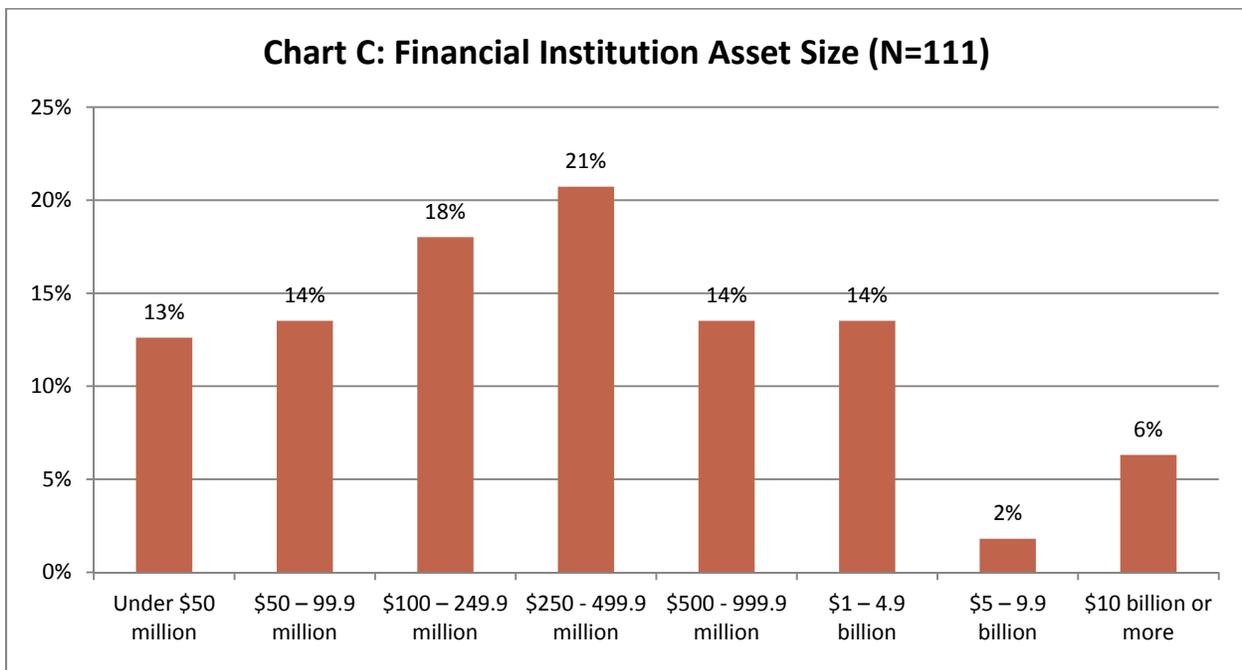


Chart C shows the number of financial institution respondents in each asset classification. About 80 percent of the financial institutions in the survey have assets of less than \$1 billion.



When asked if their organization was a member of a trade association that provides education on payments and/or payments risks, more than half of the financial services industry respondents reported belonging to a regional payments association like SWACHA. In fact, many are members of multiple trade associations that provide education on payments, such as the American Bankers Association (ABA), Independent Community Bankers of America (ICBA), Credit Union National Association (CUNA) and state banking associations. Only 3 percent of financial services industry respondents do not belong to any group that provides payments education. Thirty-two percent of nonfinancial services industry respondents do not hold membership in any such group.

Summary of Survey Results by Questions

In this section we analyze results of the survey questions. Where relevant we will compare this year’s survey’s results to those of the 2012 survey.

Payment Types Used by Nonfinancial Institution Respondents

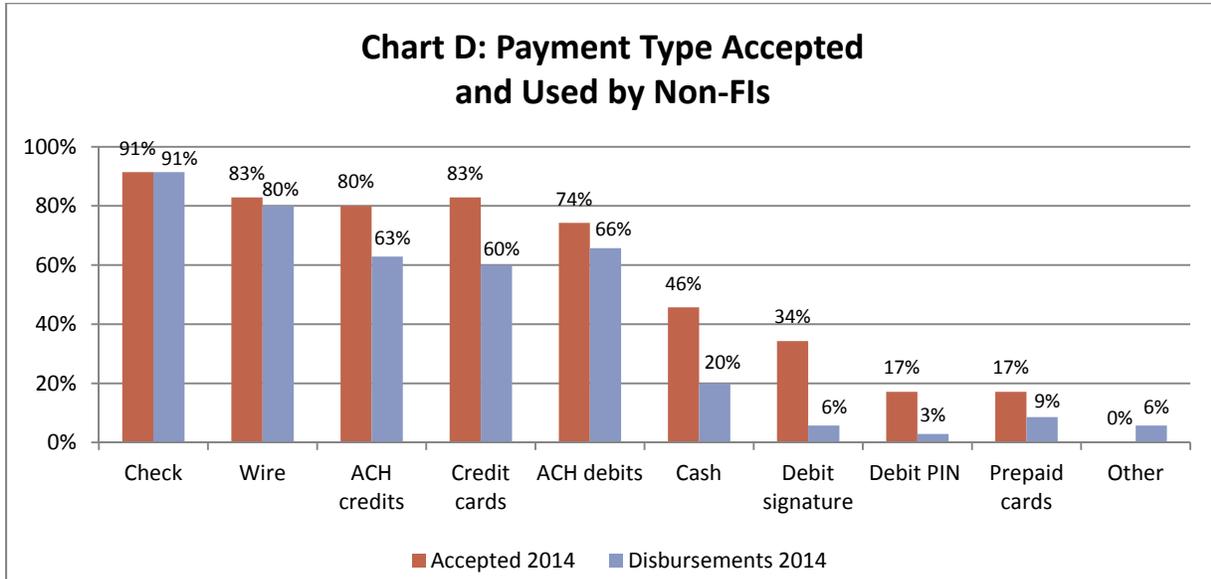
Table 1 below shows that nonfinancial institution respondents⁴ are fairly evenly split between primarily making and receiving payments to/from other businesses or to/from both consumers and businesses. None of the respondents in this group are involved in payments primarily with consumers. This data is similar to the 2012 survey.

Table 1

Non-FIs’ Payment Volume Counterparties (N=35)	2014 (N)	2014 (%)
Primarily payments to/from other businesses	18	51%
Payments to/from both consumers and businesses	17	49%
Primarily payments to/from consumers	0	0%

⁴ The term “nonfinancial institution respondents” as used here includes service providers.

Chart D shows the payment types both accepted and used for disbursement by nonfinancial institution respondents. Similar to the 2012 survey, checks, wires, ACH payments and credit cards are the primary payment types accepted and used for disbursement by nonfinancial institution respondents.



Payment Products Offered by Financial Institution Respondents

Financial institutions were asked to indicate the type of customer base to which they offer payment products. Chart E shows that two-thirds of the financial institution respondents serve both consumers and business or commercial clients, and over one-fourth serve primarily consumers.

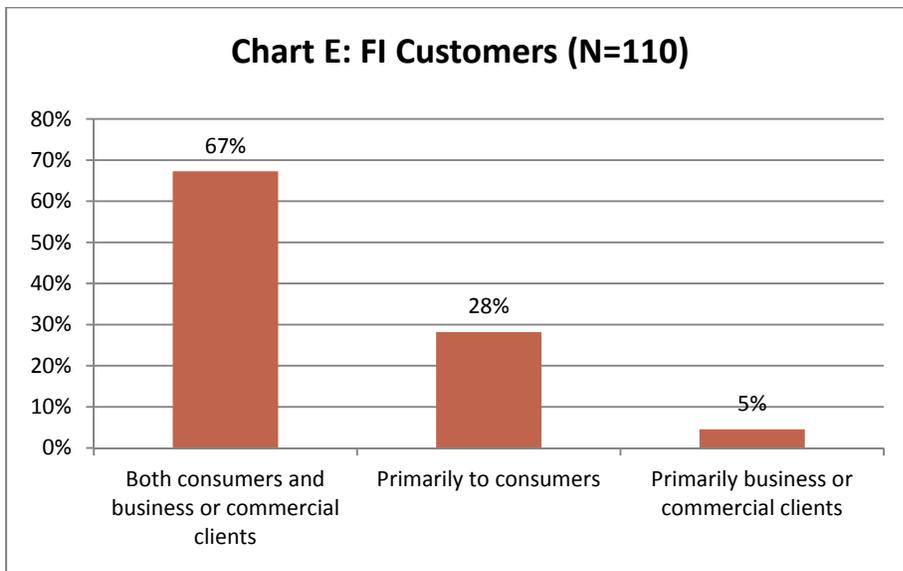


Chart F demonstrates the difference in the customer types served by banks, credit unions and thrifts.⁵

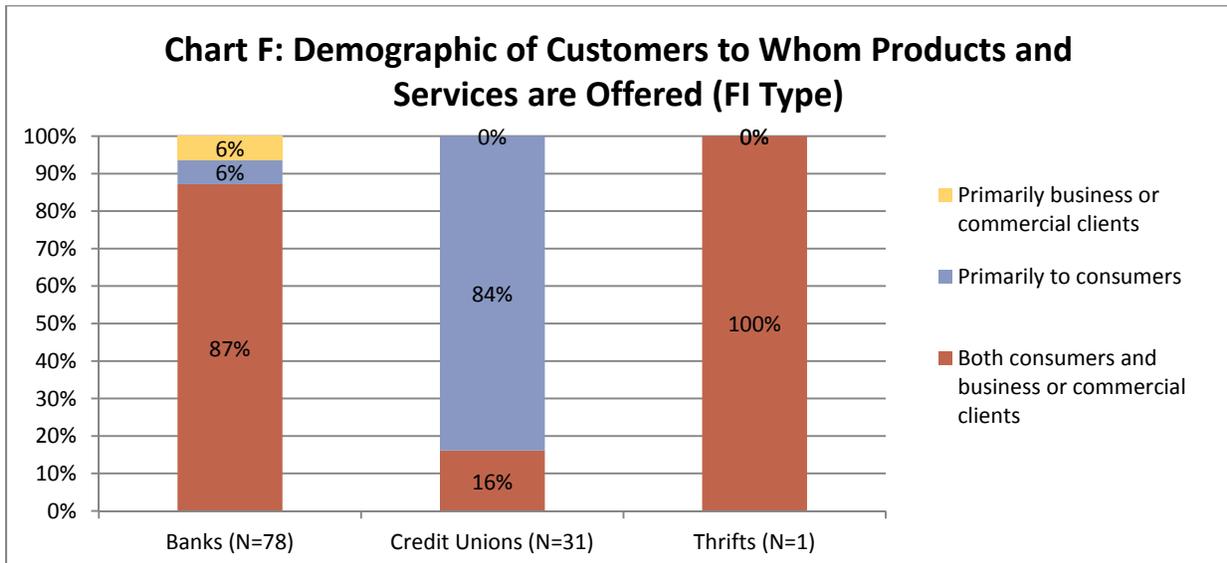
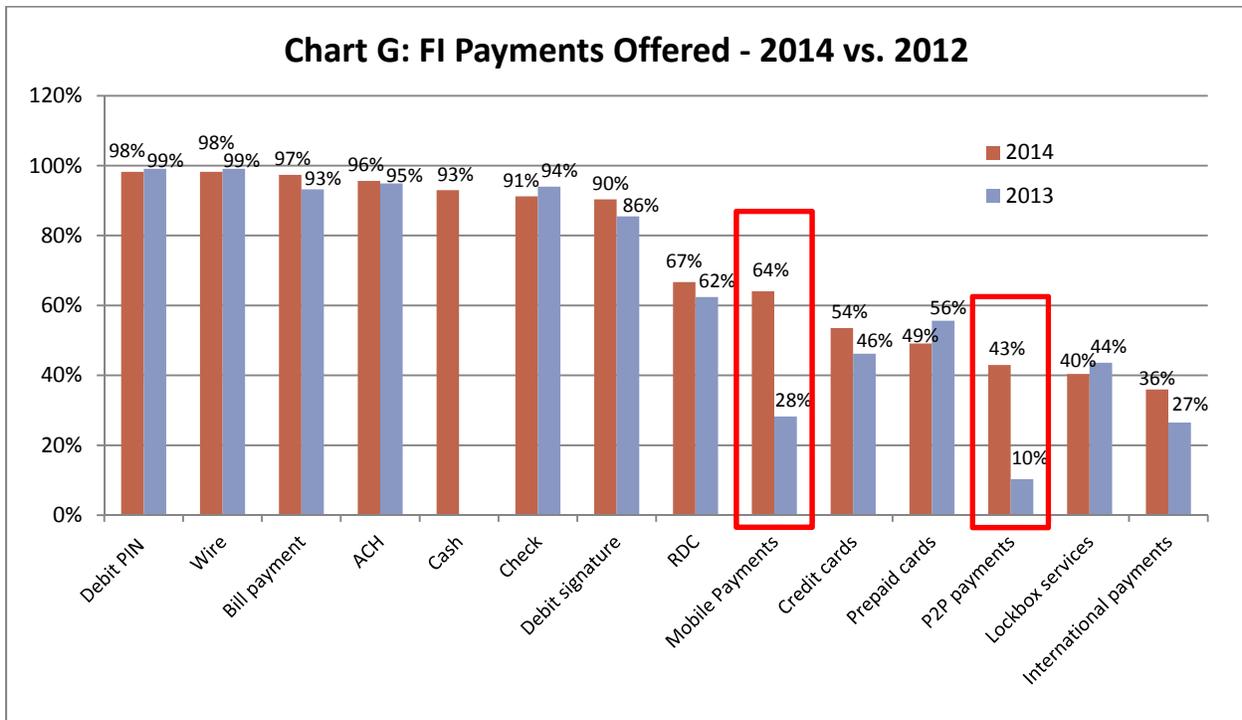
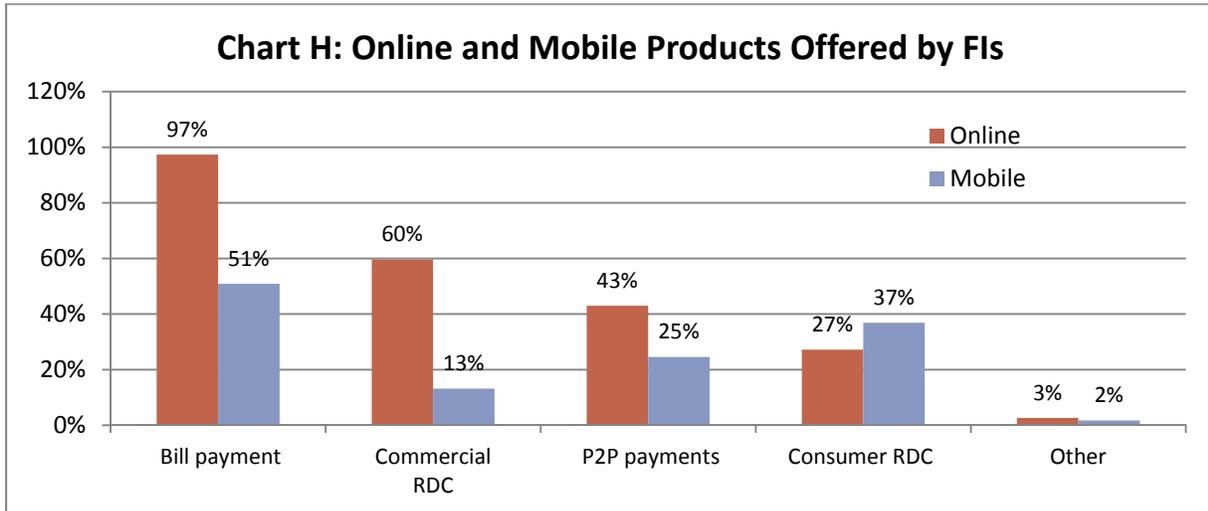


Chart G illustrates the type of payments offered by financial institution respondents and compares this survey's results with those from 2012. Not surprising is the growth shown for P2P and mobile payments, with more institutions offering these types of payments.



⁵ Note that there was only one thrift respondent to the survey, so, admittedly, the results may not be representative of all thrifts in the district.

Chart H illustrates in more detail the mobile and online offerings by financial institutions. Nearly all financial institutions surveyed offer online bill payments and half offer bill payment through mobile. More financial institutions offer remote deposit capture (RDC) to businesses as an online product (60 percent) than those that offer it as a mobile product (13 percent). But more financial institutions offer RDC to consumers as a mobile product (37 percent) than offer it to consumers as an online product (27 percent).



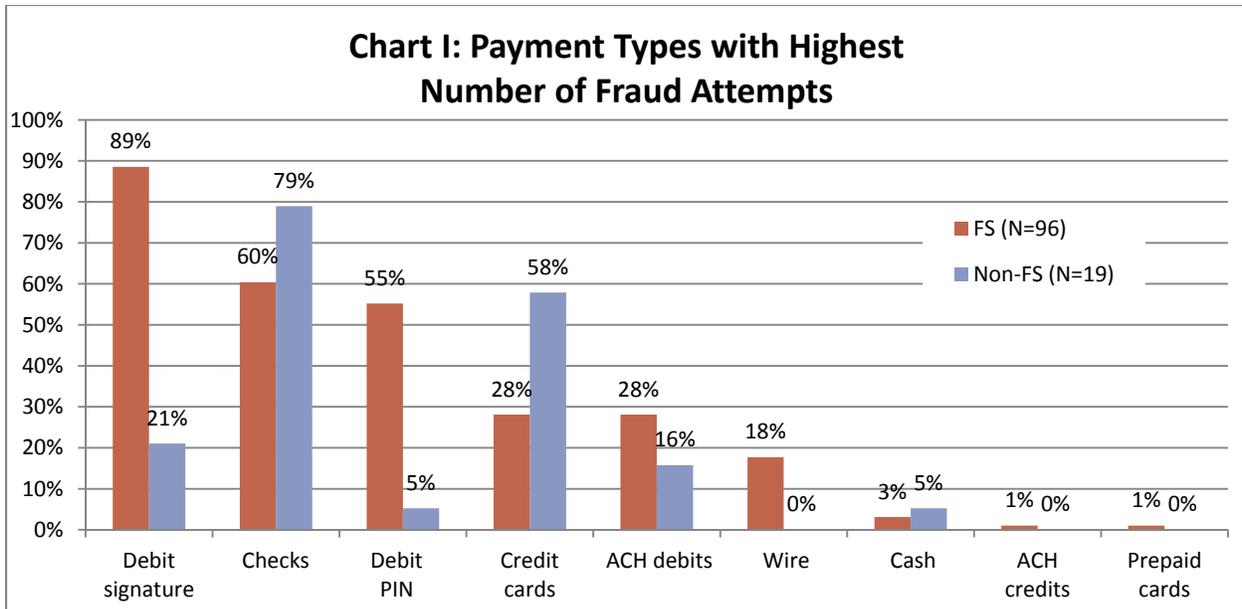
Payment Fraud Attempts and Financial Losses

This section analyzes payment fraud for different types of organizations. The survey results show that 86 percent of financial services respondents had payment fraud attempts in 2013 and 63 percent of nonfinancial services respondents had payment fraud attempts.

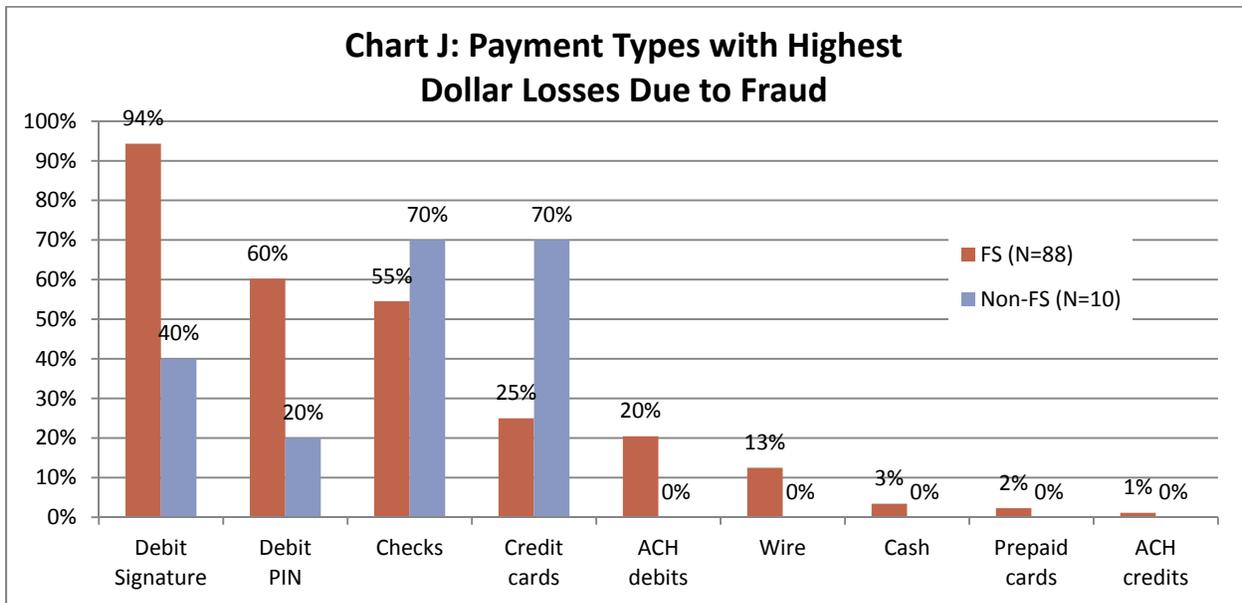
Respondents were asked to choose the top three payment types with the highest number of fraud attempts for their organization, regardless of the actual financial losses. Chart I shows the differences between financial and nonfinancial organizations and the types of fraud attempts each experienced.

