2012 Payments Fraud Survey
Summary of Results

Federal Reserve Bank of Dallas
FIRM—Financial Institution Relationship Management

August 30, 2012

1. Introduction

In April 2012, the Federal Reserve Bank of Dallas' FIRM—Financial Institution Relationship Management Department conducted research on payments-related fraud experienced by organizations in the Dallas Fed District.[1] We asked our financial institution constituents to respond to an online survey about their experiences with payments fraud and the methods they use to reduce fraud risk. In addition, the survey audience was expanded with the help of the following organizations, which sent invitations to complete the survey directly to their members: SWACHA—The Electronic Payments Resource; the Dallas Association for Financial Professionals (AFP), Fort Worth AFP, Austin AFP, Houston Treasury Management Association (TMA) and San Antonio TMA. We thank those organizations for their help in obtaining responses.

The survey covered transactions made using cash, check, debit and credit cards, automated clearinghouse (ACH), and wire transfers.

This survey effort was part of a broader initiative conducted in conjunction with the Federal Reserve Banks of Minneapolis, Boston and Richmond, as well as the Independent Community Bankers of America. We plan to repeat this survey biannually in the years ahead, which will allow us to analyze trend data on payments fraud in the district over multiple years.

2. Respondent Information

There were a total of 139 respondents to the survey based in the Dallas Fed District, 120 (86%) in the financial services industry, almost all of which are financial institutions (FIs),[2] and 19 (14%) non-financial services organizations. The remaining non-financial institution respondents classified their organizations in one of 19 industry categories, as shown in Chart A.

Respondents are also categorized by their organizations' annual revenues, shown in Chart B. Just over half of the organizations have annual revenues of less than $50 million. Chart C shows, for financial institution respondents only, the number of respondents in each of various asset-size groups. About 80% of respondents were from organizations with less than $1 billion in assets.

[1] Questions about the survey should be directed to Matt Davies, AAP, CTP, Director of Payments Outreach, Federal Reserve Bank of Dallas, at matt.davies@dal.frb.org or 214-922-5259.

[2] For the purposes of this survey, the term "financial institutions" includes both banks and credit unions.

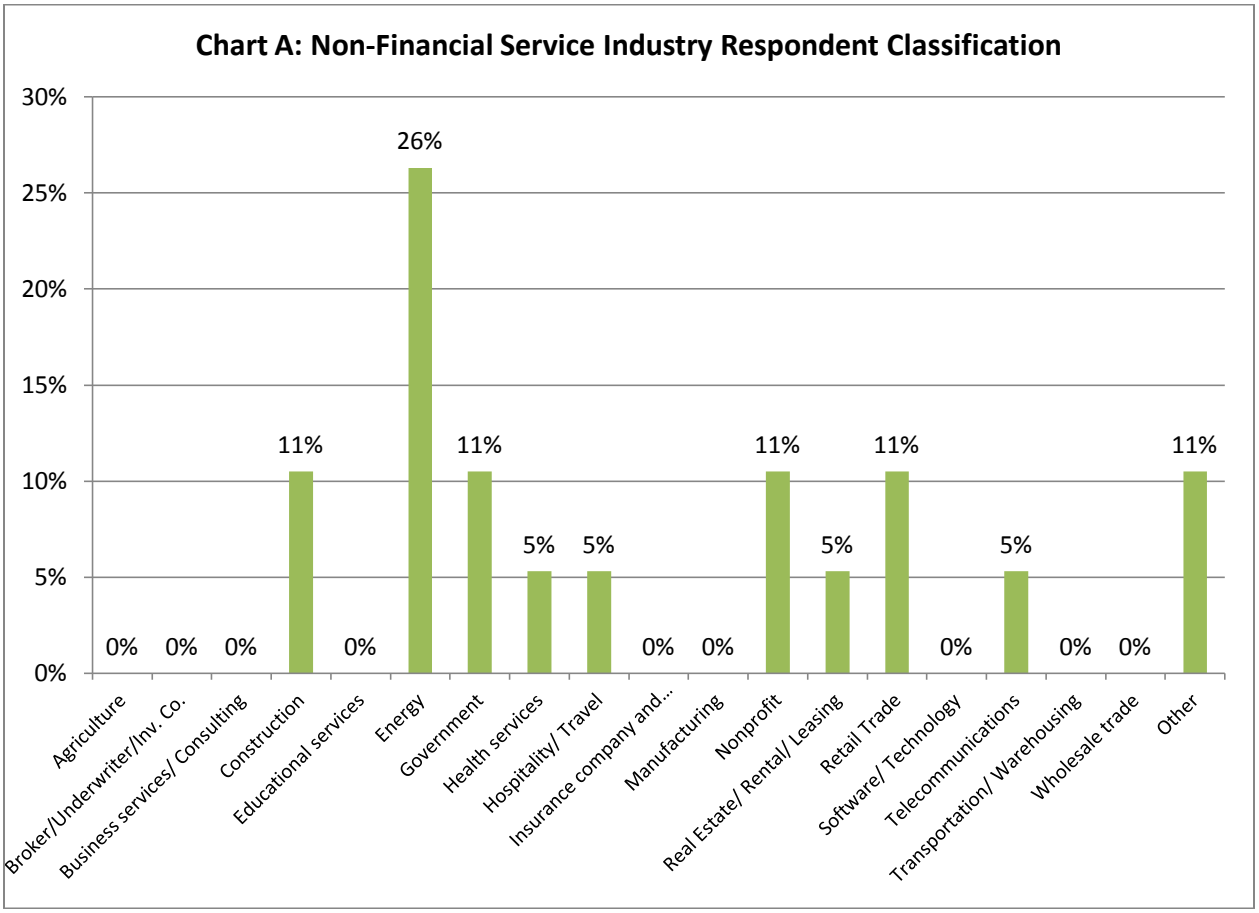


Chart A: Non-Financial Service Industry Respondent Classification
30%
25%
20%
15%
10%
5%
0%
0%
0%
0%
11%
0%
26%
11%
5%
5%
0%
0%
11%
5%
11%
0%
5%
0%
0%
11%
Agriculture
Broker/Underwriter/Inv. Co.
Business services/ Consulting
Construction
Educational services
Energy
Government
Health services
Hospitality/ Travel
Insurance company and...
Manufacturing
Nonprofit
Real Estate/ Rental/ Leasing
Retail Trade
Software/ Technology
Telecommunications
Transportation/ Warehousing
Wholesale trade
Other

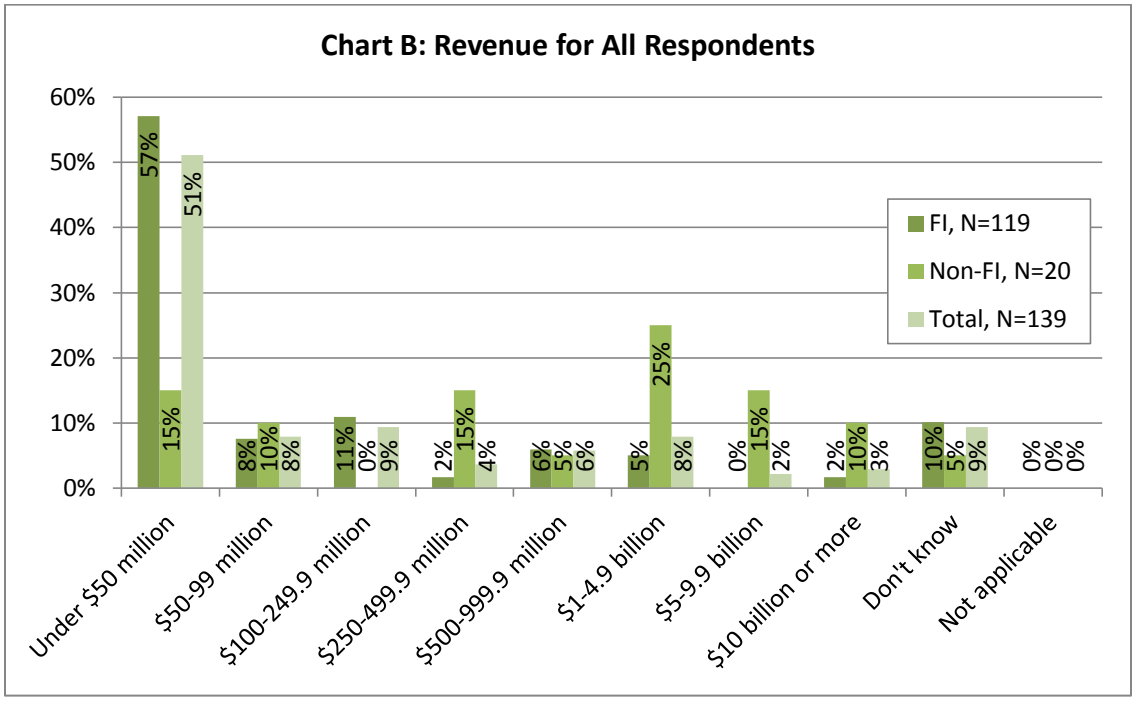
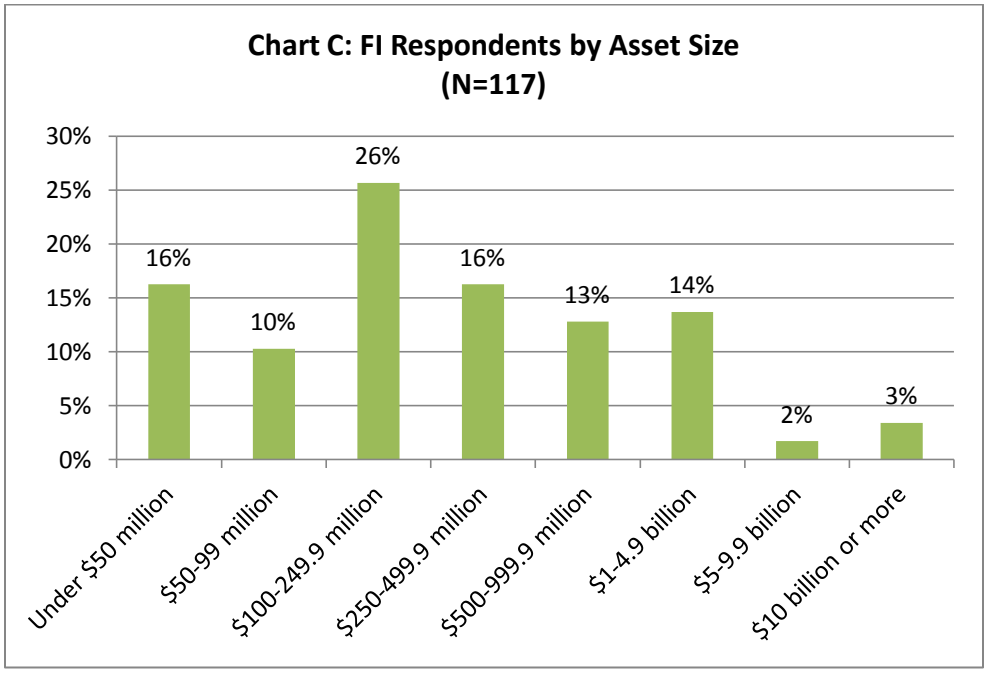