A high percentage of nonfinancial services organizations accept check and credit cards as payment options, resulting in a higher percentage reporting fraud attempts in those two payment types. The trends shown in Chart I are fairly consistent with the 2012 survey results.

The majority of financial services industry respondents reported that signature debit, checks and PIN debit were among the top three payment types with the highest fraud attempts, which follows the same trend as reported in 2012.



The majority of respondents experienced fraud losses (88 percent of financial service respondents and 38 percent of nonfinancial institution respondents⁶). Respondents that experienced fraud losses were asked to choose the top three fraud types that caused the highest dollar losses. Similar to the 2012 survey, financial services entities identified signature debit as having the highest dollar losses, followed by PIN debit and checks. However, nonfinancial services respondents identified checks and credit cards as having the highest dollar losses, followed by signature debit and PIN debit. When comparing Chart I and Chart J, you see that the top categories for fraud losses are consistent with the top categories for fraud attempts.



⁶ See Table 2 on page 13.

To better understand the true cost of payments fraud, this survey looked at the financial losses associated with a fraud event against an institution’s cost to invest in infrastructure improvements, fraud mitigation strategies and loss resolution programs, which must occur whether or not a payments fraud has occurred. Respondents were asked whether fraud prevention costs or actual fraud losses were a greater expense for their organization for each payment type listed. The results are shown in Charts K and L.

Similar to the finding in 2012, for all payment types except signature debit, a greater percentage of financial services respondents indicated their fraud prevention costs exceed their actual dollar losses to fraud than those that indicated their dollar losses were greater than their fraud prevention costs.

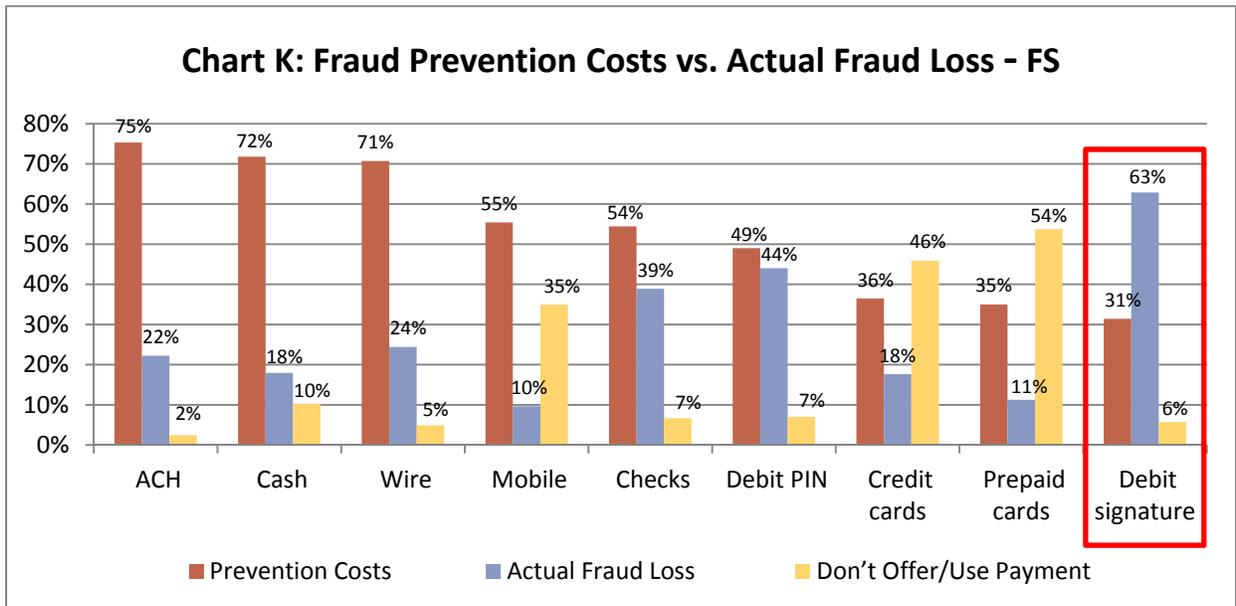
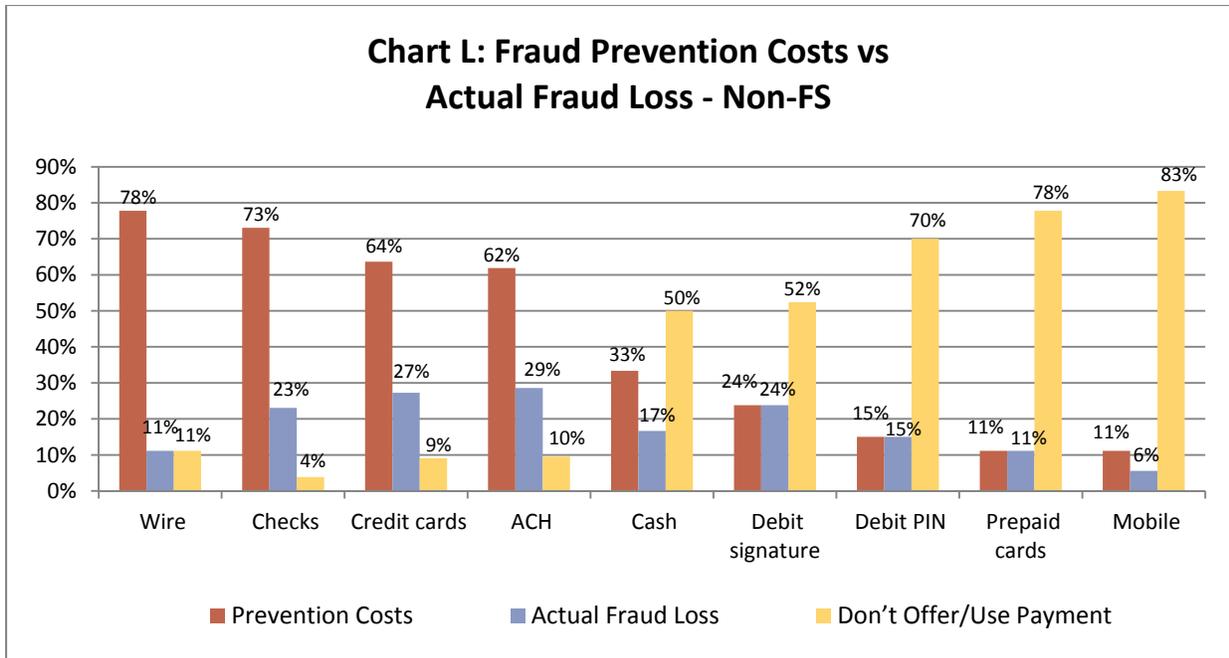
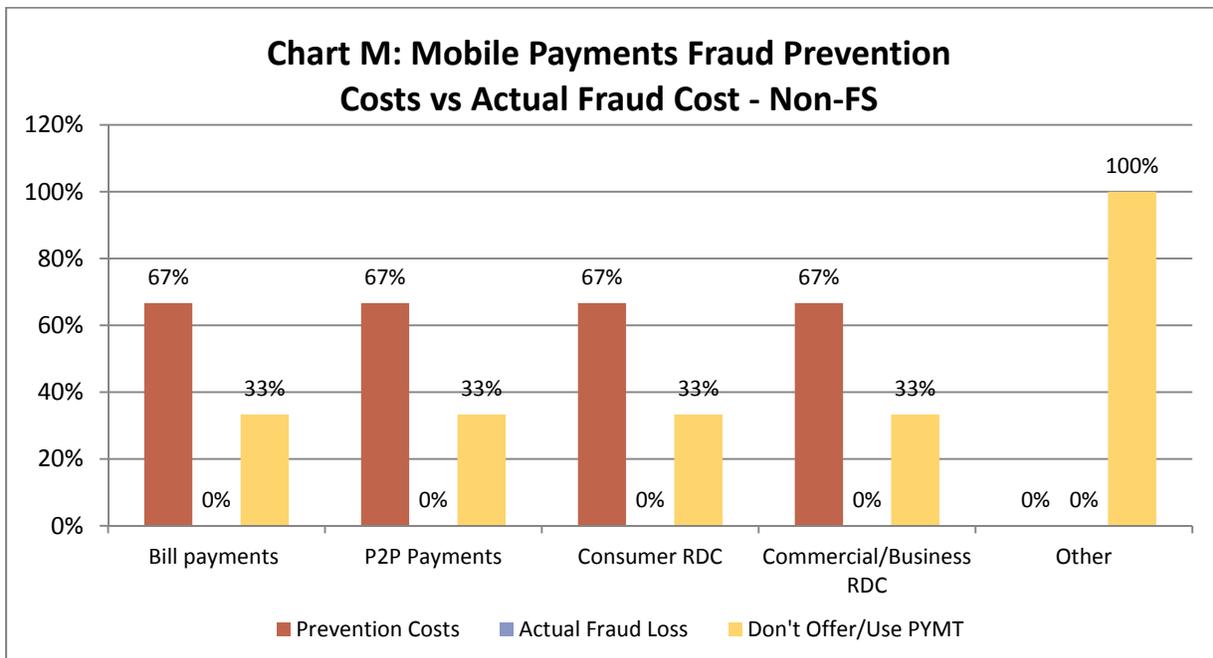


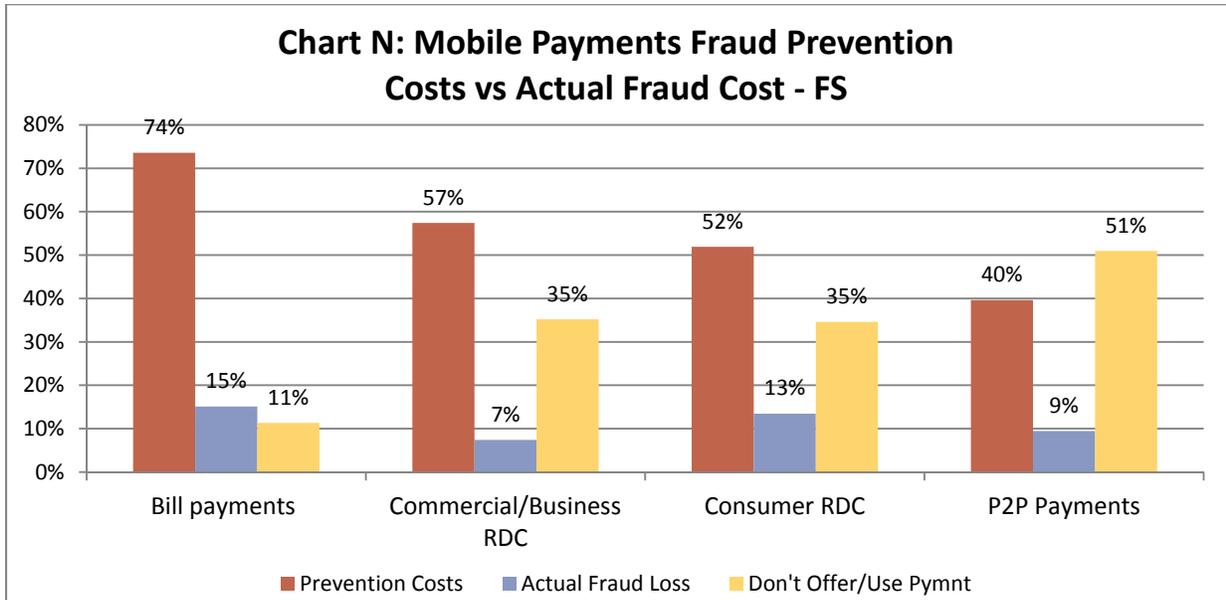
Chart L shows that a high percentage of nonfinancial services respondents do not use cash, signature debit, PIN debit, prepaid cards or mobile payments. Perhaps there is still not a good business case to accept these payment types, in light of the perceived cost for fraud prevention and possible losses. For those payment types used, the majority of nonfinancial services respondents indicated that fraud prevention costs tend to be greater than actual fraud losses.



Mobile payments are fast becoming a popular payment choice for consumers and financial institutions. There is debate about the security of mobile payments with some arguing that mobile payments carry a higher risk, especially if multiple third parties are involved in the transaction, while others argue that the mobile device itself provides the possibility of higher levels of security. Focusing specifically on mobile payments, respondents were asked if fraud prevention costs or actual fraud losses were a greater expense. The results show that only a few nonfinancial services respondents offered any of the mobile payments; for those that do, fraud prevention costs were greater than actual losses as shown in Chart M.



Financial services organizations offer mobile payment options and for the majority, fraud prevention costs exceeded their fraud losses for the four mobile payment types shown in Chart N.



It is important to note that we cannot tell from the data in the previous four charts how much higher prevention costs are than actual fraud losses. It is possible that prevention costs are higher because they are, indeed, effective, and losses might be much greater if such measures had not been in place and more actual fraud had occurred. Given the overall trends related to high levels of fraud attempts that were outlined at the beginning of this report, fraud prevention is still crucial; therefore, both prevention cost and prevention benefits should be considered when making these business decisions.

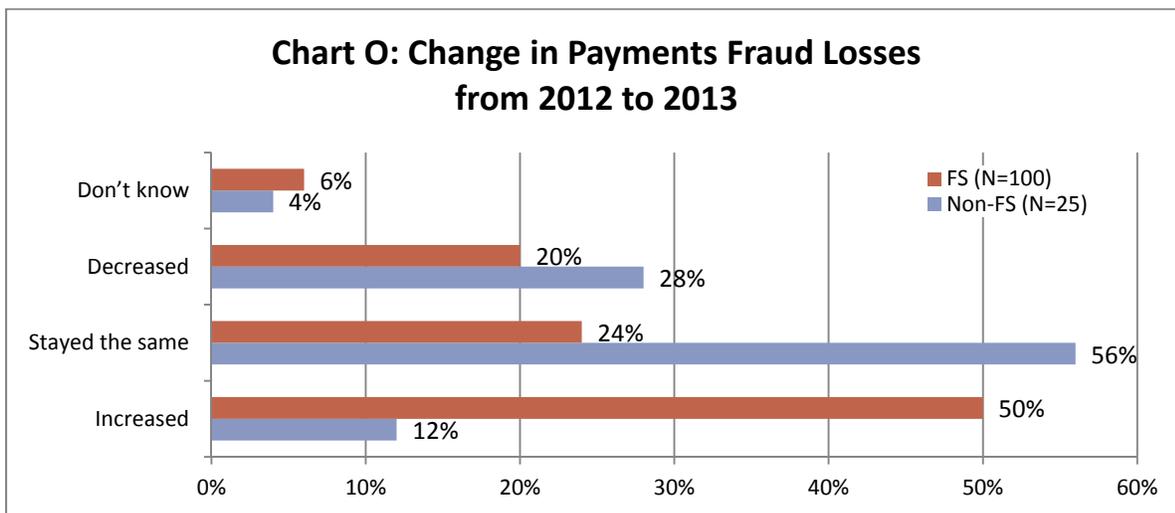
Payments fraud appears to be effectively managed when measured by financial losses incurred. Respondents were asked to estimate the losses they experienced due to fraud as a percentage of the company's total revenue. As shown in Table 2, 90 percent of the respondents reported losses due to fraud as less than 0.5 percent of their total revenue. These responses are similar to the responses in the 2012 survey, so the total loss, estimated as a percentage of revenues, continues to be relatively small for the vast majority of respondents. In fact, 12 percent of financial services respondents reported no losses in 2013 due to payments fraud.

Over half (62 percent) of the nonfinancial services respondents reported no losses; however, this is down from 77.8 percent of organizations that reported no losses incurred in 2011. Nonetheless, losses remained relatively low.

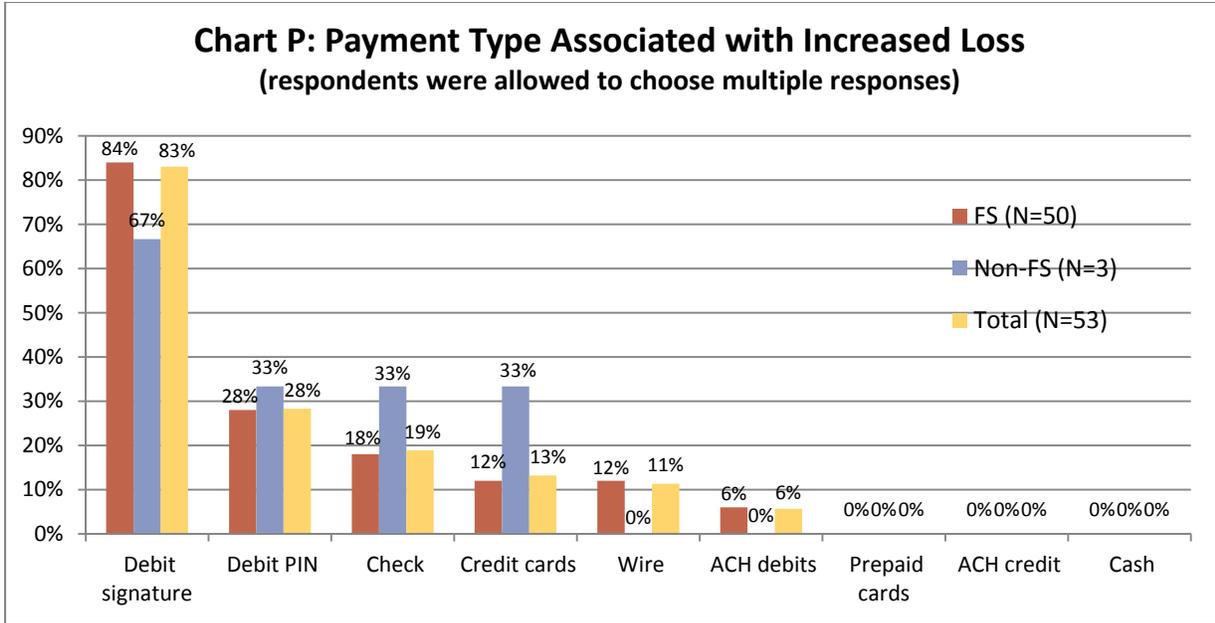
Table 2

Loss Range as a Percent of Annual Revenue	Financial Service Respondents	Nonfinancial Service Respondents	All Respondents
No losses	12%	62%	23%
Over 0%-.3%	55%	31%	50%
.3%-.5%	20%	8%	17%
.6%-1%	4%	0%	3%
1.1%-5%	8%	0%	7%
Over 5%	1%	0%	1%

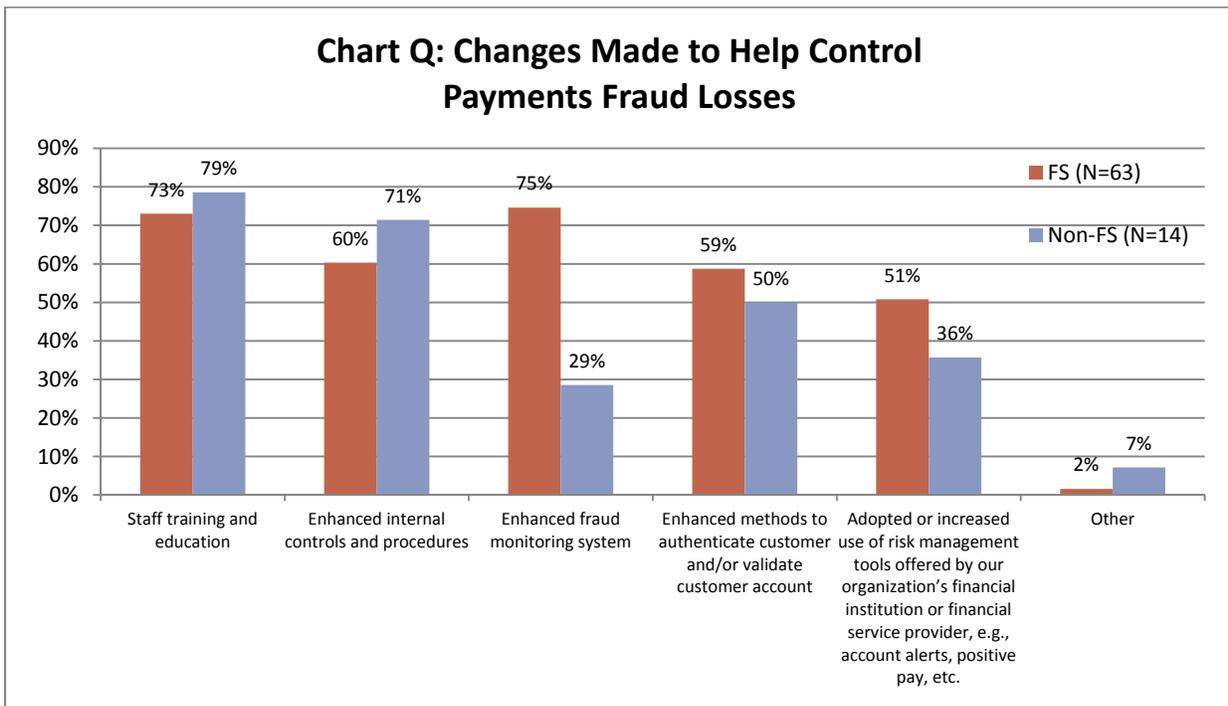
To help us understand fraud loss trends over time, respondents were asked to gauge whether fraud losses had increased, decreased or stayed the same as the year before. The results are shown in Chart O. These numbers did not change substantially from the 2012 survey, when respondents were asked this same question concerning fraud losses in 2012 over 2011.



As shown in Chart P, respondents that reported an **increase** in loss were asked to identify the payment type associated with the increased loss. The majority of the financial services respondents (84 percent) reported signature debit payments as causing increased losses. It is difficult to draw any conclusions for the nonfinancial institutions given the small number of respondents (3 respondents) to this survey question.



Respondents that reported an **increase** in fraud losses or that their fraud losses stayed the same were asked if their organizations made changes that helped to control payments fraud losses. Seventy-two percent of the financial services respondents and 58 percent of nonfinancial respondents indicated changes were made to help control fraud losses. The chart below shows a high involvement by both groups in organizational changes to help control payments fraud losses.



Organizations that indicated an increase or no changes to their fraud losses, who also indicated they enhanced their fraud monitoring systems to help control their fraud losses, were asked to indicate to which payment type the enhanced monitoring applied. Chart R shows that the majority (91 percent) of the financial services respondents enhanced the monitoring of debit card transactions, and 75 percent of nonfinancial services respondents focused more on enhancing the monitoring of credit card transactions, and 50 percent on check transactions. This corresponds to the same areas where each group experienced higher numbers of fraud attempts and dollar losses due to fraud.

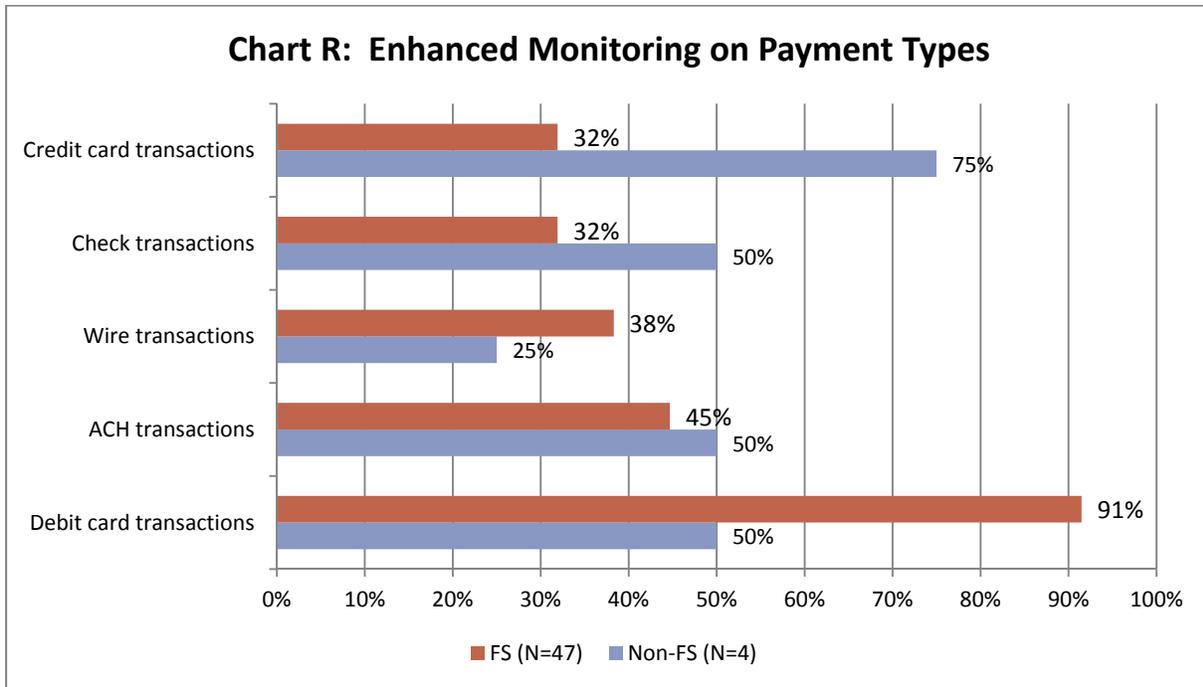
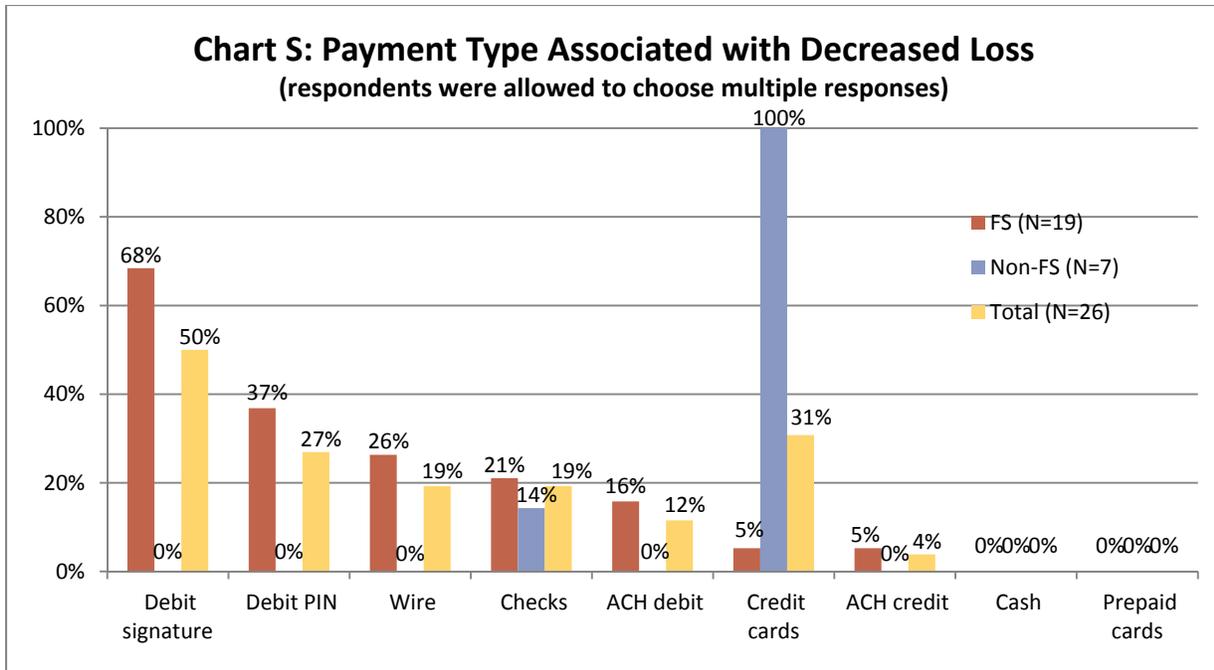
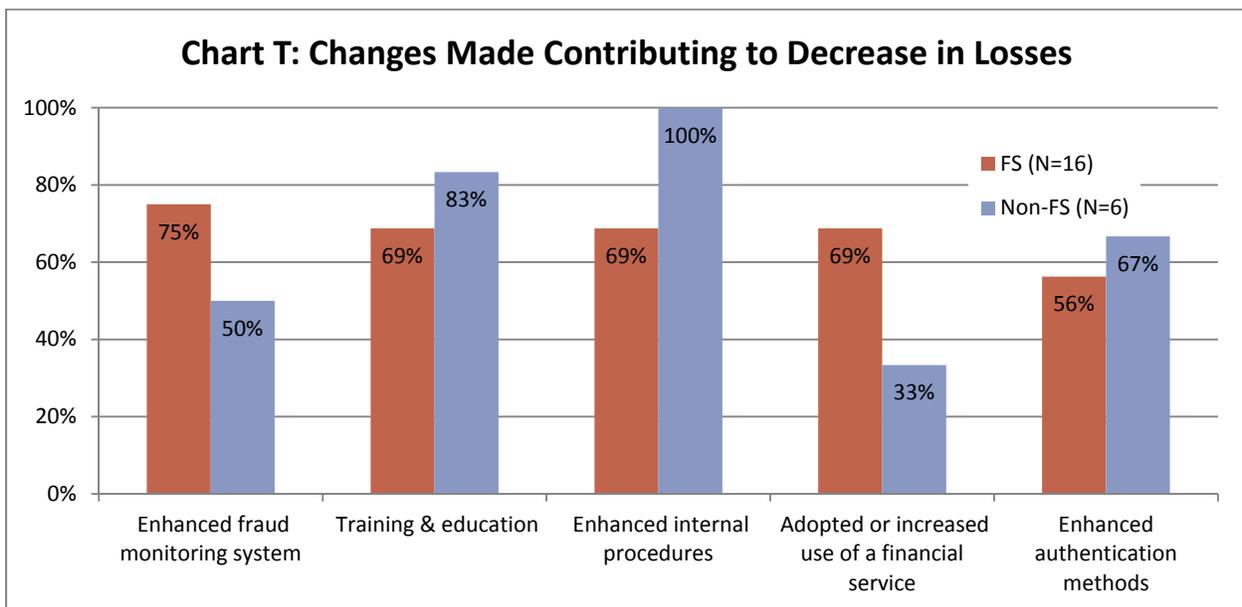


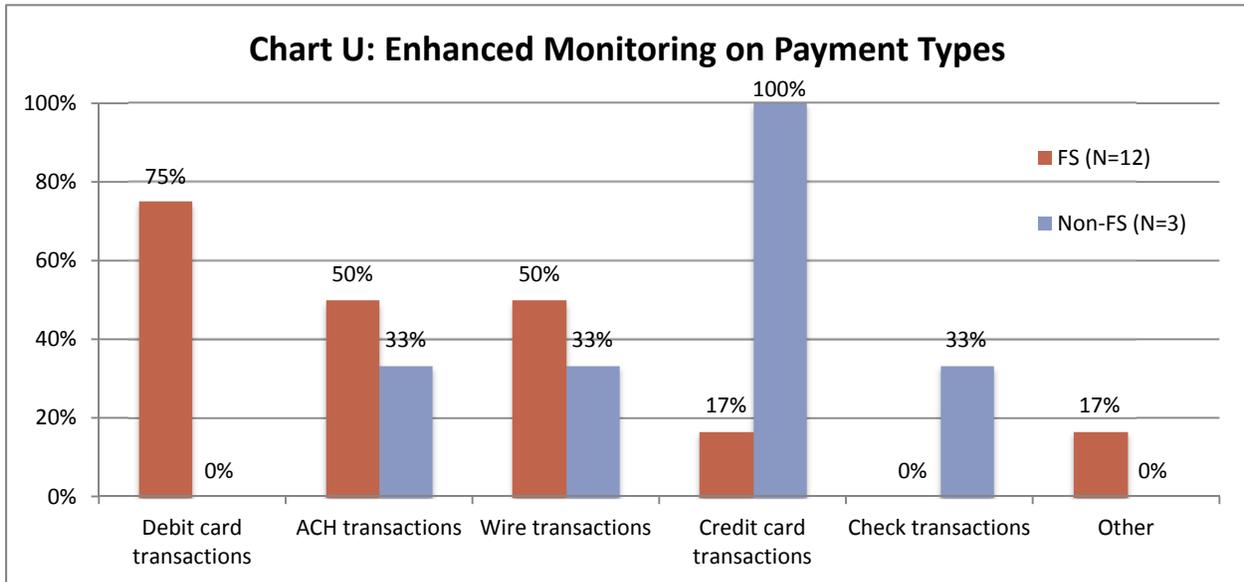
Chart S shows the results for respondents that reported a **decrease** in losses, who were then asked to identify the payment type associated with their decreased loss. Signature debit was chosen by 68 percent of the financial services respondents for causing a decrease in their losses, while all of the nonfinancial services respondents indicated credit cards caused a decrease in their losses.



The following charts illustrate the types of changes that organizations made that also reported **decreases** in their fraud losses from the previous year. When asked if their organizations made any changes to payments risk management procedures that led to the decrease in payments fraud losses, 85 percent of the financial services respondents and 86 percent of the nonfinancial services respondents indicated they had made changes. Chart T shows a high level of involvement by both groups in five types of risk management practices. Three-fourths of the financial services respondents indicated they made changes that enhanced their fraud monitoring system, and all of the nonfinancial services respondents enhanced their internal controls and procedures.



Respondents who indicated their fraud losses were reduced by enhancements to their fraud monitoring systems were asked to further identify the payment types to which the enhanced monitoring applied. Their responses are summarized in Chart U. Seventy-five percent of financial services respondents took steps they viewed as helping to decrease debit card transaction fraud, and all of the nonfinancial services respondents also viewed the enhancements to their fraud monitoring as helping to decrease credit card fraud, but because of the small number of nonfinancial respondents (3 respondents) to this survey question, it is difficult to draw any conclusions.



Perpetrators Involved in Successful Payments Fraud

The following section is an analysis of successful fraud attempts, how they were perpetrated and the types of fraud schemes that were most often used.

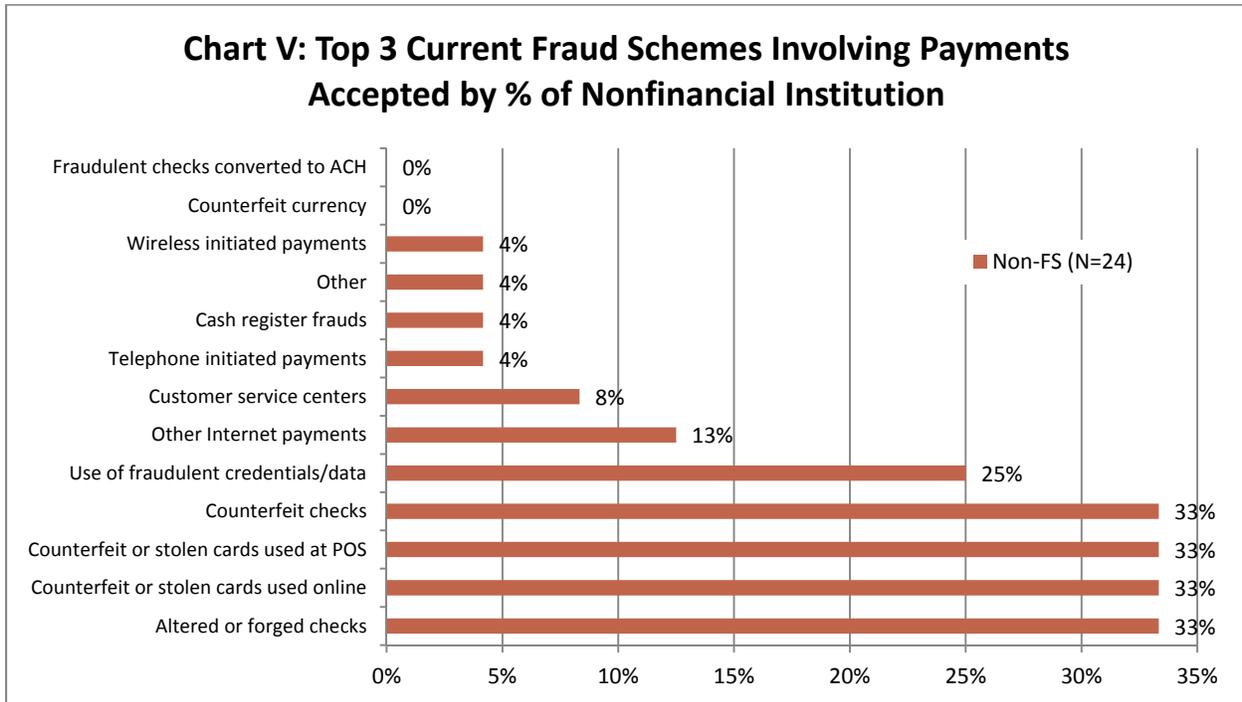
Respondents were asked whether or not their organizations had experienced any successful payment fraud attempts. Seventy percent of financial services respondents and 20 percent of nonfinancial services respondents indicated they were the victims of successful payment fraud attempts in 2013. The majority of both financial services and nonfinancial services respondents reported that the successful fraud was committed by “external parties only” and not by internal staff or internal staff working with an external party.

Most Common Fraud Schemes

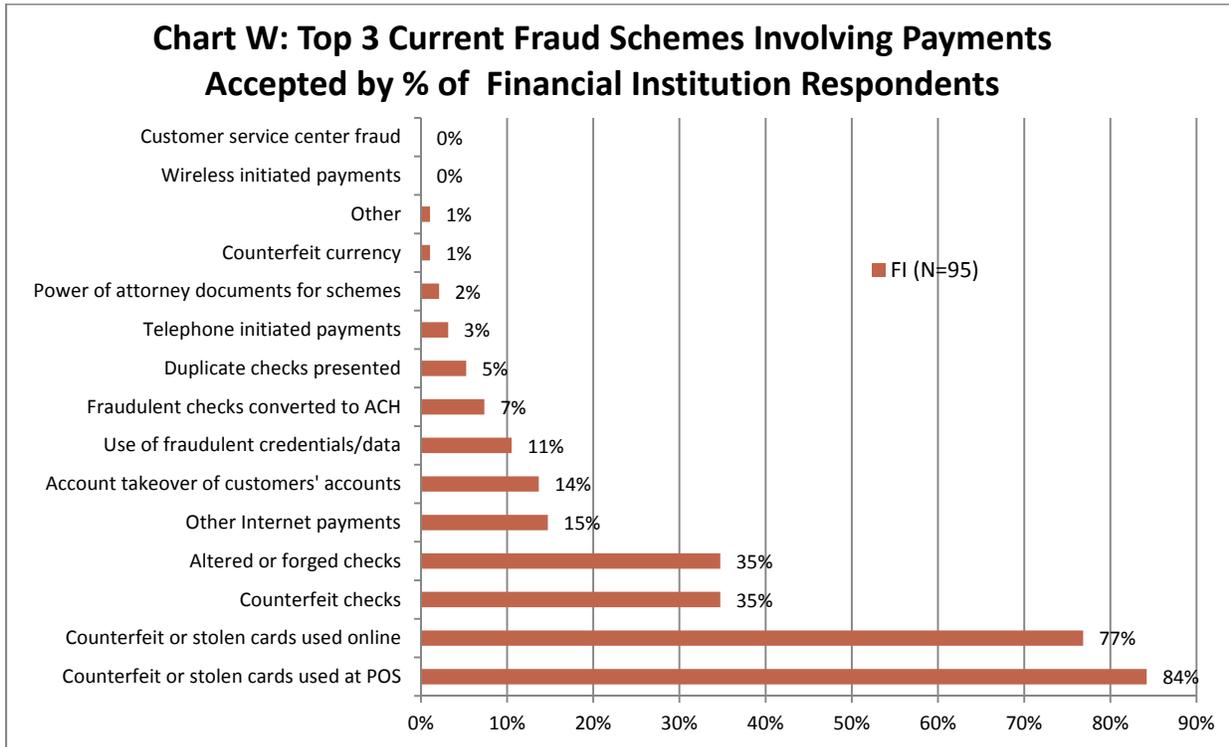
Respondents were asked to list the top three schemes used most often to initiate payments fraud in the following areas:

- Payments received or accepted by nonfinancial firms
- Payments by or on behalf of financial institutions’ customers
- Payments against the respondent’s own bank accounts

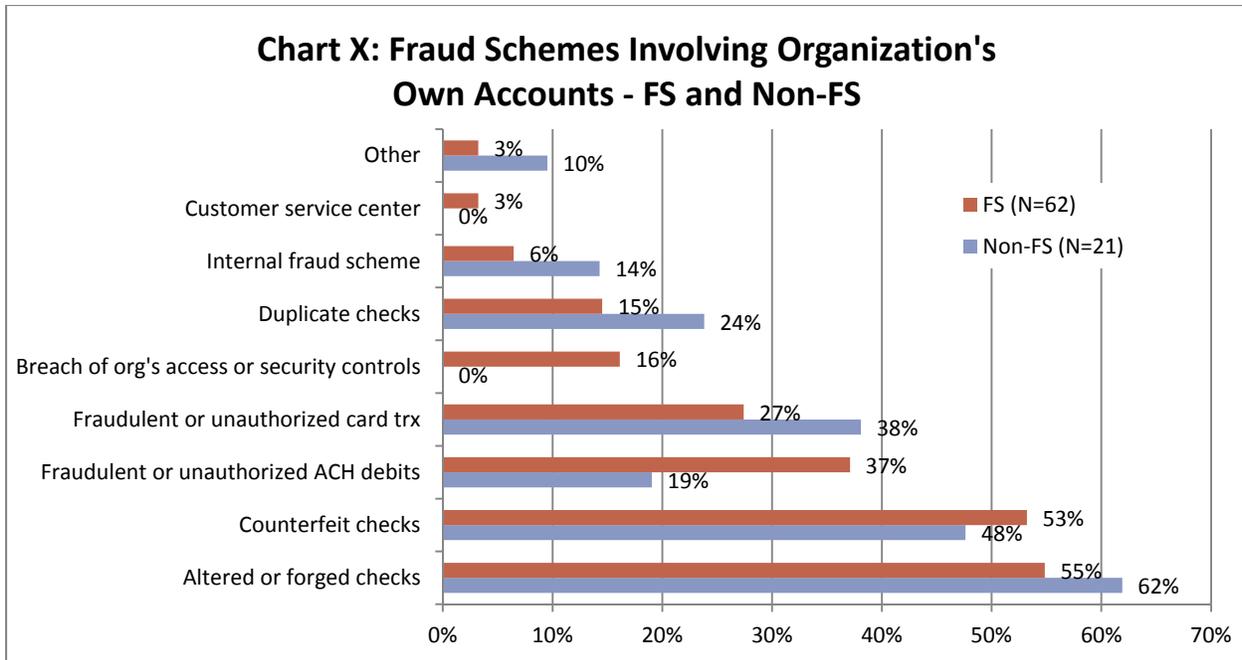
Chart V shows for payments accepted by nonfinancial institution respondents (including payment processors) the following fraud schemes were most often ranked as one of the top three: altered or forged checks, counterfeit or stolen cards used on line, counterfeit or stolen cards used at point of sale (POS), and counterfeit checks. The use of fraudulent credentials or data was ranked in the top three fraud schemes by 25 percent of nonfinancial institution respondents, which is up from only 7 percent of respondents indicating it was in the top three in 2012.