Chart B: Revenue for All Respondents
60%
50%
40%
30%
20%
10%
0%
57%
15%
51%
8%
10%
8%
11%
0%
9%
2%
15%
4%
6%
5%
6%
5%
25%
8%
0%
15%
2%
2%
10%
3%
10%
5%
9%
0%
0%
0%
FI, N=119
Non-FI, N=20
Total, N=139
Under $50 million
$50-99 million
$100-249.9 million
$250-499.9 million
$500-999.9 million
$1-4.9 billion
$5-9.9 billion
$10 billion or more
Don't know
Not applicable



3. Summary of Survey Results by Question

a. Payments Made and Payment Types Used by Respondent Organizations

Non-financial institution respondents were asked whether their organization's payments typically have as their counterparties consumers, other businesses (including government entities) or both. As can be seen in Chart D, respondents were split evenly between payments primarily to/from other businesses and payments to/from both consumers and businesses.

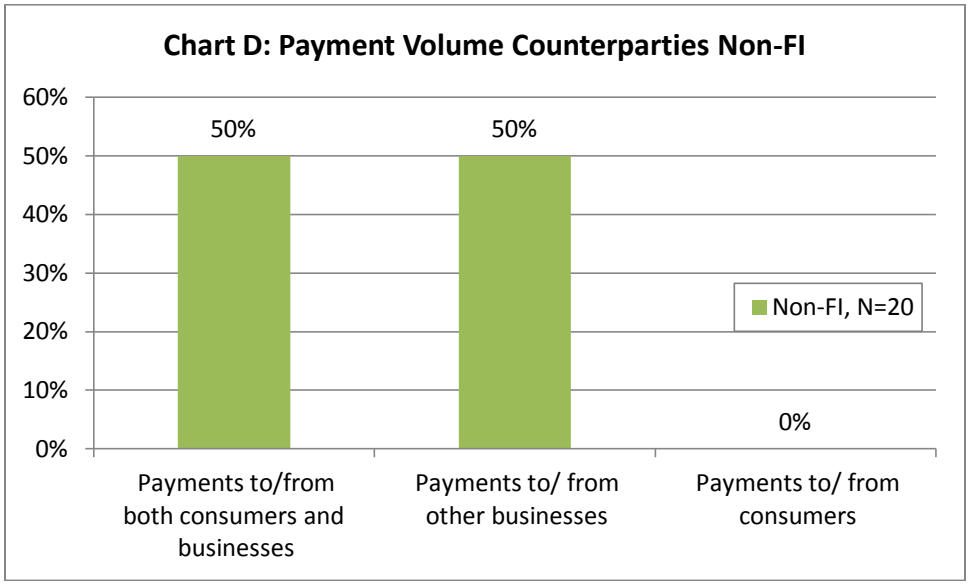
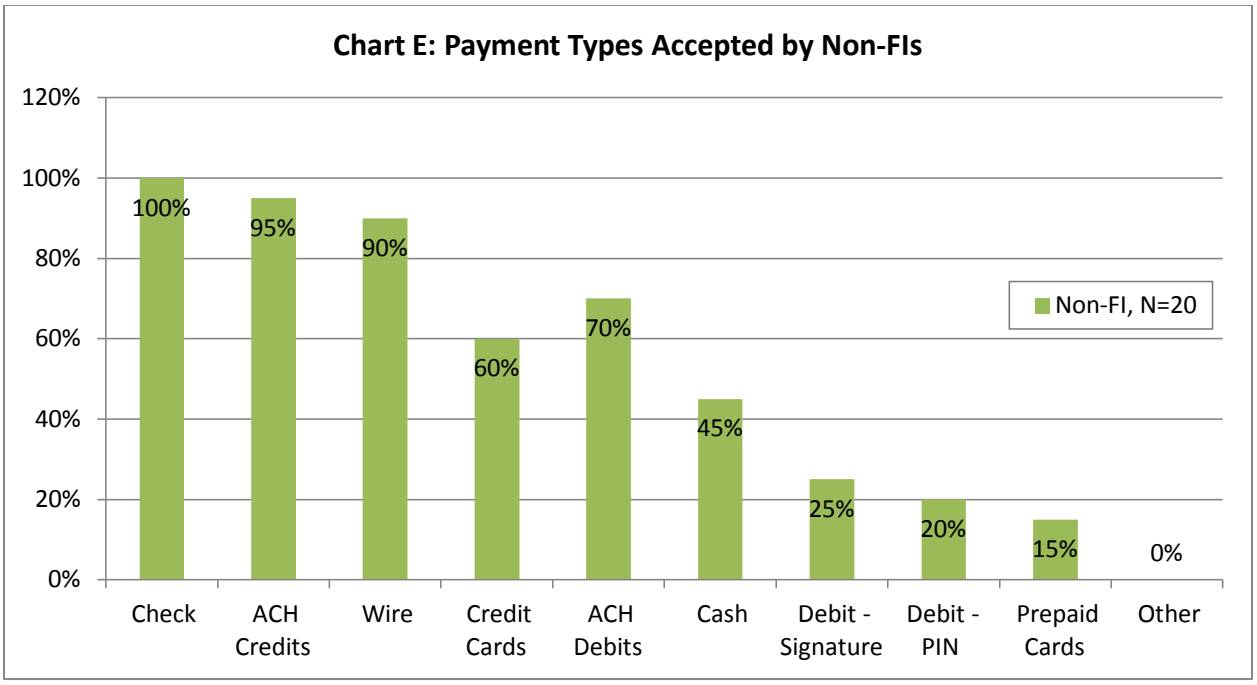
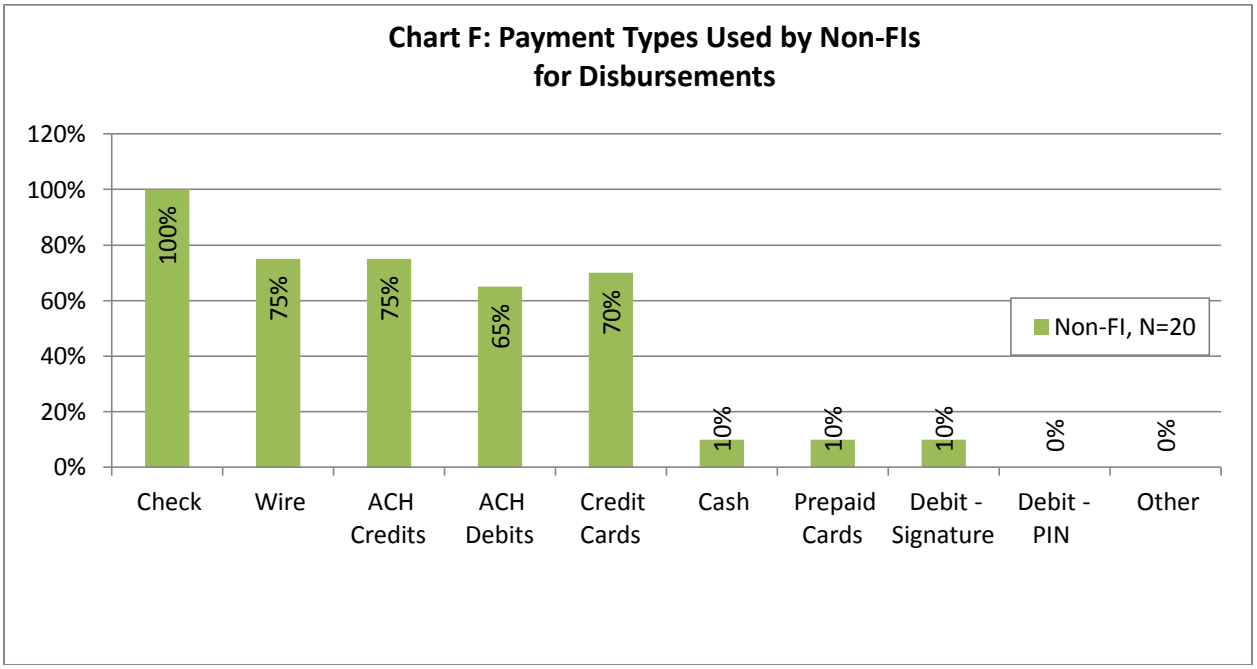


Chart E shows payment types accepted by non-financial institution respondents, while Chart F shows payment types used for disbursements by the same subset of respondents.