When financial institution respondents were asked to select the top three fraud schemes used to commit fraud for payments by or on behalf of their customers, the answers were similar to the 2012 survey. In this survey, 84 percent of banks, credit unions and thrifts chose counterfeit or stolen cards used at the POS, 77 percent chose counterfeit or stolen cards used online, and 35 percent chose both counterfeit checks and altered or forged checks (see Chart W).



When asked about the fraud against their organization’s own banking account(s), half of the financial services respondents identified altered or forged checks and counterfeit checks as the top schemes most often used, followed by fraudulent or unauthorized ACH debits (37 percent) and fraudulent or unauthorized card transactions (27 percent). Chart X combines the results of both the financial services and the nonfinancial services respondents and indicates that when experiencing fraud against their organization’s own account(s), the two groups reported similar experiences.



Criminals find extremely creative ways to perpetrate payments fraud. Firms that are seeking to combat or prevent fraud must contend with a variety of tactics that can lead to attempted or real data compromise and payments fraud. Table 3 outlines the top three information sources used in fraud schemes for both financial services entities and nonfinancial firms.

For the 2014 survey, compromised sensitive information obtained from lost or stolen cards, checks, or other physical documents or devices was listed as a top source of information used to commit fraud by 47 percent of financial services respondents, which is down from 70 percent in 2012. Data breach due to computer hacking or cyberattacks was cited by 42 percent of the financial services respondents, an increase from 27 percent in 2012. Among nonfinancial firms, 48 percent indicated that the top source of information used to commit fraud was bank account information obtained from a legitimate check issued by the organization, which is down from 67 percent in 2012. Data breach due to computer hacking or cyberattacks was cited by only 4 percent of the nonfinancial services respondents, a decrease from 20 percent that chose it in 2012.

For the first time, in 2014, respondents were allowed to choose “unknown” as a top information source used to commit fraud. Importantly, this category was listed by the highest percentage of nonfinancial firms (52 percent), and by nearly one-fourth of the financial services industries (24 percent). While we cannot compare this answer with previous years’ responses, these results imply that organizations are often unaware of the nature of the compromise that led to successful payments fraud. “Social engineering”⁷ was also added as a potential data

⁷ Social Engineering is the practice of deceiving someone, either in person, over the phone, or using a computer, with the intent of breaching some level of security. It often involves an e-mail that falsely claims to be from a legitimate person or organization.

compromise source in 2014; 12 percent of financial services respondents and none of the nonfinancial firms indicated this as one of the most significant ways that criminals were able to obtain information to perpetrate payments fraud.

Table 3

Information Sources Used to Commit Fraud	2014			2012		
	FS (N=90)	Non-FS (N=23)	All Org. (N=113)	FS (N=96)	Non-FS (N=15)	All Org. (N=111)
“Sensitive” information obtained from lost or stolen card, check or other physical document or device while in consumer’s control	47%	26%	42%	70%	33%	65%
Physical device tampering, e.g., use of skimmer on POS terminal or obtaining magnetic stripe information	43%	17%	38%	38%	0%	32%
Data breach due to computer hacking or cyberattacks	42%	4%	35%	27%	20%	26%
Email and webpage cyberattacks, e.g., phishing, spoofing and pharming to obtain “sensitive” customer information	37%	26%	35%	31%	13%	29%
Information about customer obtained by family or friend	28%	4%	23%	24%	0%	21%
Information sources are unknown	24%	52%	30%	na	na	na
Organization’s information obtained from a legitimate check issued by your organization	22%	48%	27%	25%	67%	31%
Social engineering	12%	0%	10%	na	na	na
Employee with legitimate access to organization or customer information (employee misuse)	2%	13%	4%	2%	20%	5%
Lost or stolen physical documentation or electronic devices while in control of the organization	2%	13%	4%	4%	7%	5%
Other	na	na	na	14%	20%	14%

Payments Fraud Mitigation Strategies

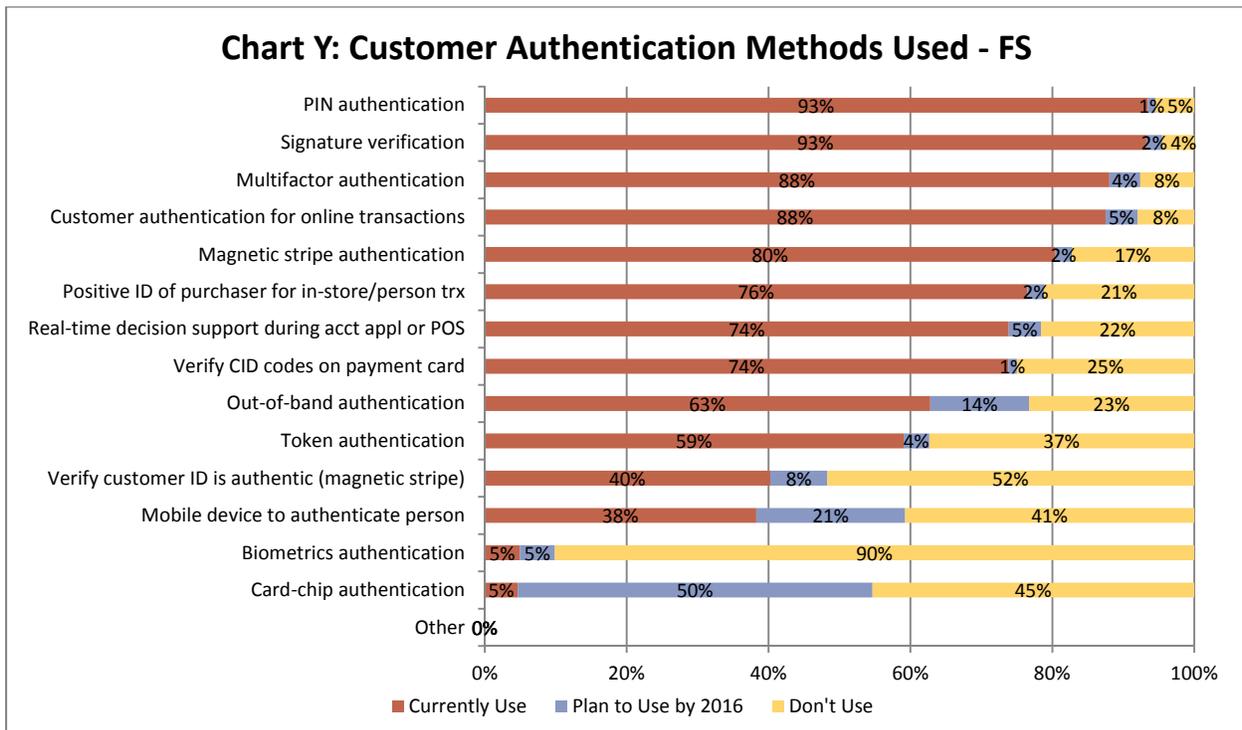
To keep up with the constantly evolving strategies that criminals use to commit payment fraud, firms must be vigilant in developing and implementing a variety of strategies to prevent fraud from occurring and lessen its impact in cases when it is successful. The next section breaks down fraud mitigation strategies into four categories and examines the respondents’ views of their usage and effectiveness. These categories are:

1. Customer Authentication Methods
2. Transaction Screening and Risk Management Methods
3. Internal Controls and Procedures
4. Risk Mitigation Services Offered by Financial Service Organizations

Customer Authentication Methods

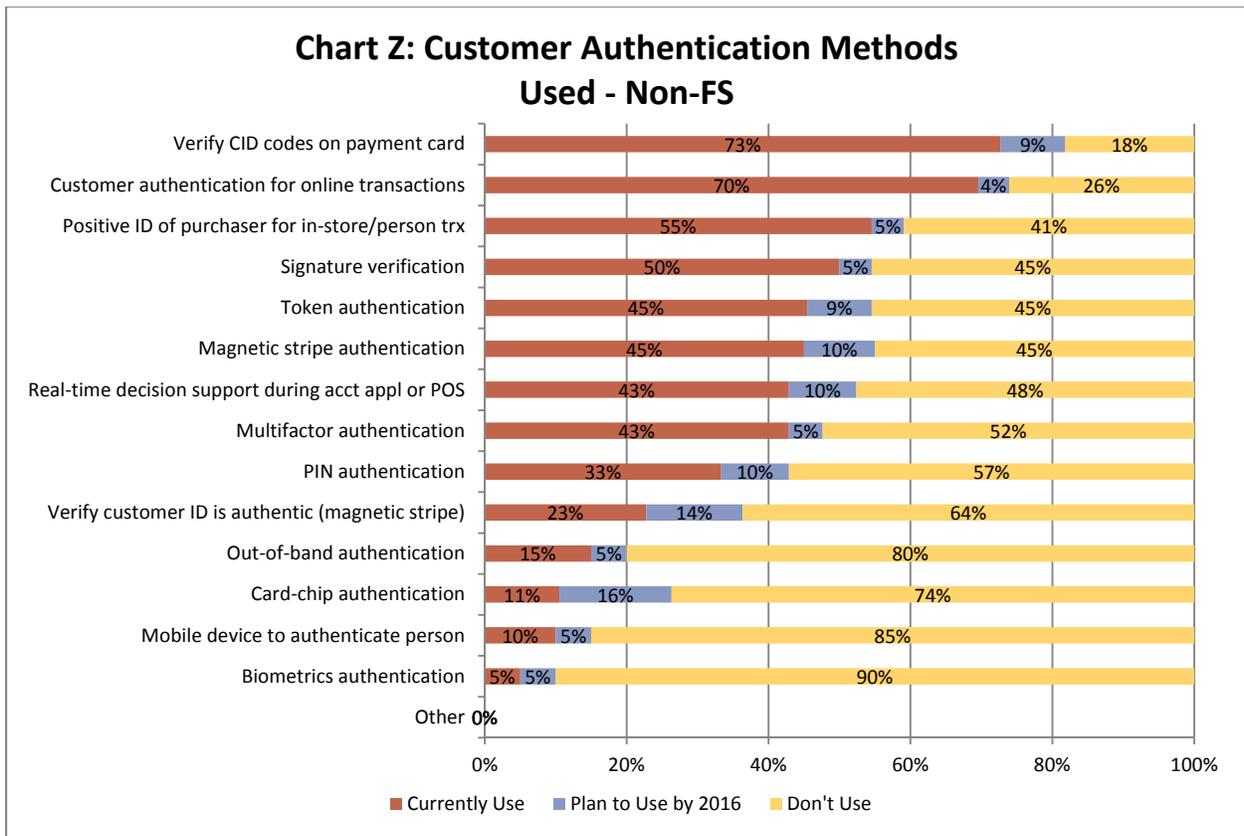
This year, the survey included 14 different authentication methods, compared to 10 that were included in 2012. New to the survey this year were token authentication, out-of-band authentication, mobile device to authenticate person and multifactor authentication.⁸ These additions reflect technological advances and changes in the marketplace.

Financial institutions rely on many of the authentication methods listed, as shown in Chart Y. Eight authentication methods are used by more than 70 percent of financial services companies. Lower levels of usage are seen of the new methods of authentication added as choices to the survey this year, such as tokens (59 percent), out-of-band authentication (63 percent) and using a mobile device to authenticate a customer (38 percent). Chip-card authentication is used by only 5 percent of financial services companies surveyed, but 50 percent expect to use chip authentication by 2016. This is likely directly related to the efforts of the major card networks to migrate from magnetic-stripe technology for cards to an EMV chip-card environment.



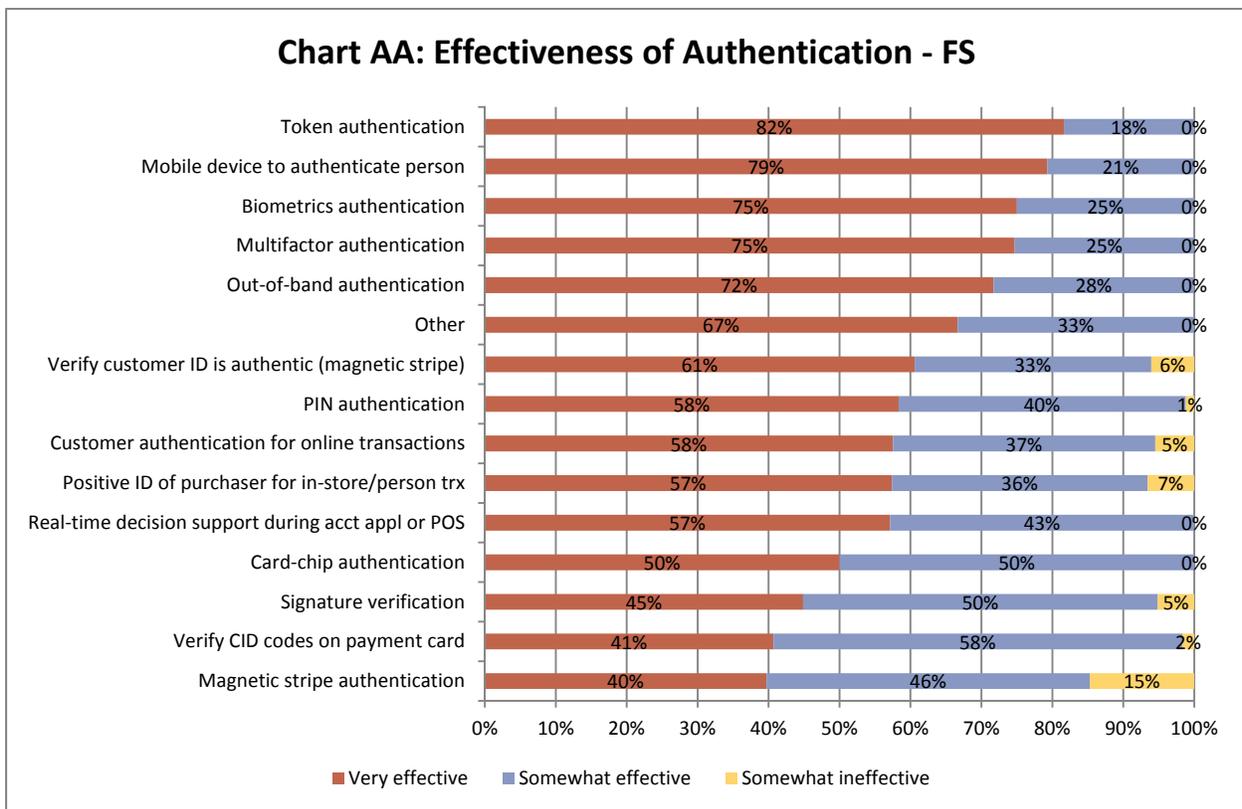
⁸ *Token authentication* as used here refers to a physical token such as a USB token or “fob.” *Out-of-band authentication* includes any technique that allows the identity of the individual originating a transaction to be verified through a channel different from the one the customer is using to initiate the transaction (i.e., a phone call, an email, or a text message). *Mobile device to authenticate person* is often used as one of the authentication factors in multifactor 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. *Multifactor authentication* uses two or more factors for authentication: something only the user knows (the PIN), something only the user has (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.

Nonfinancial firms exhibit a very different usage pattern than financial services entities in the category of customer authentication. There are only four authentication methods that are used by more than 50 percent of firms surveyed; verify CID codes⁹ on payment card, customer authentication for online transactions, positive ID of purchaser for in-store or in-person transactions and signature verification. While 88 percent of financial services respondents use multifactor authentication, only 43 percent of nonfinancial firms use more than one form of authentication for customer verification purposes. Further, Chart Z shows that most nonfinancial firms do not have plans to adopt customer authentication methods that they are not currently using in the next few years.

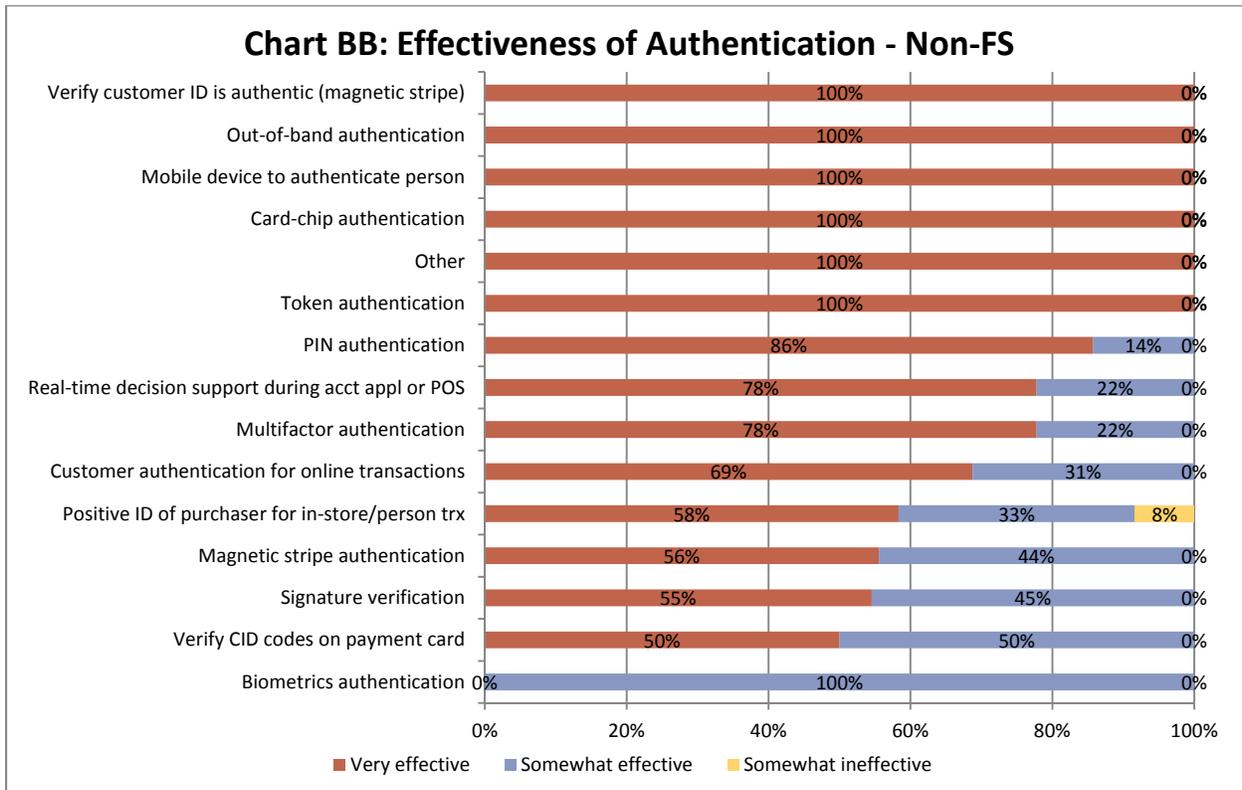


⁹ CID (card identification number), CVV (card verification value), CVC (card verification code) are different terms for a 3- or 4-digit security code that is found on either the front or the back of a payment card. It is used to verify that the cardholder is in possession of the card during a card-not-present transaction.

Survey respondents were asked to rate the effectiveness of their authentication methods. Overall, both categories of respondents indicated that the processes they have in place are effective. As shown in Chart AA, for every method listed, financial services respondents rated them as very or somewhat effective. Though only a limited number of financial services respondents (4) indicated that they use biometrics and chip-card authentication or a mobile device to authenticate the person, as previously shown in Chart Y, the majority rated them very effective, as shown below. Notably, magnetic-stripe authentication is seen as ineffective for the purpose of customer authentication by 15 percent of financial services entities surveyed, most likely because the card credentials stored on the magnetic stripe are easily copied and used to create counterfeit cards. With the move to EMV (chip) cards, successful use of counterfeit cards at the point of sale is expected to diminish because a unique code is generated and transmitted with each transaction, rendering the information, if compromised, useless for creating counterfeit cards.