Financial institution respondents were asked to indicate whether their customer base is composed primarily of consumers, commercial clients or both. As can be seen in Chart G, nearly three-fourths of financial institution respondents offer services to both consumer and commercial customers.

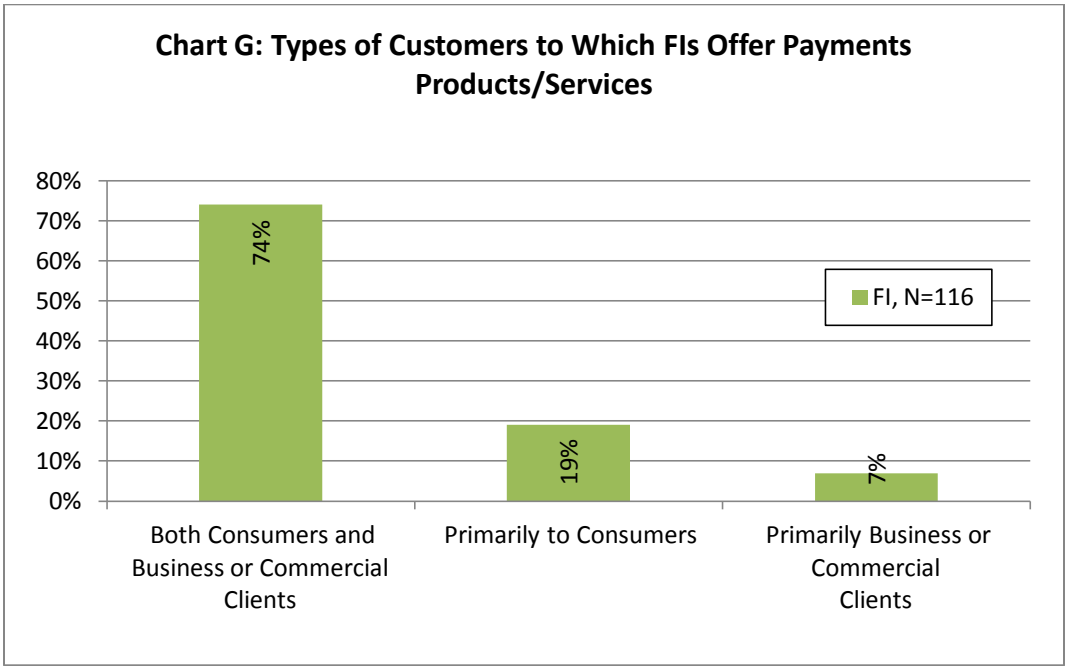
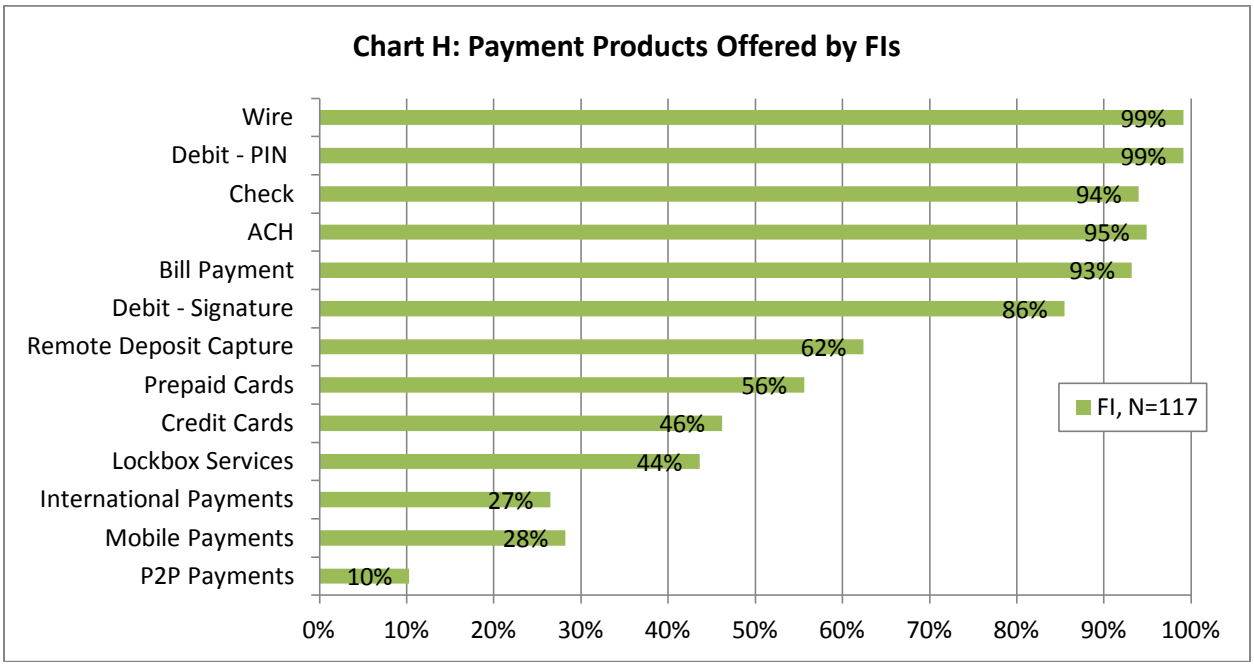


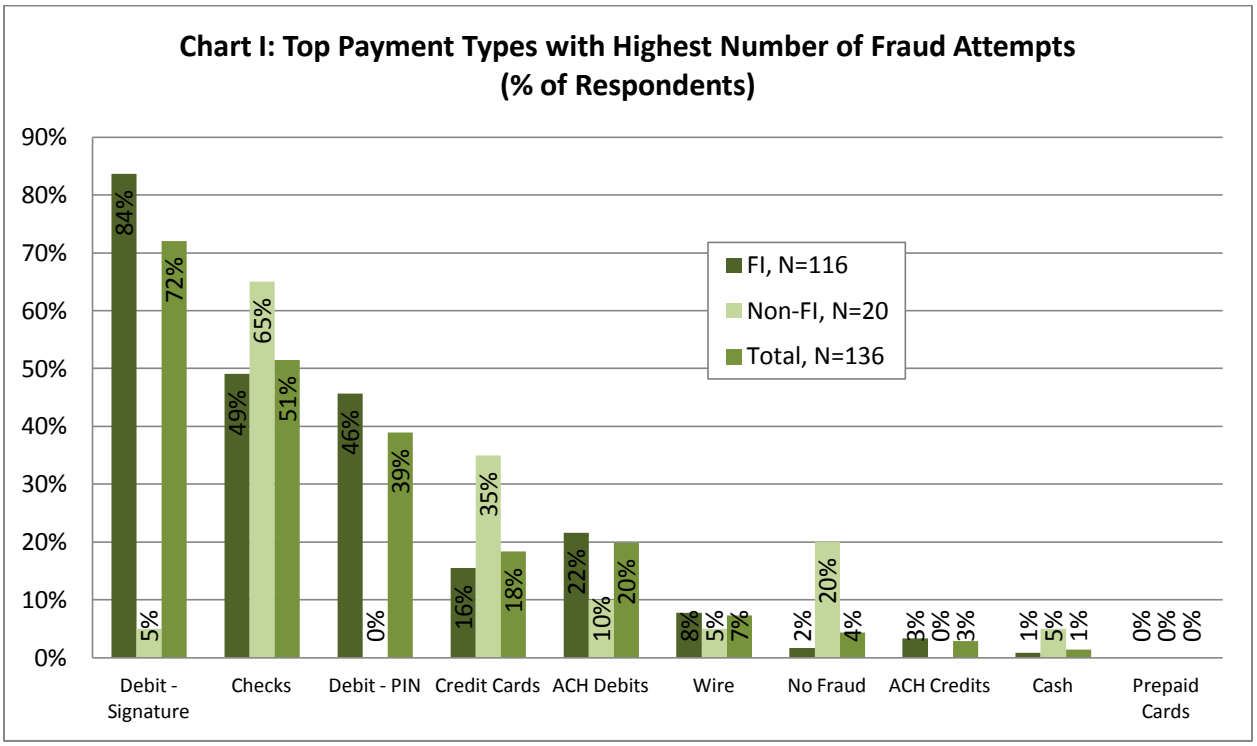
Chart H illustrates the types of payments offered by financial institution respondents.



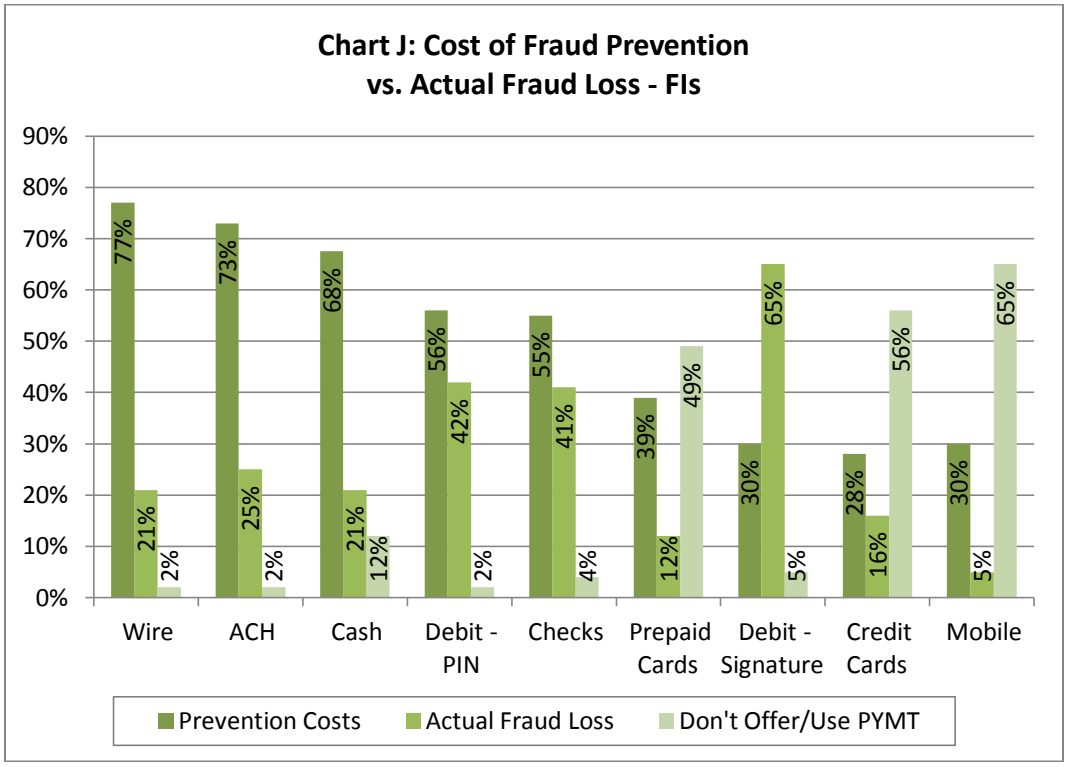
b. Payments Fraud Attempts and Financial Losses

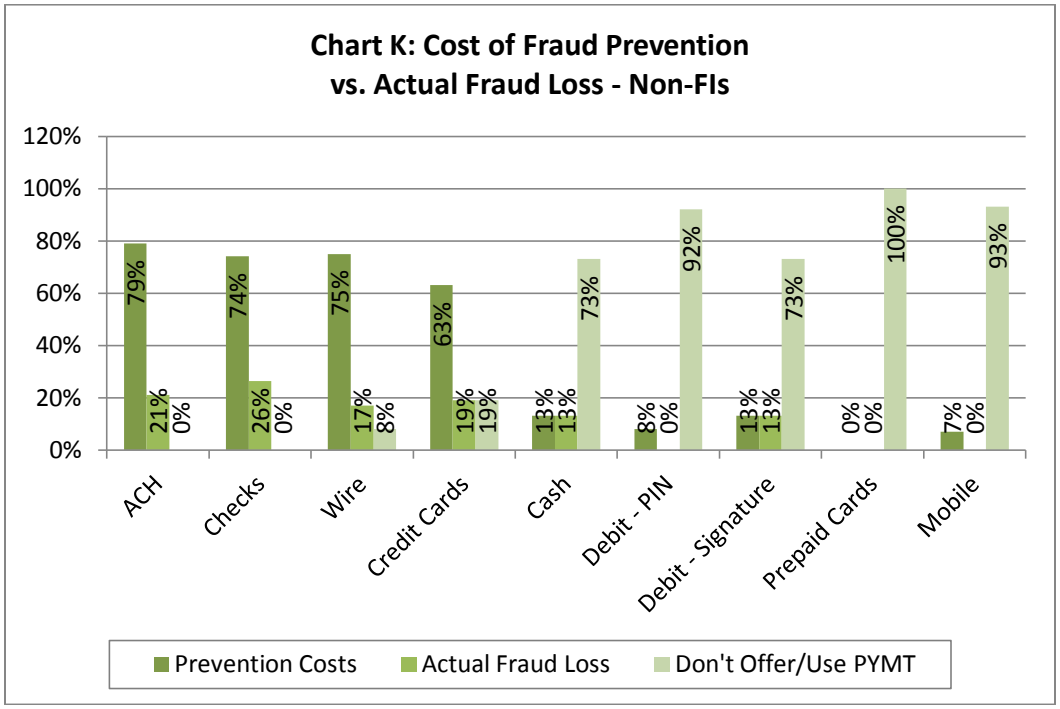
Only two (1.7%) of the financial institution respondents reported no payments fraud attempts; that figure was four (20%) for all other organizations. Respondents were asked which payment types had the highest number of attempts, as reported in Chart I. Of FI respondents, 83.6%

chose signature debit card attempts, followed by check (49.1%) and PIN debit (45.7%). Check fraud attempts were by far the highest among non-FI organizations at 65%, with credit card second highest at 35%.



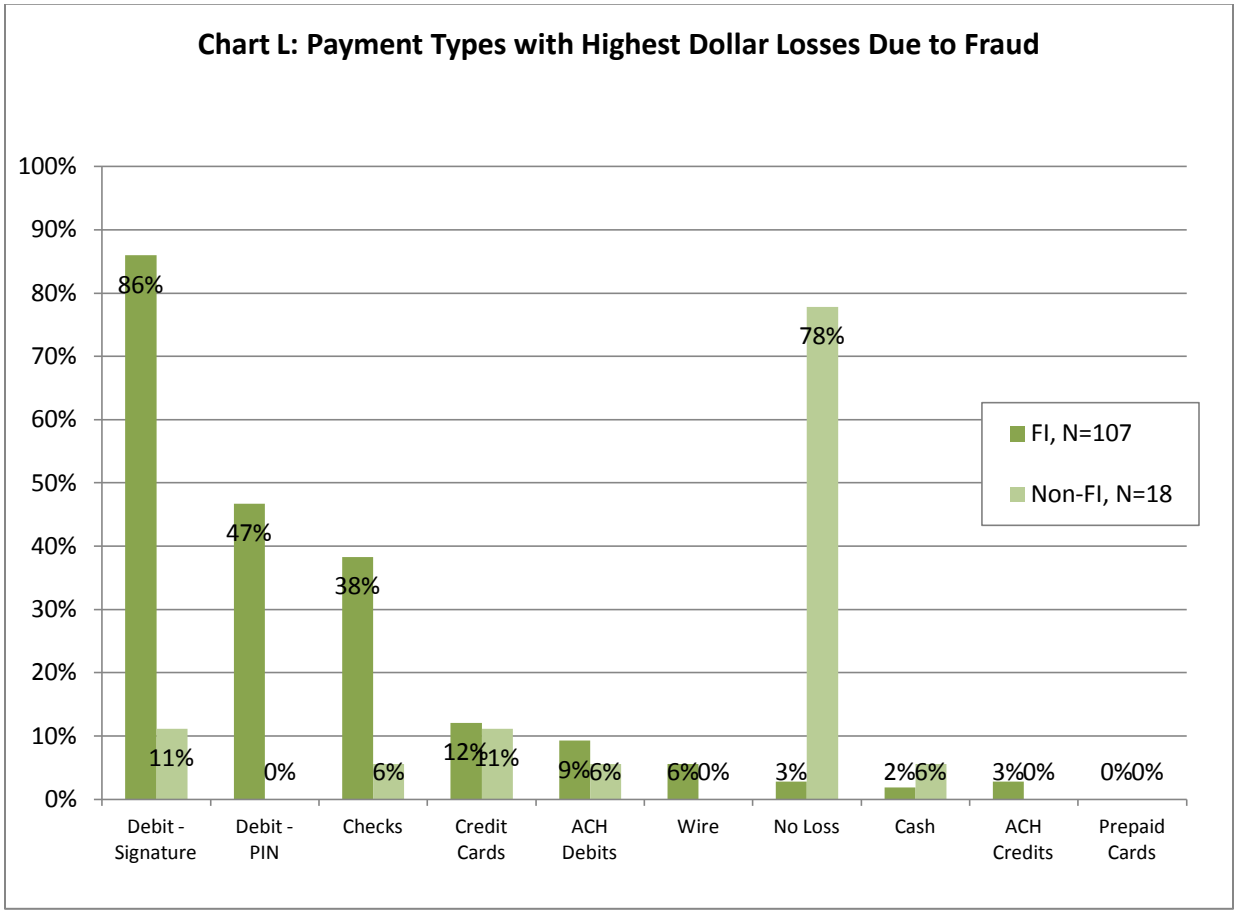
For all payment types except signature debit, the majority of financial institution respondents indicated that their fraud prevention costs exceed their actual dollar losses to fraud (Chart J). Non-financial institution respondents tended to offer or use fewer types of payments, but for those payment types offered/used, they also indicated that fraud prevention tends to be more costly than actual fraud losses (Chart K).