Nonfinancial firms also are mostly satisfied with the authentication methods they use, as seen in Chart BB.¹⁰

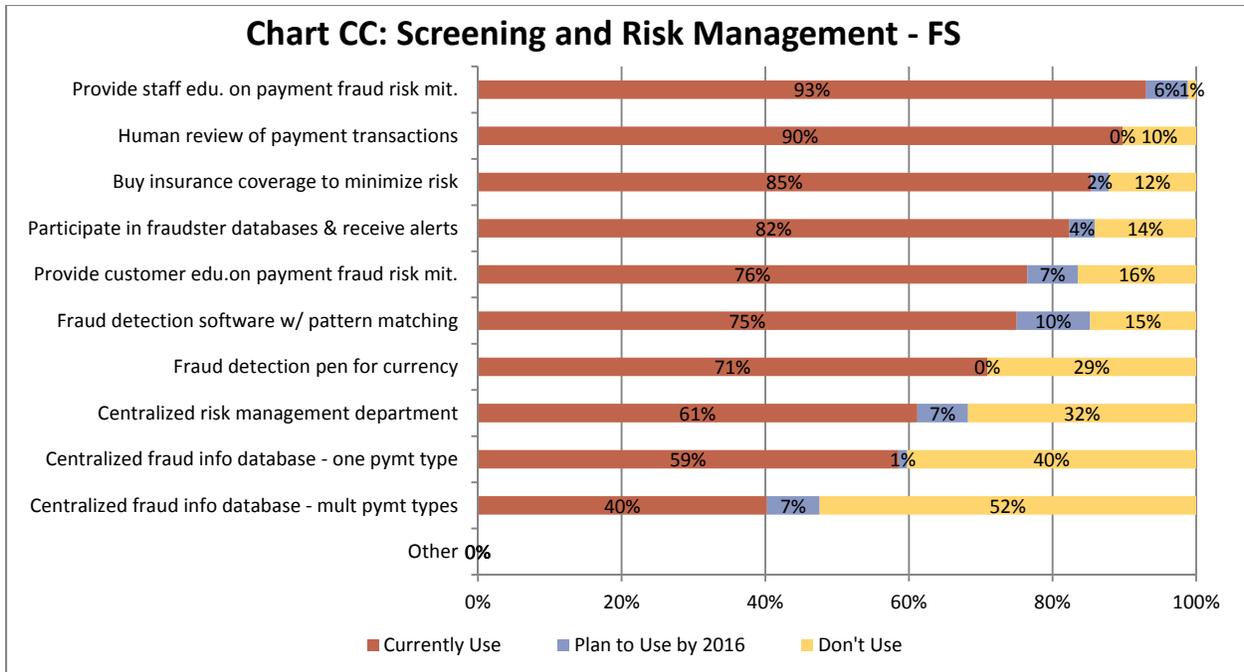


Transaction Screening and Risk Management Methods

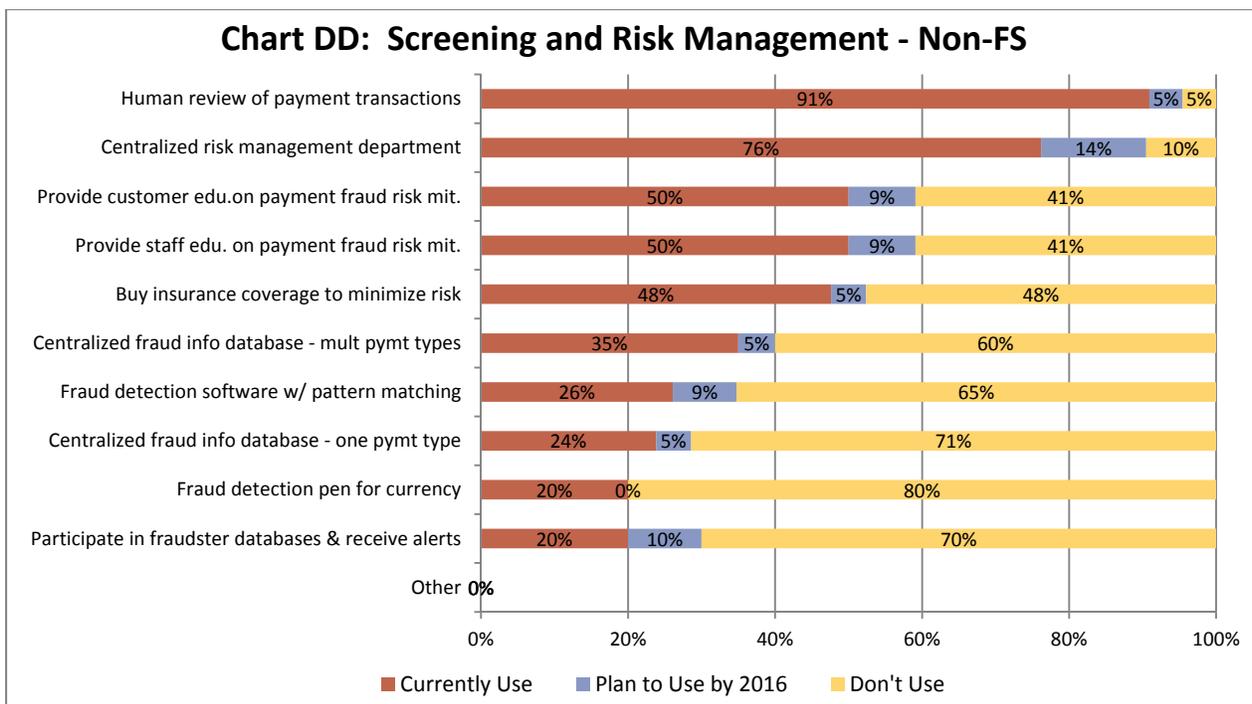
Charts CC and DD show the types of transaction-screening tools and risk management methods used by both financial services entities and nonfinancial firms. Respondents were asked about 10 different screening tools and this year’s survey included “buy insurance coverage to minimize risk” for the first time.

Overall, financial services respondents indicated they use a variety of screening and risk management tools. There are seven categories of tools used by more than 70 percent of surveyed institutions, with one of them being the new choice for this survey – buy insurance coverage. This shows a similar pattern of use compared with the 2012 survey. While 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. Ten percent of financial services respondents plan to institute fraud detection software with pattern matching, and seven percent plan to provide customer education on payment fraud risk, a centralized risk management department and a centralized fraud information database by 2016.

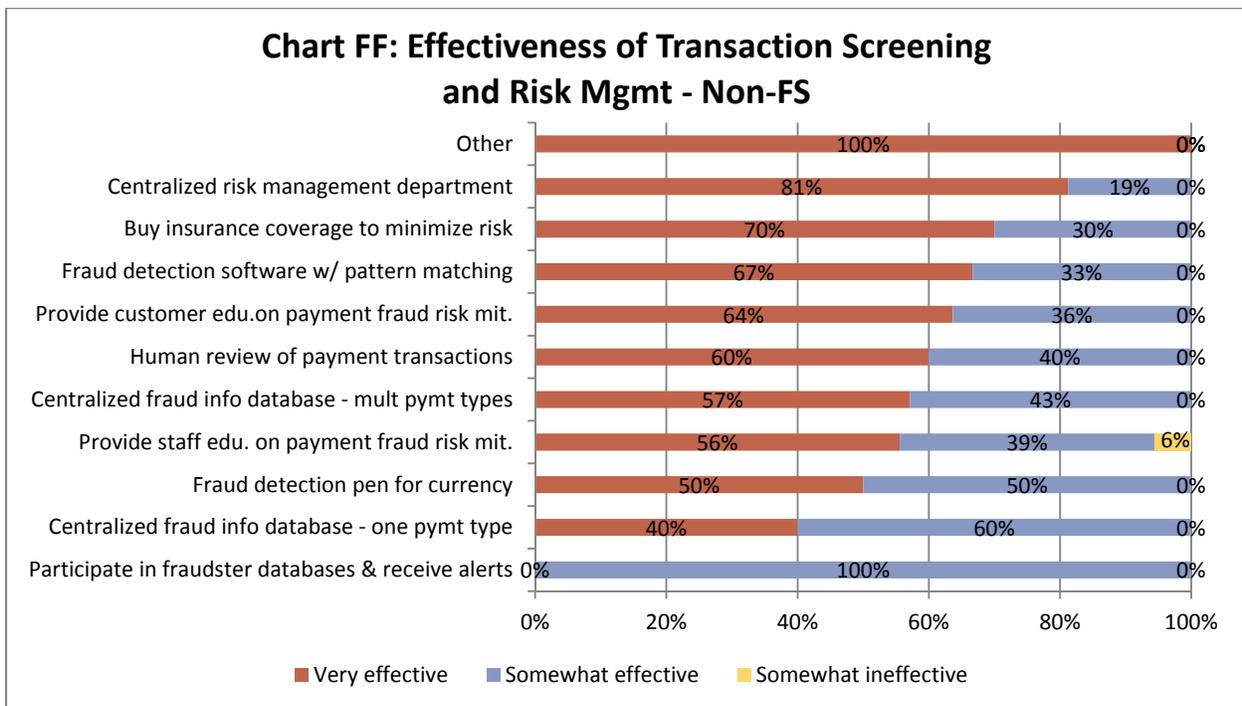
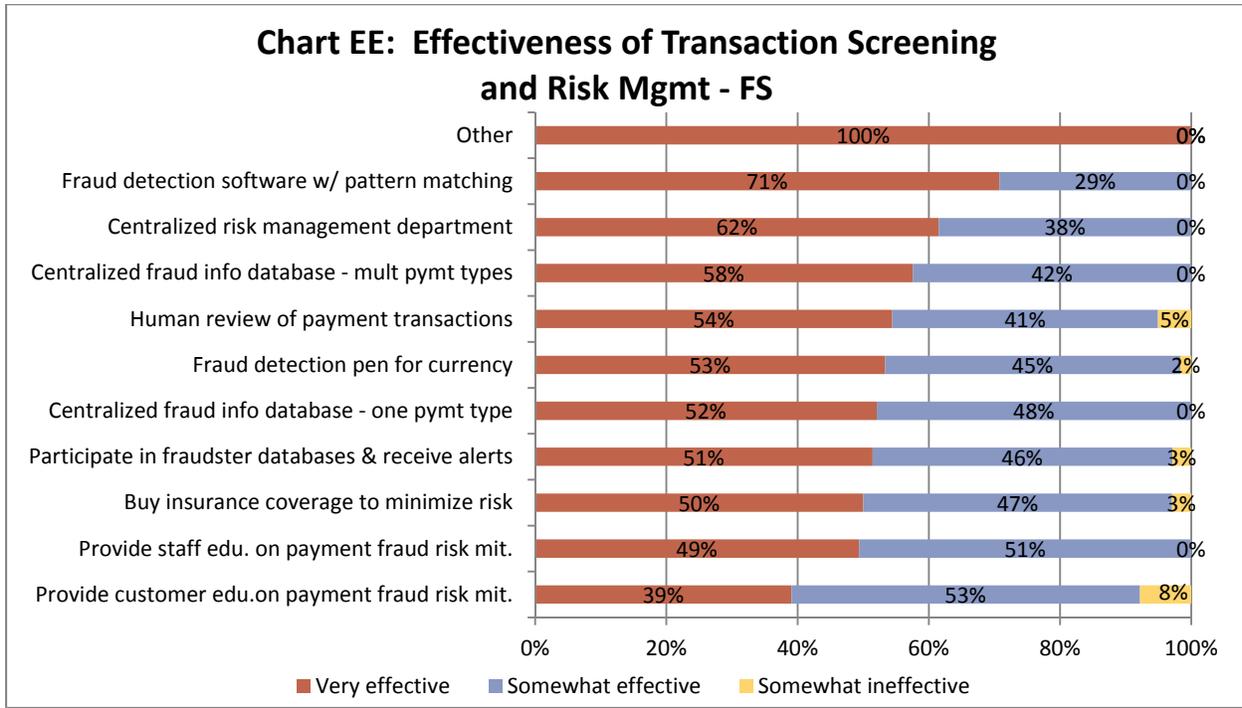
¹⁰ The sampling of respondents was very small that indicated the current use of six authentication methods, with 100% rating them as very effective. This effectiveness rating may not be an accurate indication of nonfinancial firms throughout the industry.



Nonfinancial services respondents also show a similar usage pattern for screening and risk management tools compared with the 2012 survey. Three of the top four methods used by 50 percent or more of the nonfinancial services respondents are the same as in 2012, with the new option, “buy insurance coverage,” being chosen by nearly 50 percent. Most nonfinancial firms are not planning to add new screening and risk management tools, though a centralized risk management department and participation in fraud databases and receive alerts are being considered by 14 percent and 10 percent, respectively, by the year 2016.



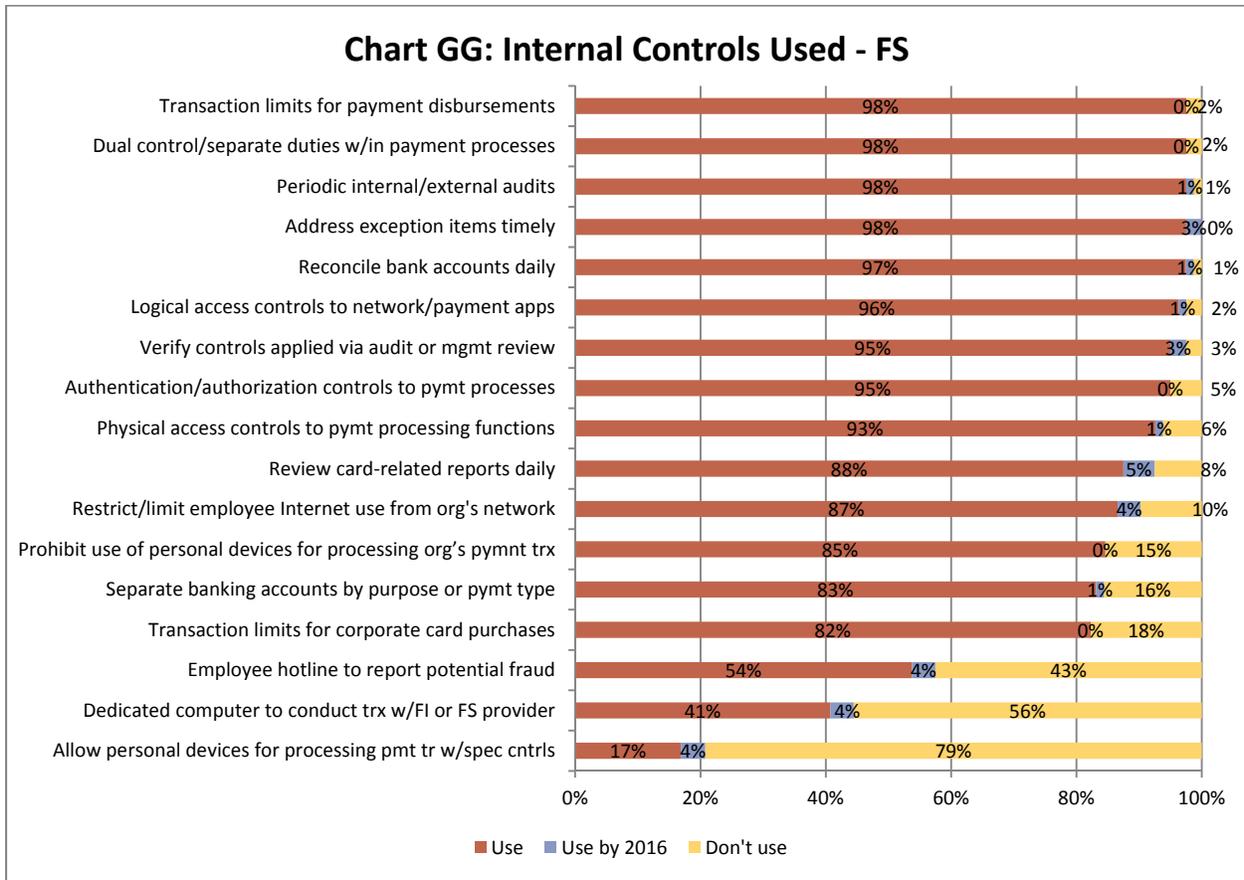
Charts EE and FF show that both financial and nonfinancial services respondents are quite satisfied with the screening and risk management tools they currently use, rating them either highly or somewhat effective.¹¹

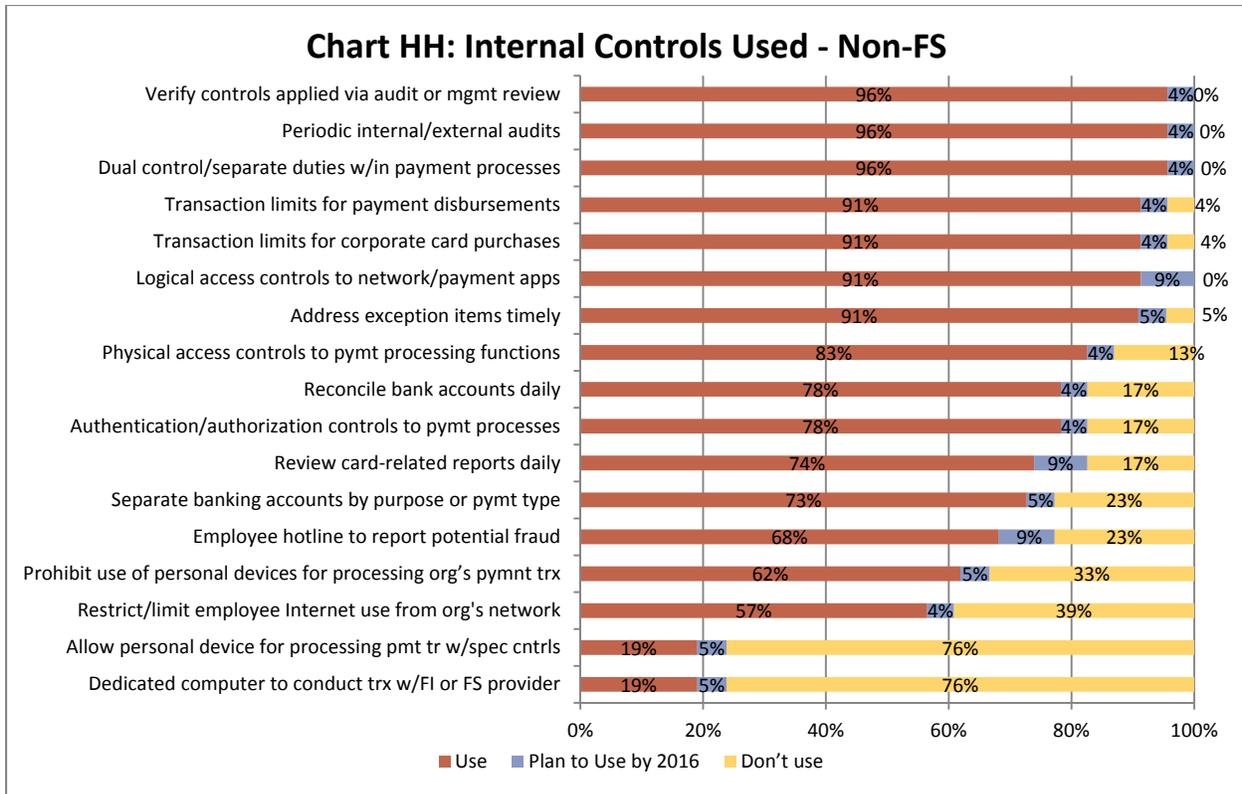


¹¹ Respondents that chose “other” listed “positive pay with bank” and “early warning systems” as screening and risk management tools they also use.

Internal Controls and Procedures

Internal controls and procedures are the fraud mitigation tools that are most likely to be used by both financial and nonfinancial services respondents. More than 80 percent of financial services respondents use 14 or more of the internal controls listed on Chart GG, while more than 60 percent of the nonfinancial firms use 14 or more of the internal controls shown on Chart HH. These two groups are similar in that over 60 percent prohibit the use of personal devices for processing of their organization’s payment transactions with specific controls, which was a choice included in this year’s survey for the first time.





Respondents in both groups that indicated they used the types of internal controls, as shown in the two previous charts, also indicated that the processes they have in place are effective. Their responses are shown in Charts II and JJ.