Only 2.8% of the FI respondents reported no dollar losses due to payments fraud; that number jumps to 77.8% for all other respondents. Respondents were asked which payment types have the highest dollar losses, as reported in Chart L. Eighty-six percent of the financial institution

respondents identified signature debit cards as having the highest dollar losses, followed by PIN debit cards and checks. In contrast, non-financial institution respondents identified credit cards and signature debit cards as having the highest dollar losses at about 11% each, followed by checks, ACH and cash at about 6% each.

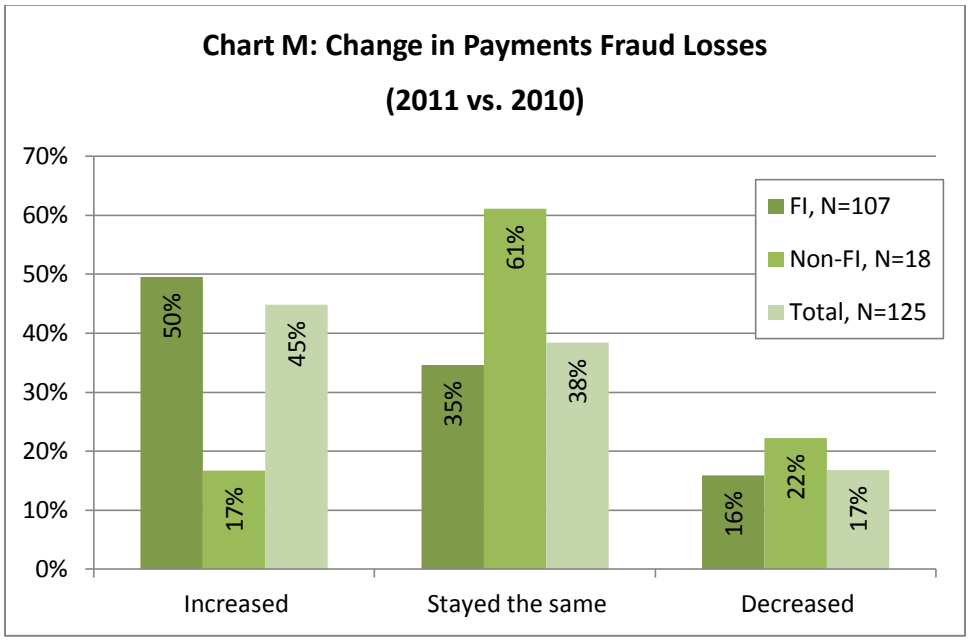


Over 74% of respondents estimated losses as 0.5% or less of their annual revenue (Table 1). Nearly 63% of all respondents selected the lowest range of loss, or less than 0.3% of annual revenues. These data suggest that losses due to payments fraud are relatively well controlled.

Table 1: Payments Fraud Financial Losses by Percentage of Respondents that Incurred Losses

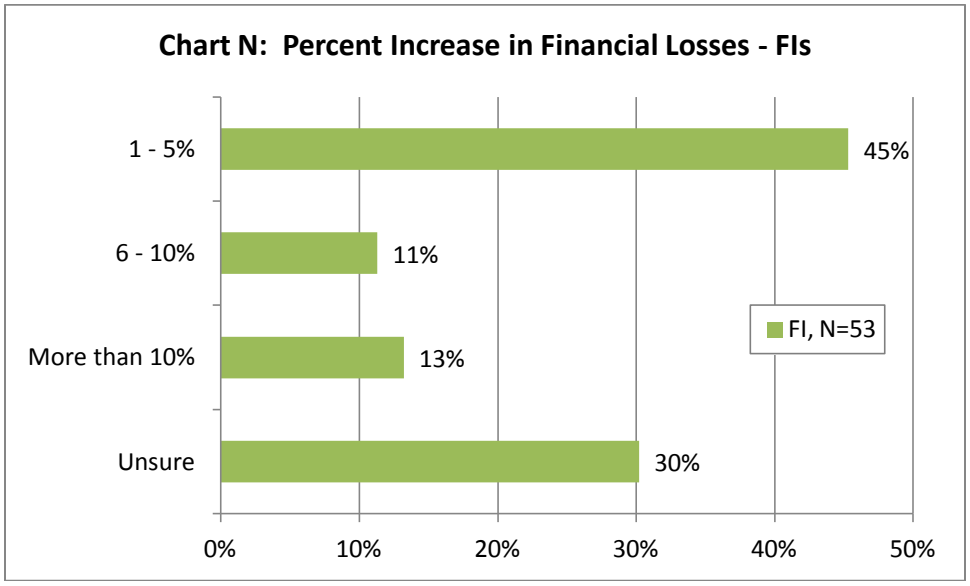
	Loss Range as a Percent of Annual Revenue					
	0%	>0% - .3%	.3% - .5%	.6% - 1%	1.1% - 5%	Over 5%
# of FI respondents (N=102)	2	72	14	9	4	1
% of FI respondents	2%	71%	14%	9%	4%	1%
# of Non-FI respondents (N=18)	14	3	0	1	0	0
% of Non-FI respondents	78%	17%	0%	6%	0%	0%
# of all respondents (N=120)	16	75	14	10	4	1
% of all respondents	13%	63%	12%	8%	3%	1%

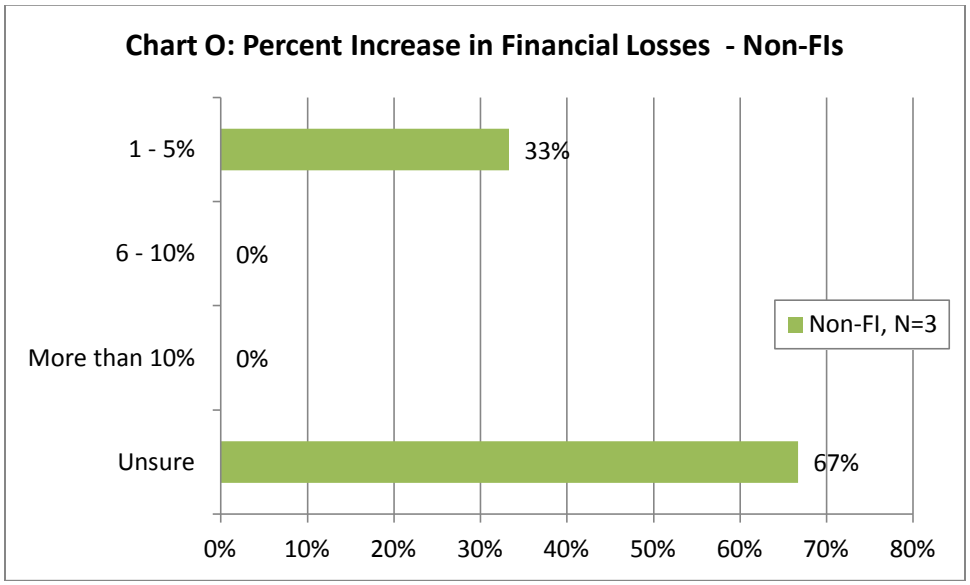
Nearly 45% of respondents experienced increased fraud loss in 2012 over 2011 (Chart M), while approximately 38% indicated their financial losses due to fraud had stayed the same, and nearly 17% reported that they had decreased.



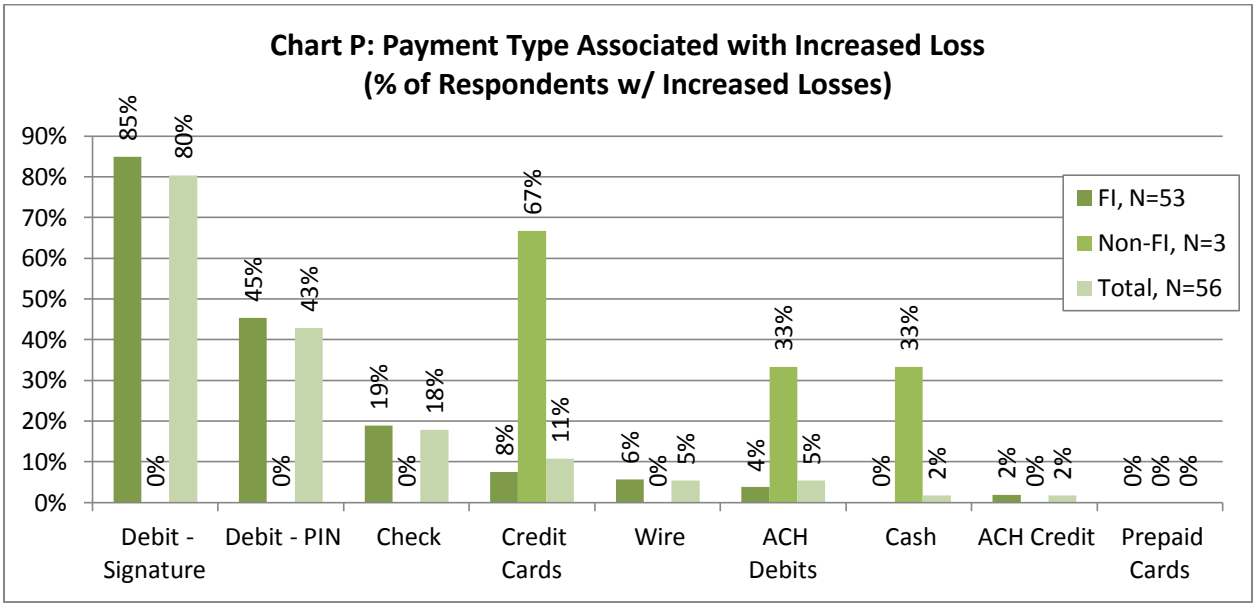
As shown in Charts N and O below, respondents that reported an increase in loss estimated the size of the increase. Nearly 45% of these respondents cited an increase of 1% to 5%, and 13%

estimated an increase of 10% or more. However, based on Table 1 above, note that, despite these increases, the total loss, estimated as a percentage of revenues, remains relatively small for the vast majority of respondents.

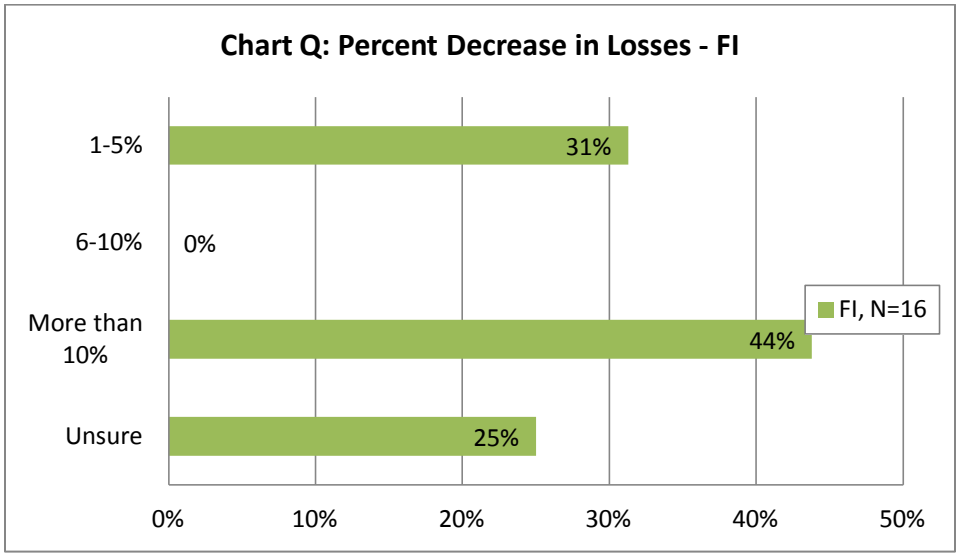




As shown in Chart P below, respondents that reported an increase in loss were also asked to identify the payment type associated with the increased loss. Signature debit led the list for financial institutions, while credit cards were tops for non-financial institution respondents.



Charts Q and R below indicate the responses of those that reported a decrease in loss, who were then asked to estimate the size of the decrease.



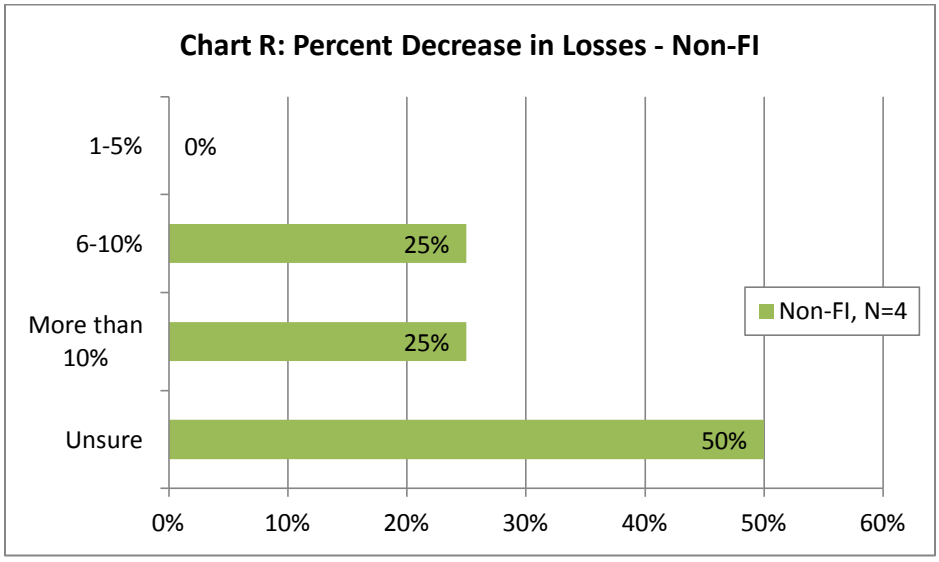
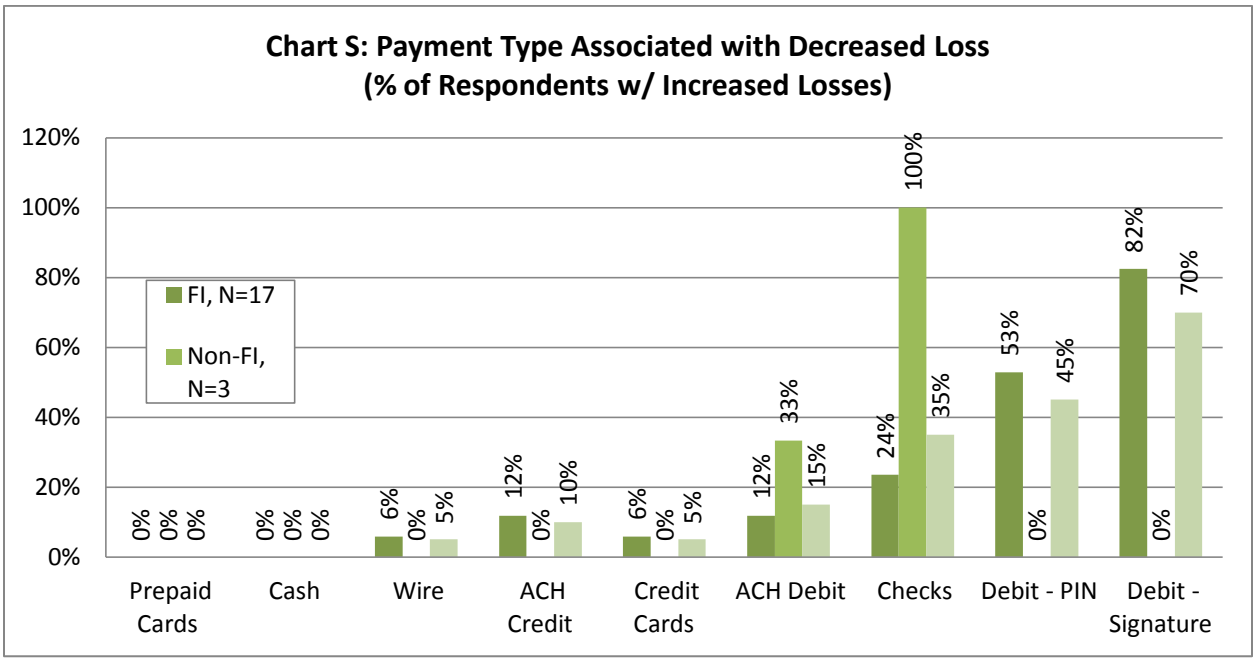
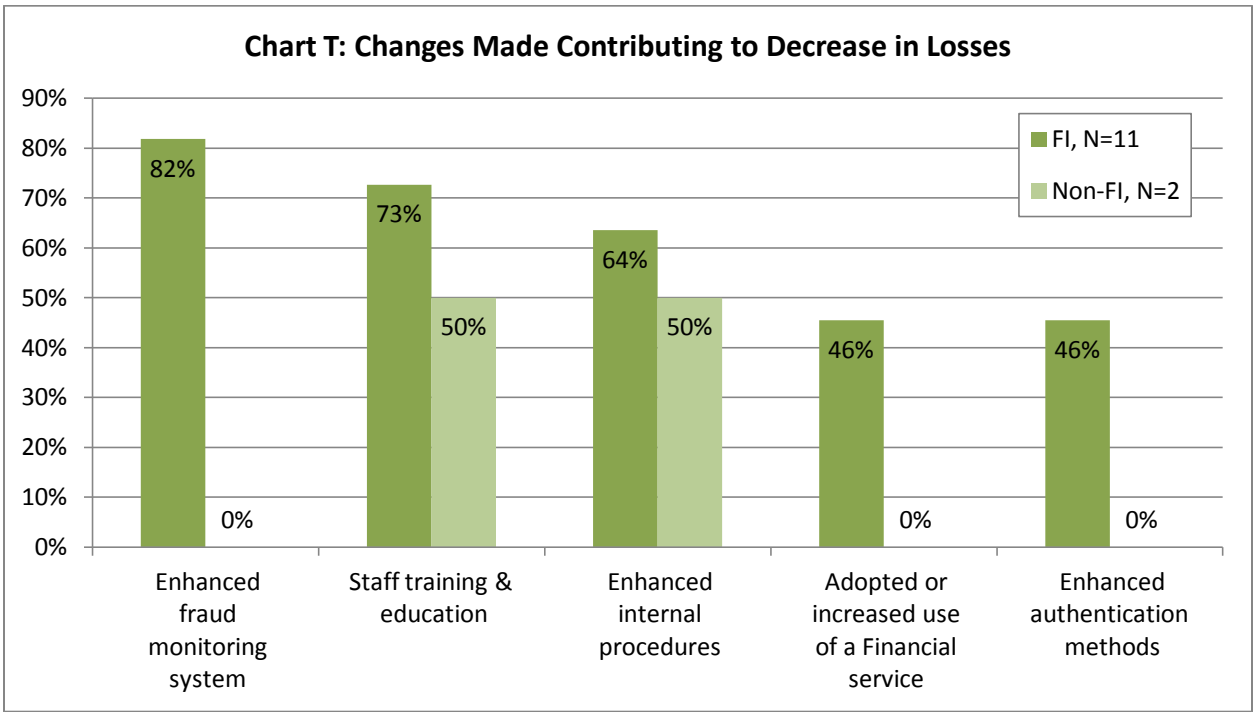