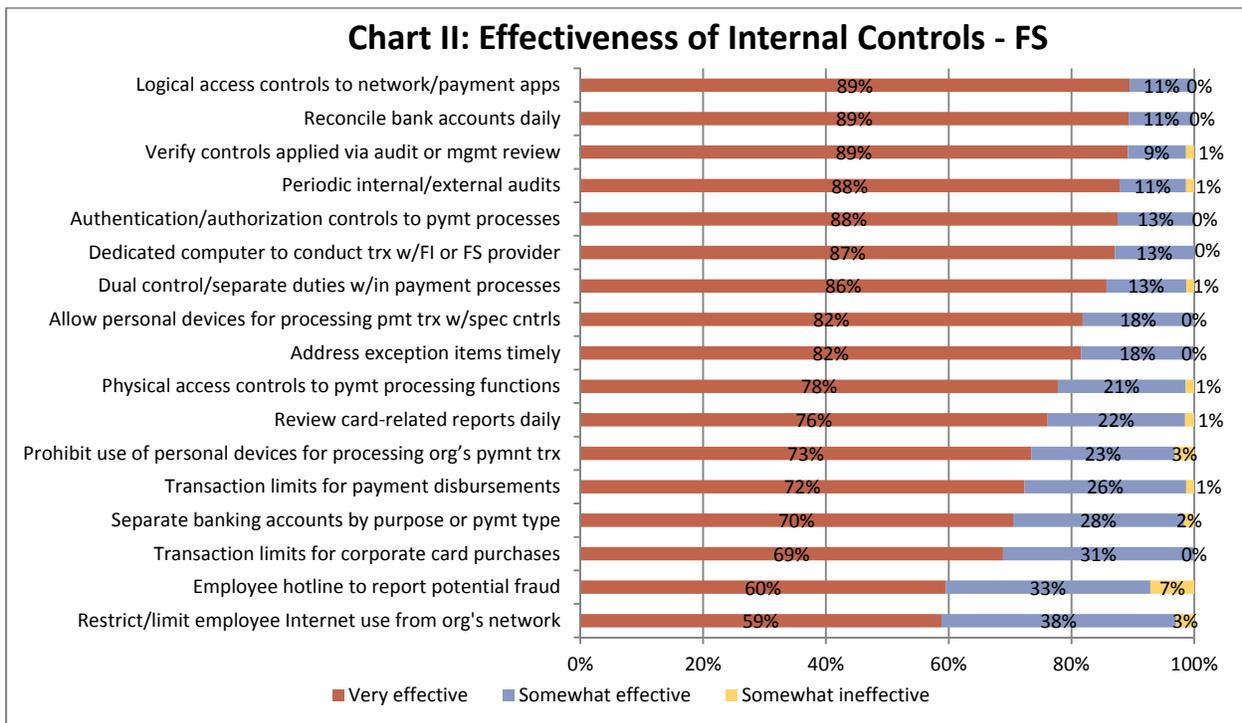
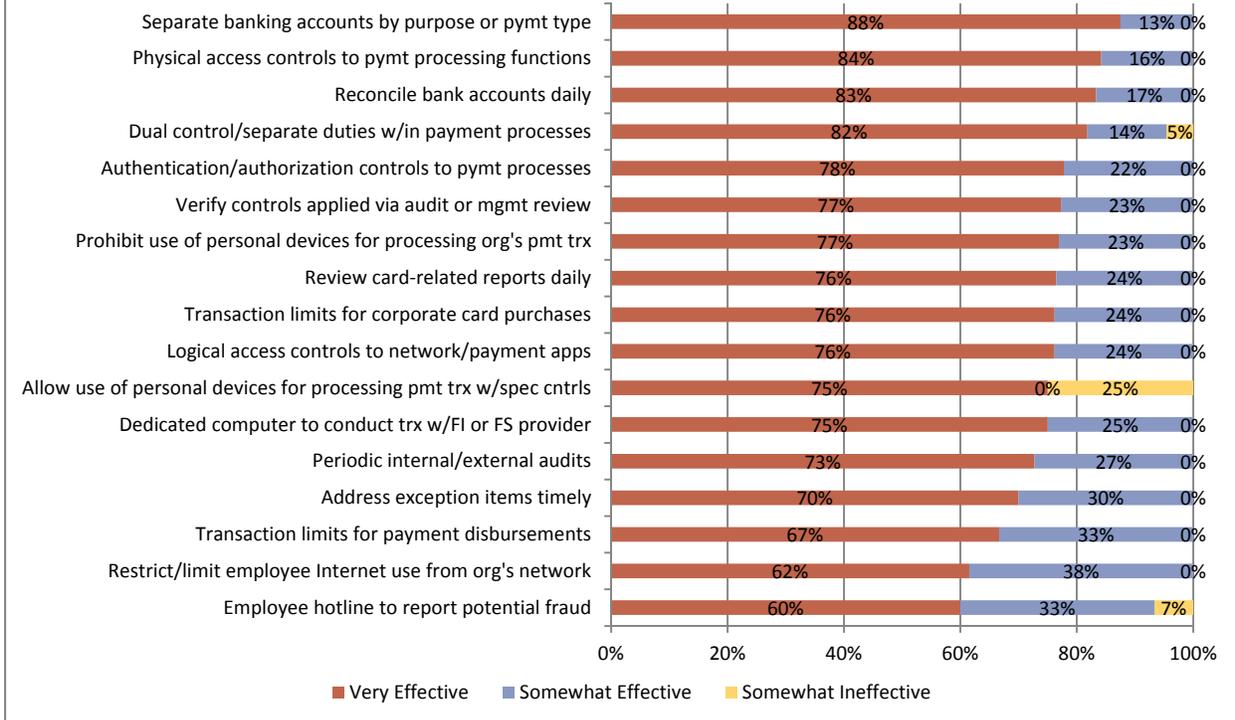
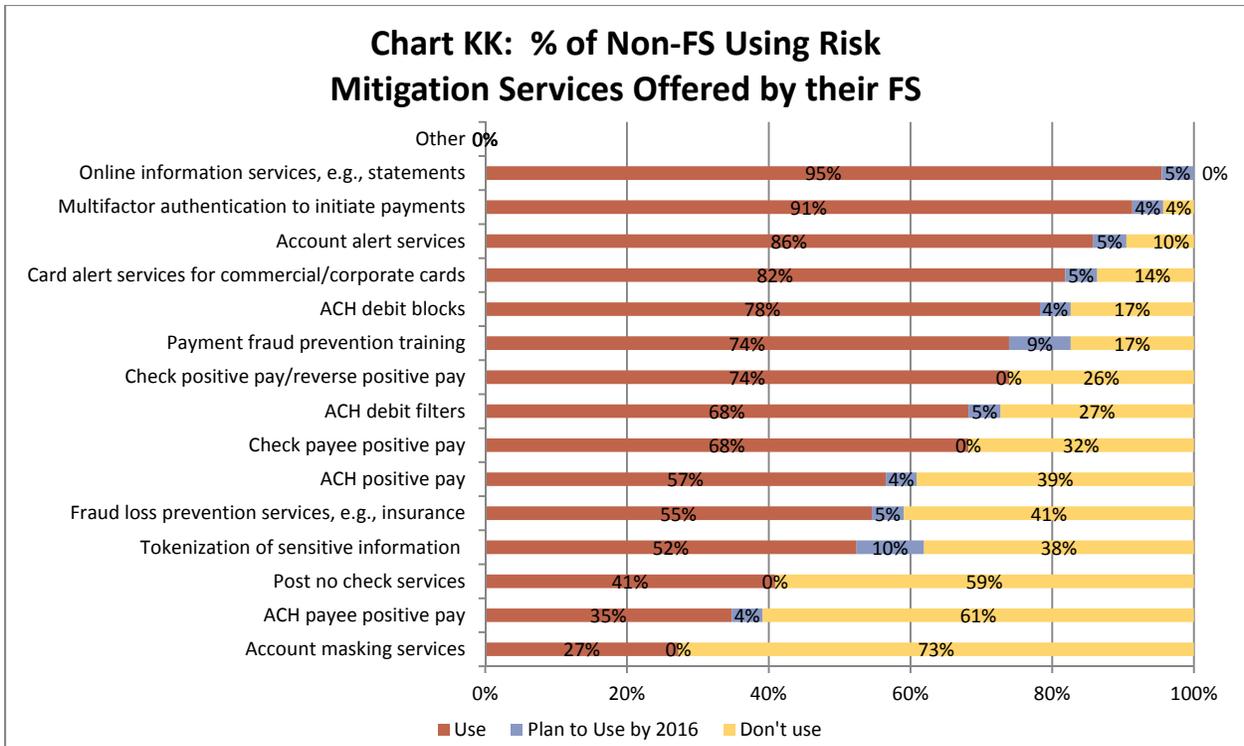


Chart JJ: Effectiveness of Internal Controls - Non-FS

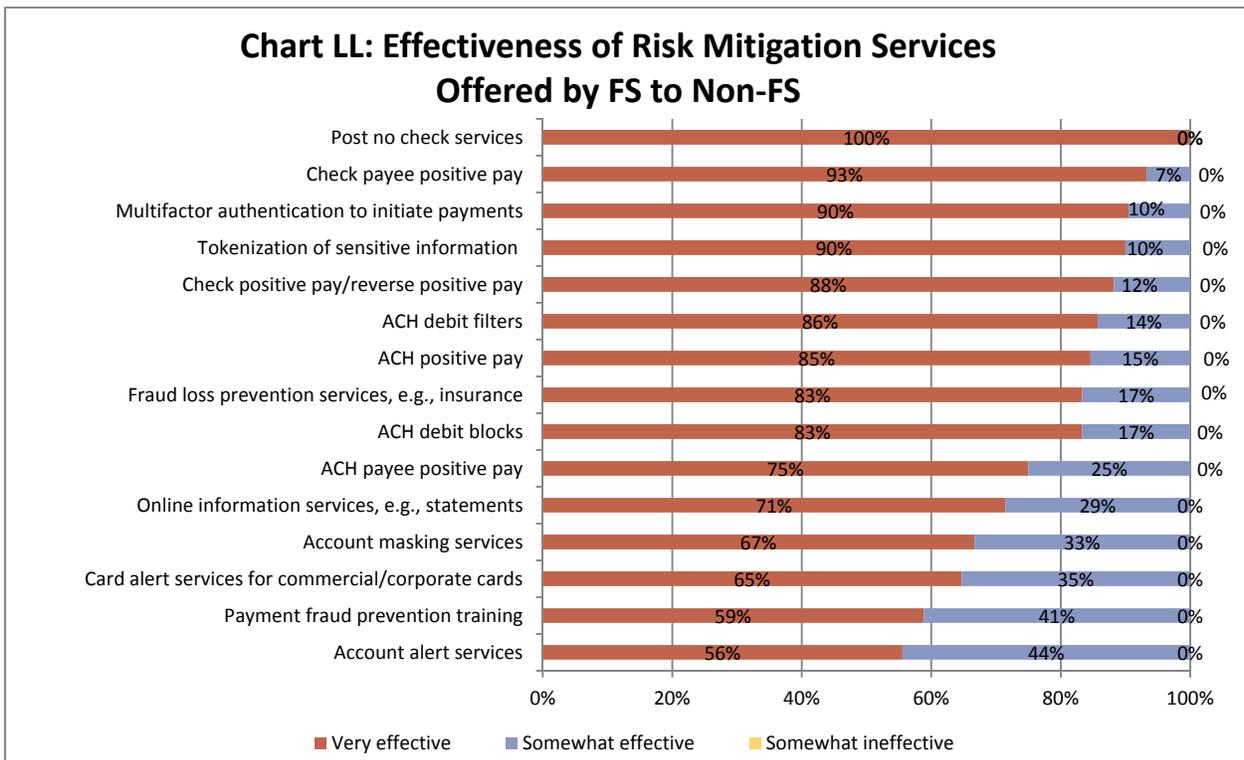


Risk Mitigation Services Offered by Financial Services Organizations

Nonfinancial institution respondents were asked to elaborate on the risk mitigation services offered to them by financial institutions and service providers. The results are shown in Chart KK. The top five services used are: online information services, multifactor authentication to initiate payments, account alert services, card alert services for commercial/corporate cards, and ACH debit blocks. When the overall results are compared with the 2012 survey, the percentage of nonfinancial firms using risk mitigation services is the same or higher in all categories, except account masking services, which shows 27 percent of the respondents using in 2014 compared to 51 percent in 2012.

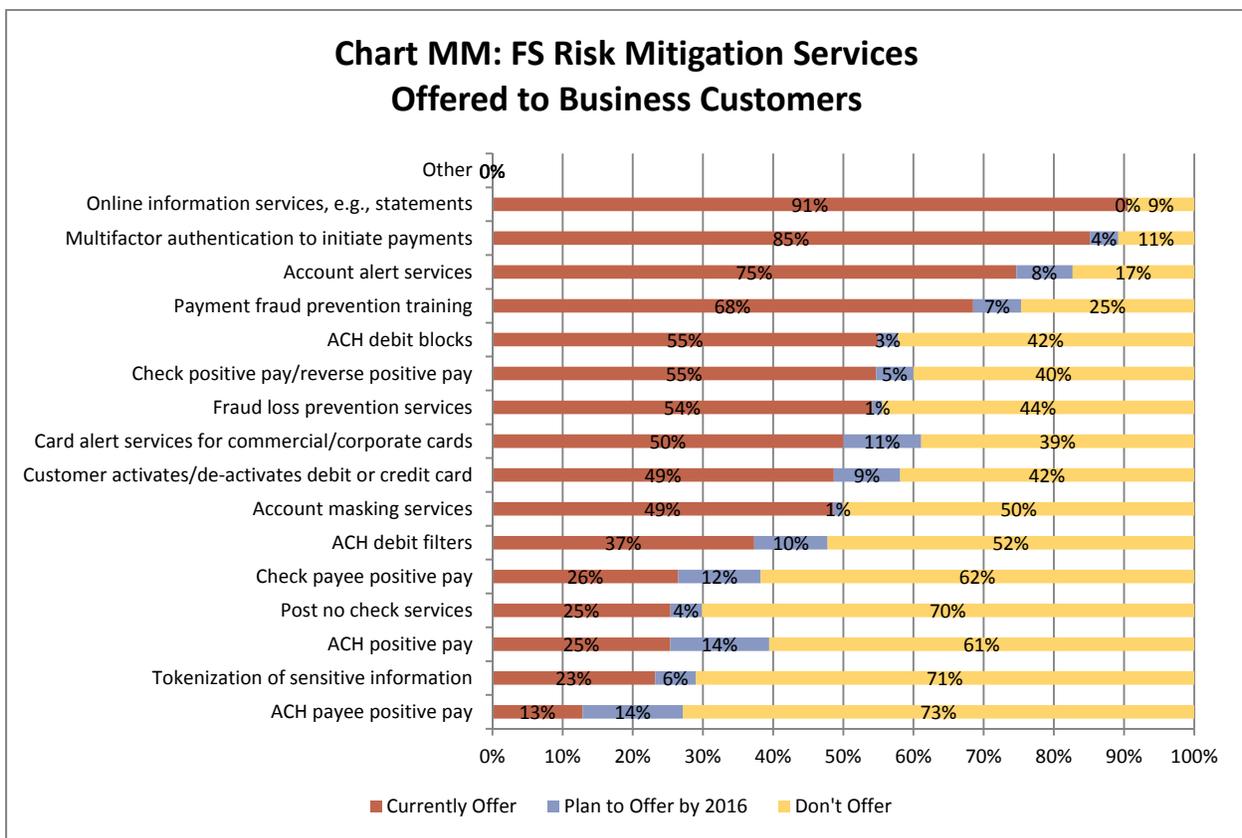


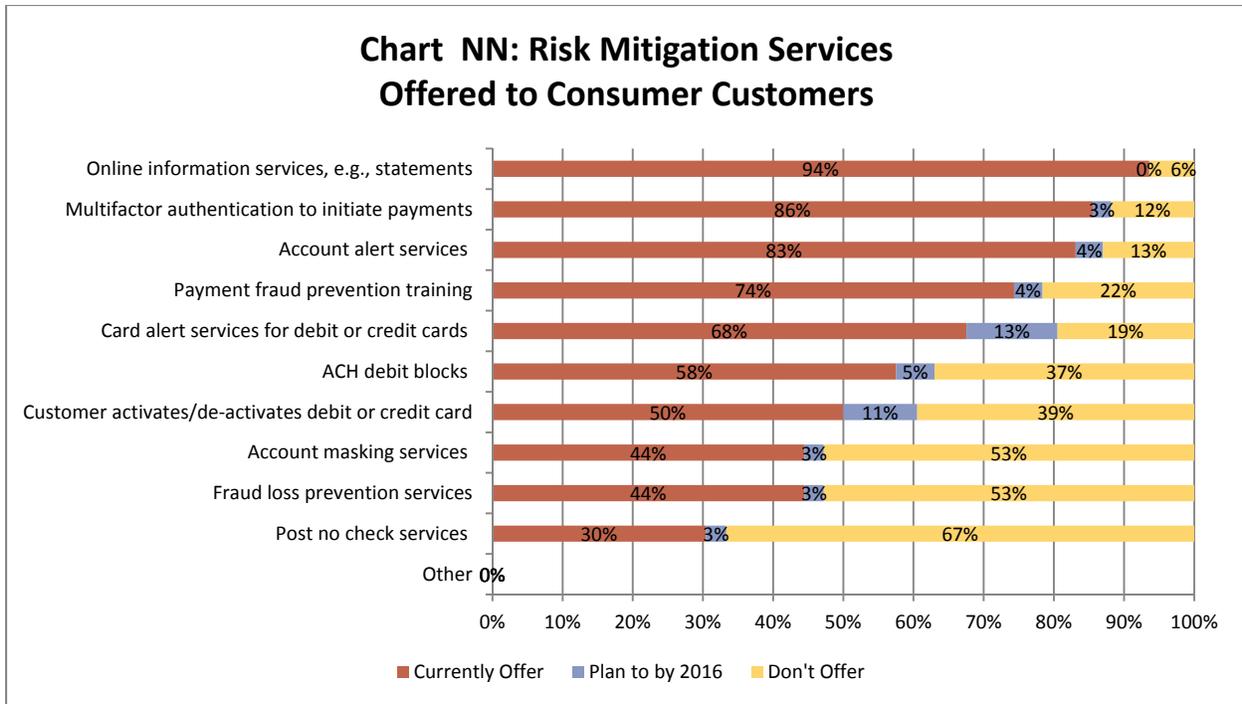
When asked to rate the effectiveness of these services, nonfinancial services respondents mostly rated them very effective, while none rated any services as somewhat ineffective, as shown in Chart LL.



For the first time, in 2014, this survey separated services that financial services respondents offer to business customers from those offered to consumers. The results are found in Charts MM and NN. Of the 10 offerings of financial services respondents to consumers, the results show very similar levels for nine of these offerings to business customers. One product showed a notable difference; card alert services for debit or credit cards are offered to consumers by 68 percent of respondents, but to business customers by only 50 percent of respondents. This difference in card alert service offerings may be a reflection of payment products offered and customers served as shown earlier in Chart E and Chart G.

In terms of future plans, more than 10 percent of financial service respondents plan to begin offering businesses alert services for corporate cards and a variety of positive pay services for check and ACH.





Financial services respondents were generally satisfied with the risk mitigation services they offer to both consumer and business customers and rated them mostly very effective.

Barriers to Reducing Payments Fraud

Fighting payments fraud is an ongoing battle. To ensure that current and new forms of payment are secure and reliable, firms must stay one step ahead of criminals who are exhibiting increasingly sophisticated ways of perpetrating fraud. This section of the report sheds light on the challenges to reducing payments fraud faced by both financial services organizations and nonfinancial firms.

Table 4 displays information about the barriers both groups experience in mitigating payments fraud, comparing the 2014 results with 2012 results. As in 2012, lack of staff resources continues to be the number one barrier for financial services organizations in 2014. While that was also the main barrier for nonfinancial organizations in 2012, the main barrier for this group in 2014 has shifted to corporate reluctance to share information due to competitive issues. Nearly one-third of financial services respondents saw cost of fraud detection tools (both commercial and in-house) as barriers in 2012. That number declined to nearly one-fourth that cited the cost of commercial fraud detection tools as a barrier in 2014, and 14 percent cited the cost of in-house fraud detection tools. The decline could be caused by an actual reduction in fraud mitigation costs, or perhaps the fear of payments fraud is driving risk mitigation acceptance, regardless of the cost. It is important to note that in 2012, there were only 10 nonfinancial organizations that responded to this question.

Table 4

Barriers to Reducing Fraud	2014			2012		
	FS (N=66)	Non-FS (N=17)	Total (N=83)	FS (N=80)	Non-FS (N=10)	Total (90)
Lack of staff resources	65%	35%	59%	64%	60%	63%
Consumer data privacy issues/concerns	50%	35%	47%	49%	30%	47%
Corporate reluctance to share information due to competitive issues	36%	47%	39%	23%	30%	23%
Lack of compelling business case (cost vs. benefit) to adopt new or change existing methods	38%	35%	37%	36%	40%	37%
Cost of implementing commercially available fraud detection tool/service	24%	6%	20%	33%	0%	29%
Unable to combine payment information for review due to operating w/multiple business areas, states or banks	20%	12%	18%	13%	30%	14%
Cost of implementing in-house fraud detection tool/service	14%	6%	12%	26%	0%	23%
Other	11%	6%	10%	10%	20%	11%

Opportunities to Reduce Payments Fraud

This section of the report looks at three types of opportunities to reduce payments fraud for both financial and nonfinancial services organizations: new or improved methods most needed, preferences for authentication methods and needed legal and regulatory changes.

New or Improved Methods Most Needed

Table 5 outlines the fraud mitigation methods respondents indicated were most needed to reduce payments fraud. In 2012, slightly more than half of the financial services respondents chose the replacement of card magnetic stripe with EMV chip technology, but in 2014 it was chosen by over 80 percent. In the nonfinancial services groups, on the other hand, 31 percent chose the shift to EMV chip technology in 2012, compared with 43 percent in 2014. The top “most needed improvements” to reduce payments fraud that were chosen by financial services respondents in 2014 were replacement of card magnetic stripe with EMV chip technology (81 percent), controls over internet payments (63 percent) and more aggressive law enforcement (62 percent). This compares with the nonfinancial services firms’ top choices of controls over mobile payments (48 percent), replacement of card/magnetic stripe with EMV chip technology,

industry-specific education on best practices for prevention and controls over internet payments (all at 43 percent). Tokenization¹² was added for the first time in 2014, and shows a difference of opinion between the two groups, 41 percent of financial services respondents and only 26 percent of nonfinancial respondents chose this as a most-needed method to reduce payments fraud.