Chart S below shows the results for respondents that reported a decrease in loss who were then asked to identify the payment type associated with the decreased loss. In this area, signature debit topped the list for financial institutions, while checks were the biggest contributing factor for non-financial institution respondents.

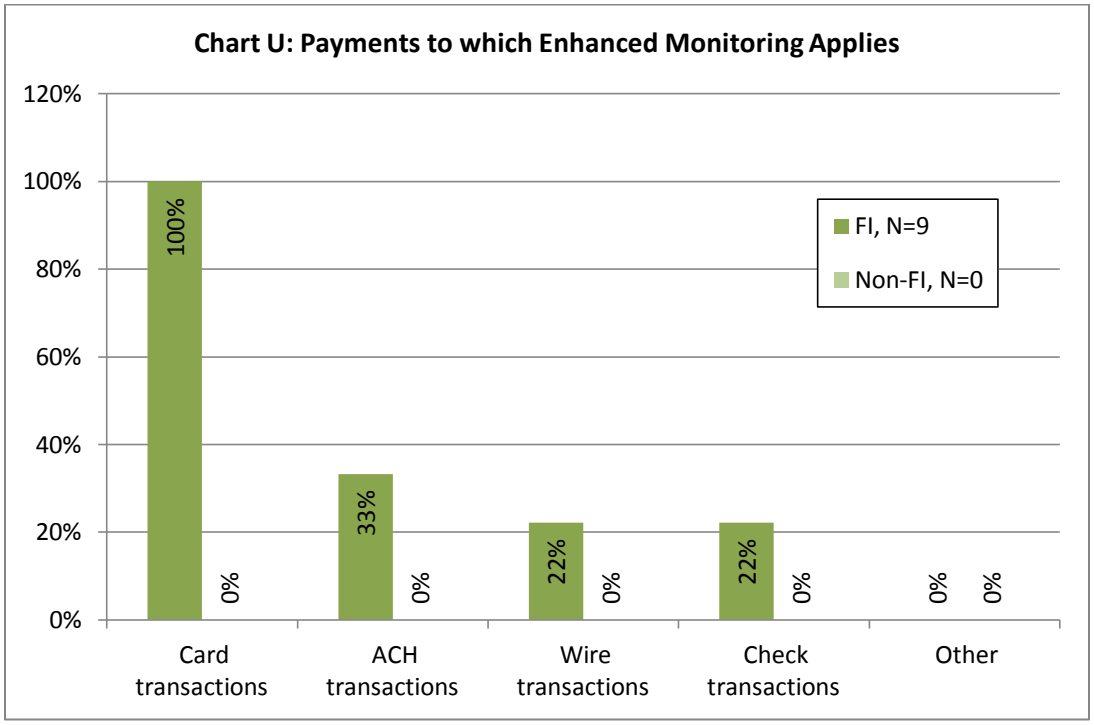


In total, 14 respondents (12 financial institutions and two non-financial institution respondents) indicated that their organizations had made changes to their payments risk management practices that led to the decrease in 2011 payments fraud losses, while seven indicated that they had not. Among those who had made changes to their practices, the most common change was to enhance the organization's systems for monitoring fraud (Chart T). Other

changes included increasing staff training/education and enhancing internal controls and procedures.

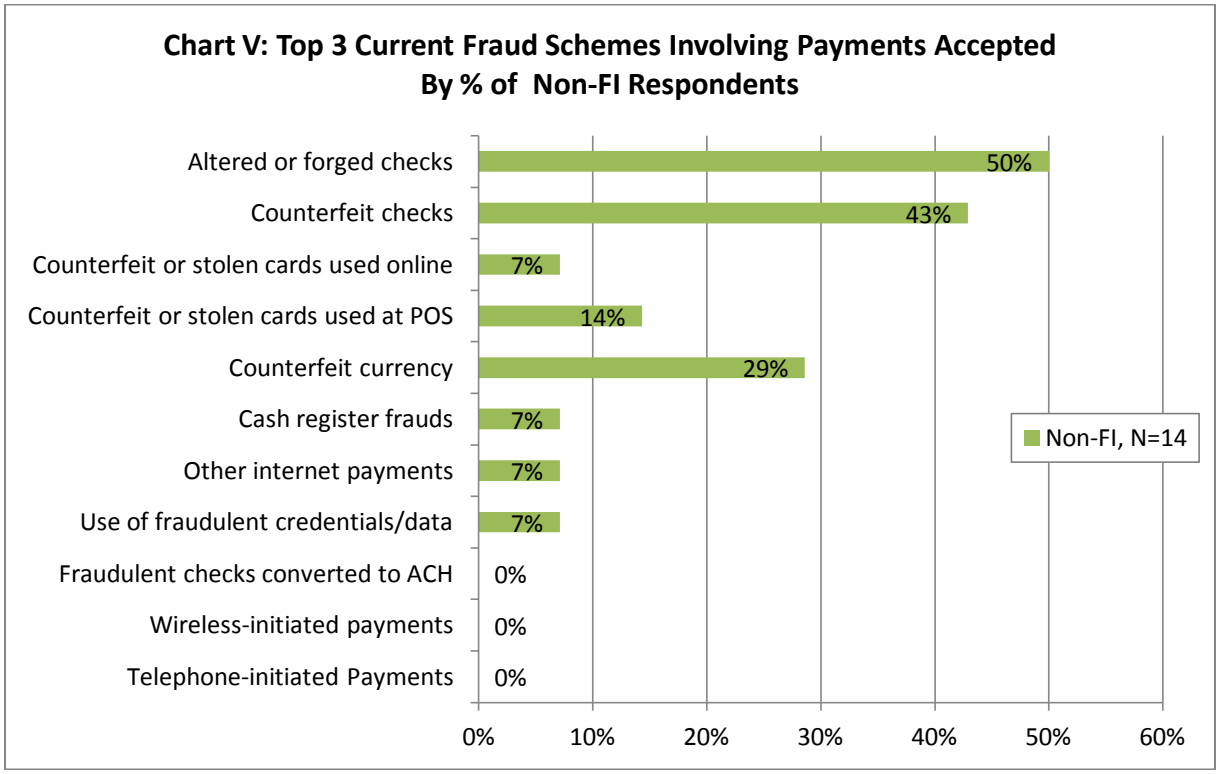


Respondents who indicated that enhancements to their organization's fraud monitoring systems had helped to reduce fraud losses were asked to further identify the payment types to which enhanced monitoring applies. Their responses are summarized in Chart U below.