Table 5

New/Improved Methods Most Needed	2014			2012		
	FS (N=79)	Non-FS (N=23)	Total (N=102)	FS (N=85)	Non-FS (N=13)	Total (N=98)
Replacement of card/magnetic strip with EMV chip technology	81%	43%	73%	57%	31%	53%
Controls over internet payments	63%	43%	59%	69%	31%	64%
More aggressive law enforcement	62%	39%	57%	51%	54%	51%
Controls over mobile initiated payments	51%	48%	50%	52%	39%	50%
Consumer education of fraud prevention	52%	35%	48%	58%	39%	55%
Information sharing on emerging fraud tactics being conducted by criminal rings	47%	39%	45%	54%	46%	53%
Tokenization of sensitive information	41%	26%	37%	na	na	na
Industry alert services	34%	22%	31%	27%	39%	29%
Industry specific education on best prevention practices for fraud	28%	43%	31%	28%	39%	30%
Image survivable check security features for business checks	18%	26%	20%	22%	23%	22%
Other	5%	17%	8%	5%	8%	5%

Authentication Methods

Table 6 details the authentication methods the respondents preferred using or may consider using to help reduce payments fraud. It is important to remember that the survey’s nonfinancial respondents do not primarily focus on consumer-facing payments but rather on

¹² 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.)

business-to-business payments and payments to both consumers and businesses. Financial services respondents provide payments to a variety of constituents.

A relatively high percentage of financial services respondents preferred chip and PIN requirements (84 percent) and chip for dynamic authentication (78 percent),¹³ while non-financial firms cited those options as the most preferred authentication methods at 58 percent and 32 percent respectively. Of interest is a shift in the top choice by nonfinancial firms, where 78 percent chose token authentication in 2012, but only 37 percent chose it in 2014.

Table 6

Authentication Method	2014			2012		
	FS (N=76)	Non-FS (N=19)	Total (N=95)	FS (N=83)	Non-FS (N=9)	Total (N=92)
Chip and PIN requirement	84%	58%	79%	52%	44%	51%
Chip for dynamic authentication	78%	32%	68%	45%	22%	42%
Multifactor authentication	55%	47%	54%	59%	44%	58%
Out-of-band/channel authentication to authorize payment	42%	26%	39%	49%	11%	46%
Physical token e.g., USB token or fob	38%	37%	38%	39%	78%	42%
Mobile device to authenticate person	41%	16%	36%	30%	33%	30%
PIN requirement	30%	32%	31%	36%	56%	38%
Biometrics	24%	16%	22%	21%	0%	18%
Other	1%	5%	2%	2%	11%	3%

Legal or Regulatory Changes

Finally, the survey asked respondents what types of legal and regulatory changes they believe might help reduce payments fraud. Generally, both groups agree that strengthening disincentives to commit fraud through stiffer penalties and more likely prosecution would help

¹³ “Chip” as used in these 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.

reduce payments fraud. They are also in close agreement on improving law enforcement cooperation on domestic and international payments fraud and fraud rings.

But there remains (as in the 2012 survey) a sharp disagreement on strategies that focus on shifting liability and responsibility for fraudulent card payments to the entity that initially accepts payment. Seventy-four percent of financial services respondents preferred this change, as opposed to 10 percent of nonfinancial respondents (see highlighted numbers in Table 7). This is not surprising because such changes would move the burden of paying for payments fraud away from financial intuitions. Currently, for most types of transactions, the primary financial responsibility for fraudulent transactions lies with the issuer or the financial institution. It is not surprising that more than 70 percent of the financial services respondents chose all three of the responsibility and liability shift changes as the most useful strategy for payments fraud. This shows a lack of support among financial institutions and issuers to continue to bear that responsibility or that they do not view it as an effective way to reduce payment fraud.

Table 7

Legal and Regulatory Changes	FS (%)	Non-FS (%)	Total (%)
Strengthen disincentives to committing fraud through stiffer penalties and more likely prosecution	72%	62%	70%
Place more responsibility on consumers and customers to reconcile and protect their payment data	71%	48%	66%
Assign liability for fraud losses to the party most responsible for not acting to reduce the risk of payment fraud	71%	33%	63%
Place responsibility to mitigate fraud and shift liability for fraudulent card payments to the entity that initially accepts the card payment	74%	10%	61%
Improve law enforcement cooperation on domestic and international payments fraud and fraud rings	60%	52%	59%
Focus future legal or regulatory changes on data breaches to where breaches occur	51%	33%	47%
Align Regulation E and Regulation CC to reflect changes in check collection systems' use of check images and conversion of checks to ACH	46%	43%	45%
Establish new laws/regs or change existing ones to strengthen the management of payments fraud risk	37%	52%	40%
Assign responsibility for mitigating fraud risk to the party best positioned to take action against fraud	40%	29%	37%
Establish new laws/regulations to require data sharing to strengthen the management of payments fraud risk	31%	19%	28%
Other	4%	14%	6%

Conclusions

- Both financial services organizations and nonfinancial corporations continue to be concerned about payments fraud.
- Eighty-six percent of financial services respondents had payment fraud attempts in 2013 and 63 percent of nonfinancial services respondents had attempts. Similar to the 2012 survey, nonfinancial firms cite checks and credit cards as the payment types with the highest number of fraud attempts, and financial services respondents cite signature debit, checks, and PIN debit.
- When it comes to payment fraud losses, 12 percent of the financial services respondents reported no fraud losses in 2014 compared with about 3 percent reporting no fraud losses in 2012. The opposite is true for nonfinancial respondents, 62 percent of which reported no losses in 2014, but about 78 percent reported no losses in 2012.
- Financial services respondents cited counterfeit or stolen cards used at point-of-sale (POS) or online as the most common form of payments fraud. Nonfinancial services respondents cited altered or forged checks, counterfeit or stolen cards used at POS or online and counterfeit checks.
- This year's survey asked about fraud experiences in 2013, prior to the escalation of data breaches in 2014. So perhaps it should not be surprising that fewer respondents chose "use of fraudulent credentials or data" as one of the top three payments fraud schemes they experienced.
- While they have different experiences with fraud, most financial and nonfinancial services respondents report total fraud losses of less than .3 percent of their annual revenue, which indicates that, despite numerous attempts at payments fraud, financial- and non-financial institution respondents are generally succeeding at keeping their fraud losses relatively low.
- Nearly half of the financial services organizations cited the top information source used to commit fraud as "sensitive" information obtained from lost or stolen card, check, or other physical document or device while in the consumer's control; but a little over half of the nonfinancial services organizations cited that the information source was "unknown."
- The majority of financial services respondents indicated they use many methods to authenticate the customer, with PIN authentication and signature verification being used by 93 percent. Fifty percent indicated they plan to use chip-card authentication by 2016. Nonfinancial firms indicated a high usage of CID verification on a payment card (73 percent) and customer authentication for online transactions (70 percent), with only 16 percent indicating a plan to use chip-card authentication by 2016.
- About two-thirds of the financial service respondents cited lack of staff resources as the main barrier to reducing payments fraud, while a little under half of the nonfinancial services respondents chose corporate reluctance to share information due to competitive issues as the main barrier to reducing payments fraud.
- A little over 80 percent of the financial services respondents see the replacement of card and magnetic stripe with EMV chip technology as the fraud mitigation strategy

most needed to reduce payments fraud, and a little under half of the nonfinancial services respondents see controls over mobile payments as the most needed fraud mitigation method to reduce payments fraud.

- When asked about their authentication preferences, 84 percent of financial services respondents preferred chip and PIN requirements and 78 percent preferred chip for dynamic authentication; nonfinancial firms preferred these authentication methods at 58 percent and 32 percent respectively.
- Financial services and nonfinancial services respondents agree that strengthening disincentives to commit fraud through stiffer penalties and more likely prosecution, and improving law enforcement cooperation on domestic and international payments fraud and fraud rings, would help reduce payments fraud.
- A large percentage of financial services respondents believe that putting the responsibility and liability for payments fraud on financial institutions and card issuers is not an effective way to reduce fraud. Instead they view shifting the liability and responsibility for fraudulent card payments to the entity that initially accepts payment as a better way to reduce payment fraud. Only 10 percent of nonfinancial services respondents prefer this as an effective way to reduce payment fraud.

Payments Fraud Questionnaire 2014

The survey will be administered online. Question numbers will not show. Information in blue font represents logic in the survey tool and is not displayed. Bullet formatting – if bullet is a circle, then it represents a radio button and limits selection to one answer. If bullets are squares, this means the respondent may select more than one answer.

Introduction

Please complete this online survey to help us better understand new or continuing challenges that your organization faces with payments fraud as well as methods you use to reduce fraud risk.

Payments Fraud Survey Instructions

- Please try to answer all questions as best you can. If you are unsure, please provide your best estimate.
- The survey should take about 20 - 30 minutes to complete. To review the questions in advance of completing the 2014 survey; see <http://www.minneapolisfed.org/about/whatwedo/paymentsinformation.cfm>
- It is best if you do not exit the survey until all questions have been completed. If needed, to return to the survey use the “Save” button to review or modify a response. You may need to copy and save a new link to return to your survey, depending on how you received the survey invitation. The online survey tool will provide this link during the save process. To return to the survey, paste the new link into your browser. You will be directed to the first survey question. Click the “Next” button to view or modify your previous answers.
- Do not use the “Back” button on your browser to review your completed questions. The survey does not support this.
- Responses will be sent to the Federal Reserve Bank after the “Submit Survey” button on the last page has been clicked.

Confidentiality of Response

The information you are providing will be publicly shared as aggregate, summary-level data. Your organization's specific responses will be shared with a limited number of staff working on this payments fraud research project. Individuals on the project team are from the Federal Reserve Banks of Boston, Chicago, Dallas, Minneapolis and Richmond.

Thank you for taking this survey. Your input is appreciated.

Organization Profile:

1a. How do you classify your organization? (Please select one answer.) A response to this question is required. [List in alpha order.](#)

- Agriculture
- Brokers, underwriters and investment company
- Business services/Consulting
- Construction
- Educational services
- Energy
- Financial Institution or Service Provider [\(If selected, go to 1b.\)](#)
- Government
- Health services
- Hospitality/Travel
- Insurance company and pension funds
- Manufacturing
- Nonprofit
- Real estate/Rental/Leasing
- Retail trade
- Software/Technology
- Telecommunications
- Transportation/Warehousing
- Wholesale trade
- Other, please specify _____

[Ask 1b when organization selected Financial Institution or Service Provider.](#)

1b. Please select the type of financial services organization from the list below. A response to this question is required.

- Bank [respondents selecting Bank will be asked "FI" questions](#)
- Credit Union [respondents selecting Credit Union will be asked "FI" questions](#)
- Thrift [respondents selecting Thrift will be asked "FI" questions](#)
- Service Provider, e.g., payments processor [respondents selecting service provider will be asked select FI questions where indicated](#)

2. What is your ... [Only ask Q2 when answer to Q1 is financial institution \(Bank, Credit Union, Thrift\) and go to Q4 next.](#)

Financial institution name _____
 City/Town _____
 State [Provide drop down list of 50 states in alpha order, also include District of Columbia.](#)
 ZIP/Postal Code _____ [Limited to 5 digits](#)
 Main nine digit routing and transit number. (Please specify the head office number.)
 _____ - _____ - [Response must be numeric.](#)

3. What is your... [Skip Q3 when answer to Q1 is financial institution \(Bank, Credit Union, Thrift\).](#)

Company Name: _____
 City/Town: _____
 State [Provide drop down list of 50 states in alpha order, also include District of Columbia.](#)
 ZIP/Postal Code _____ [Limited to 5 digits](#)

4. What is...

Your name _____ (optional)

Your title _____ (optional)

If you would like a summary of the overall survey results sent to you directly, please provide your email address.

E-mail address _____ (optional)

5. What best describes the type of department you work in? (Select one.)

- Accounts payable or receivable
- Audit
- Compliance/Risk Management/ Fraud Management
- Finance
- Operations/Payments processing function
- Management over multiple departments
- Treasury
- Other, please specify _____

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

- Under \$10 million
- \$10 million to \$24.9 million
- \$25 million to \$49.9 million
- \$50 – 99.9 million
- \$100 – 249.9 million
- \$250 - 499.9 million
- \$500 - 999.9 million
- \$1 – 4.9 billion
- \$5 – 9.9 billion
- \$10 billion or more
- Not applicable

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.) [Only ask Q7 when answer to Q1 is financial institution \(Bank, Credit Union, or Thrift\).](#)

- Under \$50 million
- \$50 – 99.9 million
- \$100 – 249.9 million
- \$250 - 499.9 million
- \$500 - 999.9 million
- \$1 – 4.9 billion
- \$5 – 9.9 billion
- \$10 billion or more

8. Are you or your organization a member of a trade association that provides education on payments and/or payments risk? (Select all that apply.)

- American Bankers Association (ABA)
- Association for Financial Professionals (AFP)
- Credit Union National Association (CUNA)
- Independent Community Bankers of America (ICBA)
- NACHA The Electronic Payments Association
- National Association of Federal Credit Unions (NAFCU)
- Regional payments association (e.g., NEACH,SFE, SWACHA, WACHA,UMACHA, etc.)
- State banking association
- State AFP or treasury management association
- Other, please specify _____
- None

Ask 8a when respondent selected “regional payments association in Q8

8a. Please select the regional payments association to which you are a member. (Select all that apply.)

- ALACHA
- EPCOR
- EastPay
- GACHA
- MACHA
- NEACH
- SFE
- SOCACHA
- SWACHA
- TACHA
- The Payments Authority
- UMACHA
- WACHA
- WesPay
- Other, please specify _____

9. In terms of your organization’s payments volume, who are the typical counterparties? Note: Businesses includes government entities. Skip Q9 when answer to Q1 is [financial institution \(Bank, Credit Union, or Thrift\)](#).

- Primarily payments to/from consumers
- Primarily payments to/from other businesses
- Payments to/from both consumers and businesses

10. What types of payments does your organization accept? [Skip Q10 when answer to Q1 is financial institution \(Bank, Credit Union, Thrift\).](#)

Payment Types	Payments Accepted/Received
Credit cards	<input type="checkbox"/>
Debit cards – PIN based	<input type="checkbox"/>
Debit cards – signature based	<input type="checkbox"/>
Prepaid cards, e.g., gift, payroll, etc.	<input type="checkbox"/>
Check instruments	<input type="checkbox"/>
Automated Clearinghouse (ACH) debits	<input type="checkbox"/>
Automated Clearinghouse (ACH) credits	<input type="checkbox"/>
Cash	<input type="checkbox"/>
Wire	<input type="checkbox"/>
Other, please specify _____	<input type="checkbox"/>

11. What types of payments does your organization use to disburse payments? [Skip Q11 when answer to Q1 is financial institution \(Bank, Credit Union, Thrift\).](#)

Payment Types	Payments Disbursed/Made
Credit cards	<input type="checkbox"/>
Debit cards – PIN based	<input type="checkbox"/>
Debit cards – signature based	<input type="checkbox"/>
Prepaid cards, e.g., gift, payroll, etc.	<input type="checkbox"/>
Check instruments	<input type="checkbox"/>
Automated Clearinghouse (ACH) debits	<input type="checkbox"/>
Automated Clearinghouse (ACH) credits	<input type="checkbox"/>
Cash	<input type="checkbox"/>
Wire	<input type="checkbox"/>
Other, please specify _____	<input type="checkbox"/>

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

[Only ask Q12 when answer to Q1 is financial institution \(Bank, Credit Union, Thrift\).](#)

- Primarily to consumers
- Primarily business or commercial clients
- Both consumers and business or commercial clients

13. Which of the following payments products does your financial institution offer? (Select all that apply.)
 Only ask Q13 when answer to Q1 is [financial institution](#) (Bank, Credit Union, Thrift).

Payment Products	Offer
Credit cards	<input type="checkbox"/>
Debit cards – PIN based	<input type="checkbox"/>
Debit cards – signature based	<input type="checkbox"/>
Prepaid cards, e.g., gift, payroll, etc.	<input type="checkbox"/>
Check instruments	<input type="checkbox"/>
Automated Clearinghouse (ACH) Origination	<input type="checkbox"/>
Wire transfer	<input type="checkbox"/>
Lockbox services	<input type="checkbox"/>
Cash	<input type="checkbox"/>
International payments	<input type="checkbox"/>

Payment Products	Offer an Online Service	Offer a Mobile Service
Bill payments	<input type="checkbox"/>	<input type="checkbox"/>
Person to person (P2P) payments	<input type="checkbox"/>	<input type="checkbox"/>
Consumer remote deposit capture	<input type="checkbox"/>	<input type="checkbox"/>
Commercial/Business remote deposit capture	<input type="checkbox"/>	<input type="checkbox"/>
Other payment products, please specify	<input type="checkbox"/>	<input type="checkbox"/>

Fraud by Payment Type:

14. Did your organization experience any payment fraud attempts in 2013? A response to this question is required.
- Yes [Go to Q15](#)
 - No [Go to Q16](#)
 - Don't know [Go to Q16](#)

2014 Payments Fraud Survey Results

15. 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.)

	1 st choice	2 nd choice	3 rd choice
Credit cards	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Debit cards – PIN based	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Debit cards – signature based	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Prepaid cards	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Check instruments	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Automated Clearinghouse (ACH) credits	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Automated Clearinghouse (ACH) debits	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cash	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Wire	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Everyone who is asked Q15 should also get asked Q16.

16. For these payment types, which is a greater expense for your organization– fraud prevention costs or actual dollar losses? (Choose one response per row.)

Payment Product	Fraud prevention costs	Actual fraud dollar losses	Don't use/offer payment type
Credit cards	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Debit cards – PIN based	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Debit cards – signature based	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Prepaid cards	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Check instruments	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Automated Clearinghouse (ACH)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mobile payment products	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cash	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Wire	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

17. For mobile payment products, which is a greater expense for your organization– fraud prevention costs or actual fraud dollar losses? (Choose one response per row.) Only ask Q17 when respondent selected “fraud prevention costs” or “actual fraud dollar losses” for Mobile payments row in Q16.

Payment Product	Fraud prevention costs	Actual fraud dollar losses	Don't use/offer as a mobile payment service
Bill payments	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Person to person (P2P) payments	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Consumer remote deposit capture	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Commercial/Business remote deposit capture	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other payment products, please specify _____	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2014 Payments Fraud Survey Results

18. Did your organization experience any payment fraud losses in 2013? A response to this question is required.

- Yes [Go to Q19](#)
- No [Go to Q22](#)
- Don't know [Go to Q27](#)

19. 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.)

	1 st choice	2 nd choice	3 rd choice
Credit cards	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Debit cards – PIN based	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Debit cards – signature based	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Prepaid cards	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Check instruments	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Automated Clearinghouse (ACH) credits	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Automated Clearinghouse (ACH) debits	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cash	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Wire	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

20a. Please indicate which payment type has the highest loss rate based on the volume of transactions for that payment type.

- Credit cards
- Debit cards – PIN based
- Debit cards – signature based
- Prepaid cards, e.g., gift, payroll, etc.
- Check instruments
- Automated Clearinghouse (ACH) debits
- Automated Clearinghouse (ACH) credits
- Cash
- Wire
- Other, please specify _____

20b. Please indicate which payment type has the highest loss rate based on the value of transactions for that payment type.

- Credit cards
- Debit cards – PIN based
- Debit cards – signature based
- Prepaid cards, e.g., gift, payroll, etc.
- Check instruments
- Automated Clearinghouse (ACH) debits
- Automated Clearinghouse (ACH) credits
- Cash
- Wire
- Other, please specify _____

21. For your organization, please estimate the financial losses experienced due to payments fraud during 2013 as a percent of the company's total revenue.
- less than .3%
 - .3% - .5%
 - .6% - 1.0%
 - 1.1% - 5.0%
 - over 5%
22. For your organization, how has the percentage of financial losses due to payments fraud changed in 2013 compared to 2012? A response to this question is required.
- Increased very substantially (more than 10%)
 - Increased substantially (5% to 10%)
 - Increased somewhat (1% to 5%)
 - Stayed the same
 - Decreased somewhat (-1% to -5%)
 - Decreased substantially (-5% to -10%)
 - Decreased very substantially (-10% or more)
 - Don't know

[ASK Q23 if answer is "increased" in Q 22](#)

23. To which payment types do you attribute the 2013 increase in your organization's actual dollar losses? (Select all that apply.) ([go to Q 27](#))
- Credit cards
 - Debit cards – PIN based
 - Debit cards – signature based
 - Prepaid cards
 - Check instruments
 - Automated Clearinghouse (ACH) credits
 - Automated Clearinghouse (ACH) debits
 - Cash
 - Wire

[ASK Q24 if answer is "decreased" in Q22](#)

24. To which payment types do you attribute the 2013 decrease in your organization's actual dollar losses? (Select all that apply.) ([go to Q25](#))
- Credit cards
 - Debit cards – PIN based
 - Debit cards – signature based
 - Prepaid cards
 - Check instruments
 - Automated Clearinghouse (ACH) credits
 - Automated Clearinghouse (ACH) debits
 - Cash
 - Wire

ASK Q25 if answer is “decreased” in Q22

25. Did your organization make changes to its payments risk management practices that led to the decrease in 2013 payments fraud losses? A response to this question is required. [If answer to Q25 is “no”, then skip Q26 and go to Q27.](#)

- Yes – [Go to Q26](#)
- No – [Go to Q27](#)
- Don’t know – [Go to Q28](#)

26. What are the key changes made by your organization that you think have contributed to the decrease in your organization’s payments fraud losses? (Select all that apply.) [\(go to Q28\)](#)

- Staff training and education
- Enhanced methods to authenticate customer and/or validate customer account
- Enhanced internal controls and procedures
- Adopted or increased use of risk management tools offered by our organization’s financial institution or financial service provider, e.g., account alerts, positive pay, etc.
- Enhanced fraud monitoring system [If selected, then also list:](#)
To which payments does enhanced monitoring apply? Select all that apply.
 - ACH transactions
 - Debit card transactions
 - Credit card transactions
 - Check transactions
 - Wire transactions
- Other, please describe _____

[ASK Q27 if answer is “increased” or “stayed the same” in Q22, Ask if answer is “no”/“DON’T KNOW to question 25.](#)

27. Did your organization make changes that helped to control your organization’s payments fraud losses? (Select all that apply.)

- Yes [\(go to Q27A\)](#)
- No [\(go to Q28\)](#)

27a. Which of the following changes did your organization make that helped to control your organization’s payments fraud losses? (Select all that apply.)

- Staff training and education
- Enhanced methods to authenticate customer and/or validate customer account
- Enhanced internal controls and procedures
- Adopted or increased use of risk management tools offered by our organization’s financial institution or financial service provider, e.g., account alerts, positive pay, etc.
- Enhanced fraud monitoring system [If selected, then also list:](#)
To which payments does enhanced monitoring apply? Select all that apply.
 - ACH transactions
 - Debit card transactions
 - Credit card transactions
 - Check transactions
 - Wire transactions
- Other, please describe _____

2014 Payments Fraud Survey Results

28. Did your organization experience any payment fraud attempts that were successful in 2013 (i.e., fraudster had financial gain)? . A response to this question is required.
- Yes ([go to Q29](#))
 - No ([go to Q30](#))
 - Don't know ([go to Q30](#))

29. For payment fraud that was successful, please estimate the percentage that involved: (Answers should total 100%. Please enter only numbers from 0 – 100, without a decimal point, % sign or space.) [An error message will be provided when response does not total 100%.](#)

Only internal staff from your own organization _____ %
 Internal staff collaborating with external parties _____ %
 Only external parties _____ %
 Unknown- could not determine _____ %

Common Fraud Schemes and Mitigation Strategies:

30. 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.) [SKIP Q30 when answer to Q1 is financial institution \(Bank, Credit Union, or Thrift\) or service provider.](#)

	1 st choice	2 nd choice	3 rd choice
Altered or forged checks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Counterfeit checks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Counterfeit currency	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Counterfeit or stolen cards (debit, credit, or prepaid) used at point-of-sale (POS)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Counterfeit or stolen cards (debit, credit, or prepaid) used online	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other Internet initiated payments, e.g., unauthorized ACH WEB transactions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fraudulent checks converted to ACH payments, e.g., point-of-purchase (POP), back office conversion (BOC), or account receivable conversion (ARC)/lockbox	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Telephone-initiated payments, e.g., unauthorized ACH TEL payment or remotely created checks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Wireless-initiated payments, e.g., payments initiated through mobile device (PDA, cell phone) or other contactless card	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cash register frauds, e.g., over or under-rings, checks or cash for deposit stolen by employee	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Use of fraudulent credentials or other data to establish new accounts or to defraud existing accounts, etc.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Customer service center fraud	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other, please specify _____	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2014 Payments Fraud Survey Results

31. 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.)

Only ask Q31 when answer to Q1 is [financial institution](#) (Bank, Credit Union, or Thrift) or [service provider](#).

	1 st choice	2 nd choice	3 rd choice
Altered or forged checks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Counterfeit checks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Duplicate checks presented	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Counterfeit currency	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Counterfeit or stolen cards (credit, debit, or prepaid) used at point-of-sale	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Counterfeit or stolen cards (credit, debit, or prepaid) used online	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other Internet initiated payments, e.g., unauthorized ACH WEB transactions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fraudulent checks converted to ACH payments, e.g., point-of-purchase (POP), back office conversion (BOC), or account receivable conversion (ARC)/lockbox	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Telephone-initiated payments, e.g., unauthorized ACH TEL payment or remotely created checks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Wireless-initiated payments, e.g., payments initiated through mobile device (PDA, cell phone) or other contactless card	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Use of fraudulent credentials or other data to establish new accounts or to defraud existing accounts, etc.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Account takeover of your customers' accounts due to breach of their security controls	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Use of power of attorney document for schemes against the elderly or vulnerable persons	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Customer service center fraud	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other, please specify _____	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2014 Payments Fraud Survey Results

32. 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.)

[Ask all this question](#)

	1 st choice	2 nd choice	3 rd choice
Altered or forged checks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Counterfeit checks drawn against your own accounts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Duplicate checks presented	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fraudulent or unauthorized ACH debits against your accounts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fraudulent or unauthorized card transactions against your corporate/commercial card accounts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Payment fraud due to breach of access or other data security controls to your organization's payment processes, e.g., account takeovers	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Check or electronic payment made by your organization due to internal fraud scheme	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Customer service center fraud	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Other, please specify _____	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

33. 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.) [Ask all this question](#)

	1 st choice	2 nd choice	3 rd choice
Information about customer obtained by family or friend	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
"Sensitive" information obtained from lost or stolen card, check, or other physical document, mobile phone or other device while in consumer's control	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Physical device tampering e.g., use of skimmer on POS terminal or ATM to obtain card magnetic stripe information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Email and webpage cyber-attacks e.g., phishing, spoofing, and pharming used to obtain "sensitive" customer information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lost or stolen physical documentation or electronic PC/device while in control of your organization	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data breach due to computer hacking, e.g., use of default or guessable credentials, brute force attacks, access through open ports or services, etc.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Organization's information obtained from a legitimate check issued by your organization	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Employee misuse, e.g., employee with legitimate access to organization or customer information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Social engineering used to obtain information used in the fraud scheme	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Information sources are unknown	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2014 Payments Fraud Survey Results

The next series of questions will ask about risk mitigation practices and are grouped by:

- Authentication methods
- Transaction screening and risk management approach
- Internal control and procedures
- Risk services offered by financial institutions/financial service providers

34. Which of the following authentication methods does your organization currently use or plan to use to mitigate payment risk? [Limit response to one per row in Q34](#)

	Currently use	Plan to use before 2016	Don't use
Verify customer state identification card is authentic (e.g., machine read magnetic stripe or 2-D bar code of driver's license or other state issued ID)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Positive identification of purchaser or valid account for in-store/in-person transactions, e.g., review picture ID	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Card security code located on back of payment card verified, e.g., CVV2, CVC2, or CID codes verified	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Signature verification	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Customer (consumer or business) authentication for online transactions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Biometrics (e.g., use of fingerprints, hand geometry, retina patterns, voice patterns, etc.) to authenticate the person	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Magnetic stripe authentication	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Card chip authentication	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PIN authentication	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Token (USB token or fob)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mobile device to authenticate person	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Out-of-band authentication (e.g., an online banking user is accessing their online bank account with a login and a one-time password is sent to their mobile phone via SMS that is entered into the online channel to identify them)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Multi-factor authentication	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Real-time decision support during account application or point of sale (e.g., score or alert on potential or known ID fraud or account takeover)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

34a. Are there any other authentication methods your organization currently uses to mitigate payments risk?

Other authentication methods , please specify _____

2014 Payments Fraud Survey Results

35. Please rate the effectiveness of authentication methods currently used by your organization. **Only allow a response to row in Q35 when Q34 answer in the same row is “currently use”.**

	Very effective	Some what effective	Some what ineffective
Verify customer state identification card is authentic (e.g., machine read magnetic stripe or 2-D bar code of driver’s license or other state issued ID)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Positive identification of purchaser or valid account for in-store/in-person transactions, e.g., review picture ID	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Card security code located on back of payment card verified, e.g., CVV2, CVC2, or CID codes verified	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Signature verification	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Customer (consumer or business) authentication for online transactions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Biometrics (e.g., use of fingerprints, hand geometry, retina patterns, voice patterns, etc.) to authenticate the person	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Magnetic stripe authentication	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Card chip authentication	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PIN authentication	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Token (USB token or fob)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mobile device to authenticate person	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Out-of-band authentication (e.g., an online banking user is accessing their online bank account with a login and a one-time password is sent to their mobile phone via SMS that is entered into the online channel to identify them)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Multi-factor authentication	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Real-time decision support during account application or point of sale (e.g., score or alert on potential or known ID fraud or account takeover)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2014 Payments Fraud Survey Results

36. Which of the following transaction screening and risk management methods does your organization currently use or plan to use to mitigate payment risk? [Limit response to one per row in Q36](#)

	Currently use	Plan to use before 2016	Don't use
Human review of payment transactions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fraud detection pen for currency	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Software that detects fraud through pattern matching, predictive analytics, anomaly detection or other indicators	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Centralized fraud-related information database for one payment type	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Centralized fraud-related information database for multiple payment types	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Participate in fraudster databases and receive alerts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Centralized risk management department	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provide customer education and training on payment fraud risk mitigation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provide staff education and training on payment fraud risk mitigation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Buy insurance coverage to minimize risk	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

36a. Are there any other transaction screening and risk management methods your organization currently uses to mitigate payments risk?

Other transaction screening and risk management methods, please specify _____

2014 Payments Fraud Survey Results

37. Please rate the effectiveness of the transaction screening and risk management methods currently used by your organization. **Only allow a response to row in Q37 when Q36 answer in the same row is “currently use”.**

	Very effective	Some what effective	Some what ineffective
Human review of payment transactions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fraud detection pen for currency	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Software that detects fraud through pattern matching, predictive analytics, anomaly detection or other indicators	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Centralized fraud-related information database for one payment type	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Centralized fraud-related information database for multiple payment types	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Participate in fraudster databases and receive alerts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Centralized risk management department	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provide customer education and training on payment fraud risk mitigation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Provide staff education and training on payment fraud risk mitigation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Buy insurance coverage to minimize risk	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2014 Payments Fraud Survey Results

38. Which of the following internal controls and procedures does your organization currently use or plan to use? **Limit response to one per row in Q38**

	Currently use	Plan to use before 2016	Don't use
Physical access controls to payment processing functions (e.g., controls that limit physical access to a place or resource such as restricted access or locked room where payment processes are performed, using a safe for storage of blank check stock, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Logical access controls to your computing network and payment processing applications (e.g., technical controls that enforce restrictions on who or what can access computing resources. Access is the ability to read, create, modify or delete records, files, execute a program, use an external connection, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Dedicated computer used to conduct transactions with financial institution or financial service provider (e.g., computer used only for payment processing and cannot be used for other purposes like ordering offices supplies, using email, web browsing, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Authentication and authorization controls to payment processes (authentication is proving that the users are who they claim to be and authorization is the permission to use a resource given by the application or system owner)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Restrict or limit employee use of Internet from organization's network	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Dual controls and segregation of duties within payment initiation and receipt processes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Transaction limits for payment disbursements	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Transaction limits for corporate card purchases	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Reconcile bank accounts daily	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Review card related reports daily	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Address exception items timely (e.g., meet deadlines for chargebacks, returning payments, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Separate banking accounts by purpose or by payment type	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Employee hotline to report potential fraud	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Verify application of controls via audit or management review	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Periodic internal/external audits	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Prohibit use of personal devices for processing of organization's payment transactions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Allow use of personal devices for processing of organization's payment transactions with specific controls, e.g., dollar limits, type of transaction, dual controls, etc.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

38a. Are there any other internal controls and procedures your organization currently uses to mitigate payments risk?

Other internal controls and procedures please specify _____

2014 Payments Fraud Survey Results

39. Please rate the effectiveness of the internal controls and procedures currently used by your organization.
 Only allow a response to row in Q39 when Q38 answer in the same row is “currently use”.

	Very effective	Some what effective	Some what ineffective
Physical access controls to payment processing functions (e.g., controls that limit physical access to a place or resource such as restricted access or locked room where payment processes are performed, using a safe for storage of blank check stock, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Logical access controls to your computing network and payment processing applications (e.g., technical controls that enforce restrictions on who or what can access computing resources. Access is the ability to read, create, modify or delete records, files, execute a program, use an external connection, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Dedicated computer used to conduct transactions with financial institution or financial service provider (e.g., computer used only for payment processing and cannot be used for other purposes like ordering offices supplies, using email, web browsing, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Authentication and authorization controls to payment processes (authentication is proving that the users are who they claim to be and authorization is the permission to use a resource given by the application or system owner)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Restrict or limit employee use of Internet from organization’s network	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Dual controls and segregation of duties within payment initiation and receipt processes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Transaction limits for payment disbursements	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Transaction limits for corporate card purchases	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Reconcile bank accounts daily	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Review card related reports daily	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Address exception items timely (e.g., meet deadlines for chargebacks, returning payments, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Separate banking accounts by purpose or by payment type	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Employee hotline to report potential fraud	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Verify application of controls via audit or management review	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Periodic internal/external audits	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Prohibit use of personal devices for processing of organization’s payment transactions	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Allow use of personal devices for processing of organization’s payment transactions with specific controls, e.g., dollar limits, type of transaction, dual controls, etc.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2014 Payments Fraud Survey Results

40. What risk mitigation services offered by your financial institution/service provider does your organization currently use or plan to use? Skip Q40-41 if answer to Q1 is [financial institution \(Bank, Credit Union, Thrift\)](#) or [service provider](#). For all other responses to Q1 ask Q40 and 41. Limit response to one per row in Q40.

	Currently use	Plan to use before 2016	Don't use
Check positive pay/reverse positive pay	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Check payee positive pay	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Post no check services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACH debit blocks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACH debit filters	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACH positive pay	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACH payee positive pay	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Account masking services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tokenization of sensitive information (e.g., cardholder primary account number is replaced with a randomized token that represents the cardholder data reducing transmission and storage of actual cardholder sensitive data)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Account alert services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Card alert services for commercial/corporate cards	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fraud loss prevention services e.g., insurance	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online information services, e.g., statements, check images	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Multi-factor authentication controls to initiate payments from bank account	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Payment fraud prevention training (e.g., classes, webinars, workshops, print or online materials, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

40a. Are there any other risk mitigation services your organization currently uses to mitigate payments risk?
 Other risk mitigation services, please specify _____

2014 Payments Fraud Survey Results

41. Please rate the effectiveness of risk mitigation services currently used by your organization. **Only allow a response to row in Q41 when Q40 answer in the same row is "currently use".**

	Very effective	Some what effective	Some what ineffective
Check positive pay/reverse positive pay	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Check payee positive pay	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Post no check services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACH debit blocks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACH debit filters	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACH positive pay	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACH payee positive pay	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Account masking services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tokenization of sensitive information (e.g., cardholder primary account number is replaced with a randomized token that represents the cardholder data reducing transmission and storage of actual cardholder sensitive data)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Account alert services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Card alert services for commercial/corporate cards	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fraud loss prevention services e.g., insurance	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online information services, e.g., statements, check images	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Multi-factor authentication controls to initiate payments from bank account	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Payment fraud prevention training (e.g., classes, webinars, workshops, print or online materials, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2014 Payments Fraud Survey Results

42. What risk mitigation services/products does your organization currently offer or plan to offer to your business customers? *Ask Q42 only when the answer to Q1 is financial institution (Bank, Credit Union, Thrift) or service provider. Selection is limited to one per row in Q42.*

	Currently Offer	Plan to Offer before 2016	Don't Offer
Check positive pay/reverse positive pay	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Check payee positive pay	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Post no check services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACH debit blocks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACH debit filters	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACH positive pay	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACH payee positive pay	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Account masking services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tokenization of sensitive information (e.g., cardholder primary account number is replaced with a randomized token that represents the cardholder data reducing transmission and storage of actual cardholder sensitive data)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Account alert services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Card alert services for commercial/corporate cards	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Customer activates/de-activates debit or credit card as needed for use or to block use	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fraud loss prevention services, e.g., insurance	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online information services, e.g., statements, check images	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Multi-factor authentication controls to initiate payments from bank account	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Payment fraud prevention training (e.g., classes, webinars, workshops, print or online materials, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

42a. Are there any other risk mitigation service/products your organization currently offers to your business customers?

Other risk mitigation service/products, please specify _____

2014 Payments Fraud Survey Results

43. Please rate the effectiveness of risk mitigation services currently offered by your organization to your business customers. Only allow a response to row in Q43 when Q42 answer in the same row is “currently offer”.

	Very effective	Some what effective	Some what ineffective
Check positive pay/reverse positive pay	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Check payee positive pay	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Post no check services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACH debit blocks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACH debit filters	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACH positive pay	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACH payee positive pay	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Account masking services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tokenization of sensitive information (e.g., cardholder primary account number is replaced with a randomized token that represents the cardholder data reducing transmission and storage of actual cardholder sensitive data)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Account alert services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Card alert services for commercial/corporate cards	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Customer activates/de-activates debit or credit card as needed for use or to block use	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fraud loss prevention services, e.g., insurance	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online information services, e.g., statements, check images	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Multi-factor authentication controls to initiate payments from bank account	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Payment fraud prevention training (e.g., classes, webinars, workshops, print or online materials, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

2014 Payments Fraud Survey Results

44. What risk mitigation services/products does your organization currently offer or plan to offer to your consumer customers? **Ask Q44 only when the answer to Q1 is financial institution (Bank, Credit Union, Thrift) or service provider. Selection is limited to one per row in Q44.**

	Currently Offer	Plan to Offer before 2016	Don't Offer
Post no check services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACH debit blocks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Account masking services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Account alert services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Card alert services for debit or credit cards	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Customer activates/de-activates debit or credit card as needed for use or to block use	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fraud loss prevention services, e.g., insurance	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online information services, e.g., statements, check images	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Multi-factor authentication controls to initiate payments from bank account	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Payment fraud prevention training (e.g., classes, webinars, workshops, print or online materials, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

44a. Are there any other risk mitigation service/products your organization currently offers to your consumer customers?

Other risk mitigation service/products, please specify _____

45. Please rate the effectiveness of risk mitigation services currently offered by your organization to your consumer customers. **Only allow a response to row in Q45 when Q44 answer in the same row is "currently offer".**

	Very effective	Some what effective	Some what ineffective
Post no check services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACH debit blocks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Account masking services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Account alert services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Card alert services for debit or credit cards	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Customer activates/de-activates debit or credit card as needed for use or to block use	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fraud loss prevention services, e.g., insurance	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online information services, e.g., statements, check images	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Multi-factor authentication controls to initiate payments from bank account	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Payment fraud prevention training (e.g., classes, webinars, workshops, print or online materials, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

46. From your organization's perspective, what new or improved methods are most needed to reduce payments fraud? (Select those you think would be most helpful.)
- Authentication controls over Internet initiated payments
 - Authentication controls over mobile device initiated payments
 - Replacement of card magnetic stripe with EMV chip technology
 - Tokenization of sensitive information, e.g., cardholder primary account number is replaced with a randomized token that represents the cardholder data reducing transmission and storage of actual cardholder data
 - Improved methods for information sharing on emerging fraud tactics, e.g., those being conducted by criminal rings
 - More aggressive law enforcement
 - Image survivable check security features for business checks
 - Industry alert services
 - Industry specific education on payments fraud prevention best practices
 - Consumer education of fraud prevention
 - Other, please specify _____
47. What authentication methods would your organization prefer or consider adopting to help reduce payments fraud? (Select all methods your organization would most likely prefer or consider for adoption.)
- Biometrics
 - EMV chip and signature requirement
 - EMV chip and PIN requirement
 - PIN requirement
 - Physical token (USB token or fob)
 - Mobile device to authenticate person
 - Out-of-band authentication
 - Multi-factor authentication
 - Other, please specify _____
48. What are the main barriers to mitigate payments fraud that your organization experiences? (Select all that you consider to be the main barriers.)
- Consumer data privacy regulatory restrictions/other concerns if customer data shared with others to help mitigate fraud
 - Corporate reluctance to share information due to competitive issues
 - Cost of implementing in-house fraud detection tool/method [If selected ask:](#)
Please describe what tool/method your organization wants to implement, but cannot afford to do so

 - Cost of implementing commercially available fraud detection tool/service [If selected ask:](#)
Please describe what tool/service your organization wants to implement, but cannot afford to do so

 - Lack of compelling business case (cost vs. benefit) to adopt new or change existing methods
 - Lack of staff resources
 - Unable to combine payment information for review due to payments operations performed in multiple business areas, multiple states, with multiple banks, etc.
 - Corporate reluctance to share information due to competitive issues
 - Other, please specify _____

49. Please indicate what types of legal or regulatory changes you think would help reduce payments fraud. (Select all that apply.)

- Establish new laws/regulations or change existing ones in order to strengthen the management of payments fraud risk
- Establish new laws/regulations to require data sharing to strengthen the management of payments fraud risk
- Strengthen disincentives to committing fraud through more likely prosecution and increased penalties for fraud and attempted fraud
- Improve law enforcement cooperation on domestic and international payments fraud and fraud rings
- Assign responsibility for mitigating fraud risk to the party best positioned to take action against fraud
- Assign liability for fraud losses to the party most responsible for not acting to reduce the risk of payment fraud
- Place more responsibility on consumers and customers to reconcile and protect their payments data
- Place responsibility to mitigate fraud and shift liability for fraudulent card payments to the entity that initially accepts the card payment
- Focus future legal or regulatory changes on data breaches to where the breaches occur
- Align Regulation E and Regulation CC to reflect changes in check collection systems' use of check images and conversion of checks to ACH transactions
- Other, please specify _____

50. Is there anything else that you would like to share as part of this survey? _____

Thank you for taking the time to complete our survey. Your responses are greatly appreciated to help provide feedback about best practices and challenges for the payments industry.