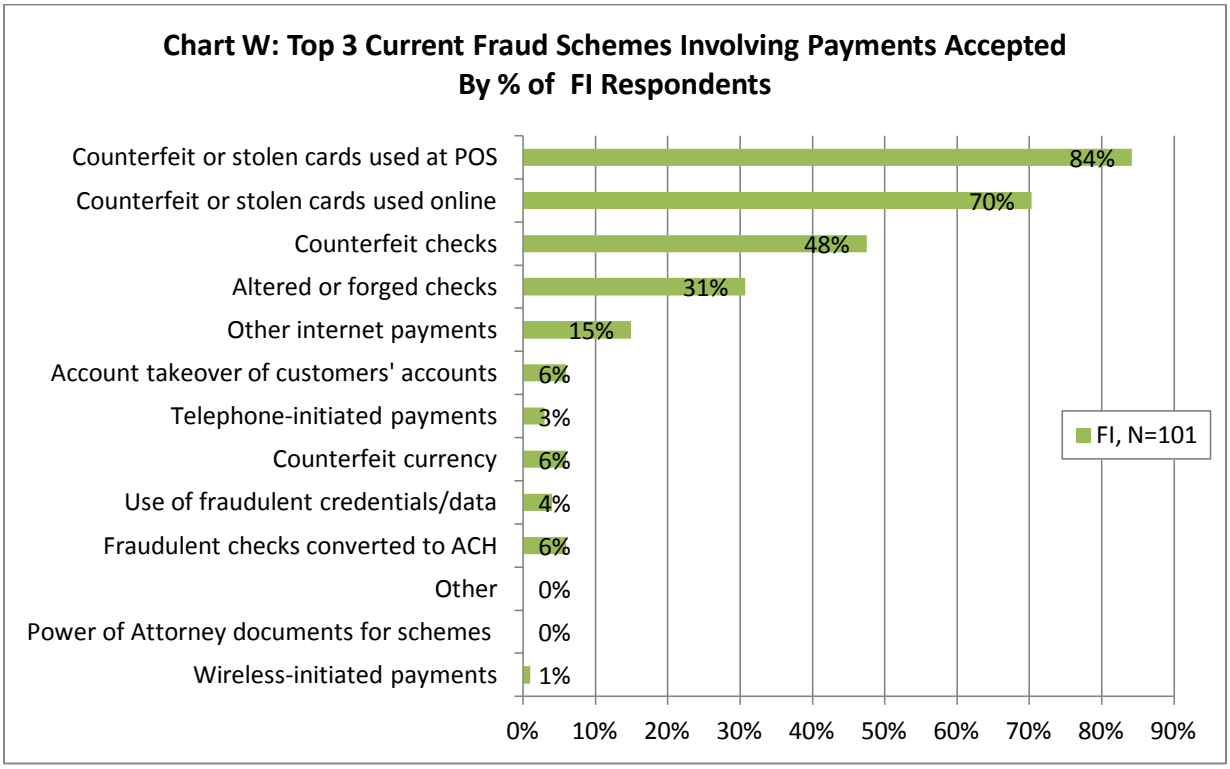


c. Most Common Fraud Schemes

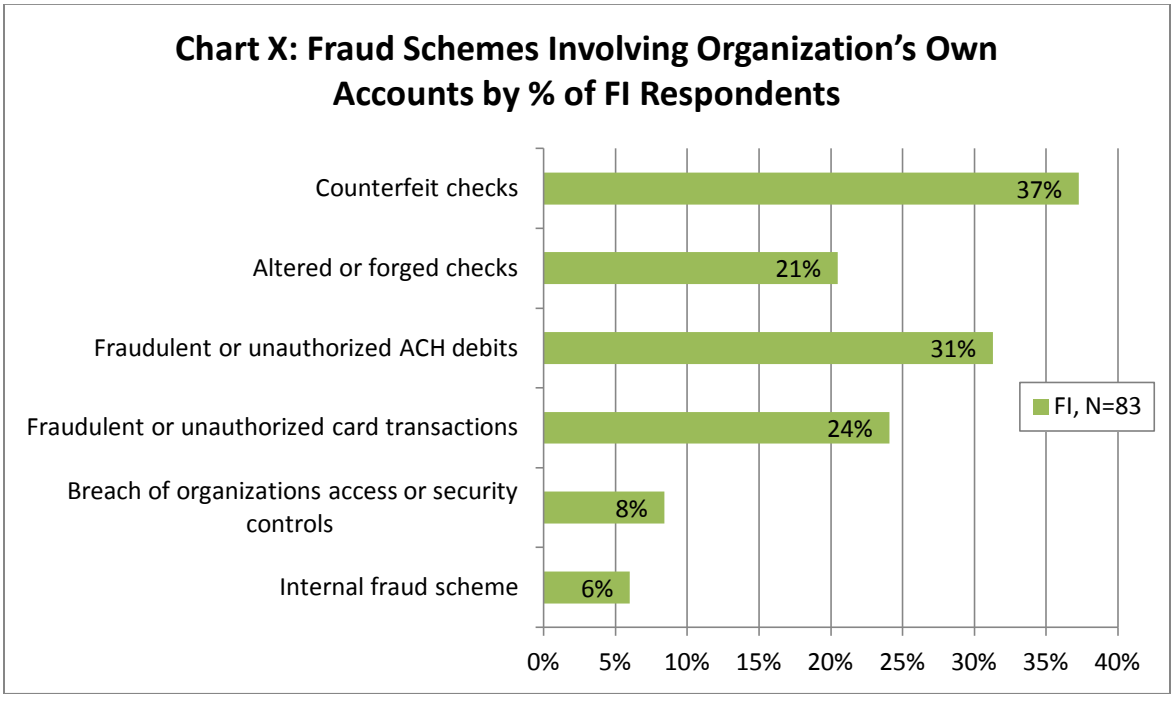
For payments received by non-financial institution respondents, the top two current fraud schemes most often used were altered/forged checks and counterfeit checks (Chart V). Fifty percent of non-FI respondents reported altered or forged checks as the top scheme most often used, followed by counterfeit checks at 43%.



Financial institution respondents indicated that, in payments by or on behalf of their customers, the top two current fraud schemes most often used by fraudsters were counterfeit or stolen cards used at the point of sale (84%) and used online (70%), with counterfeit checks (48%) rounding out the top three (Chart W). Surprisingly, while "corporate account takeover" is a theme often highlighted in the press as a major issue, it was not cited as a significant theme that affected respondents to this survey.

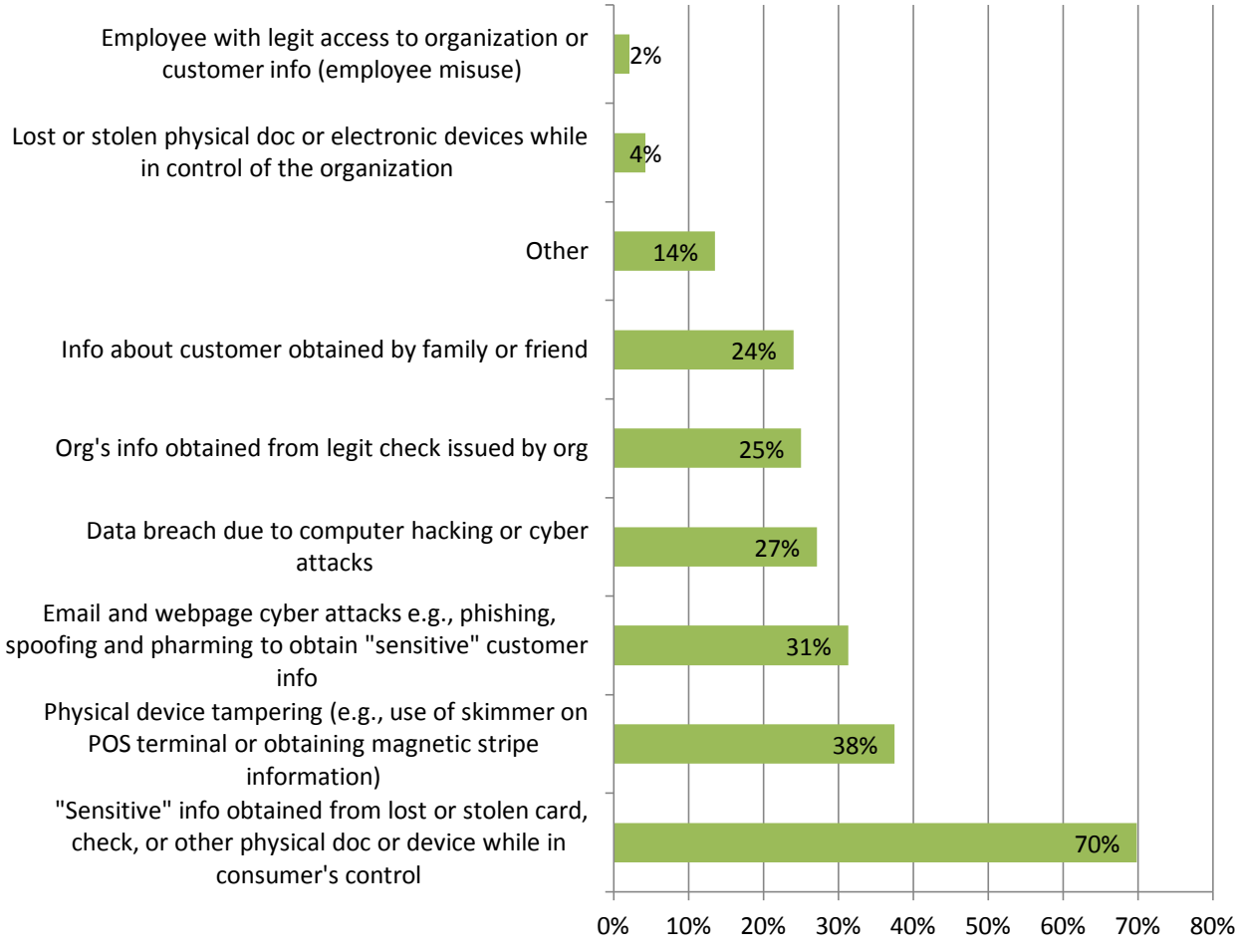


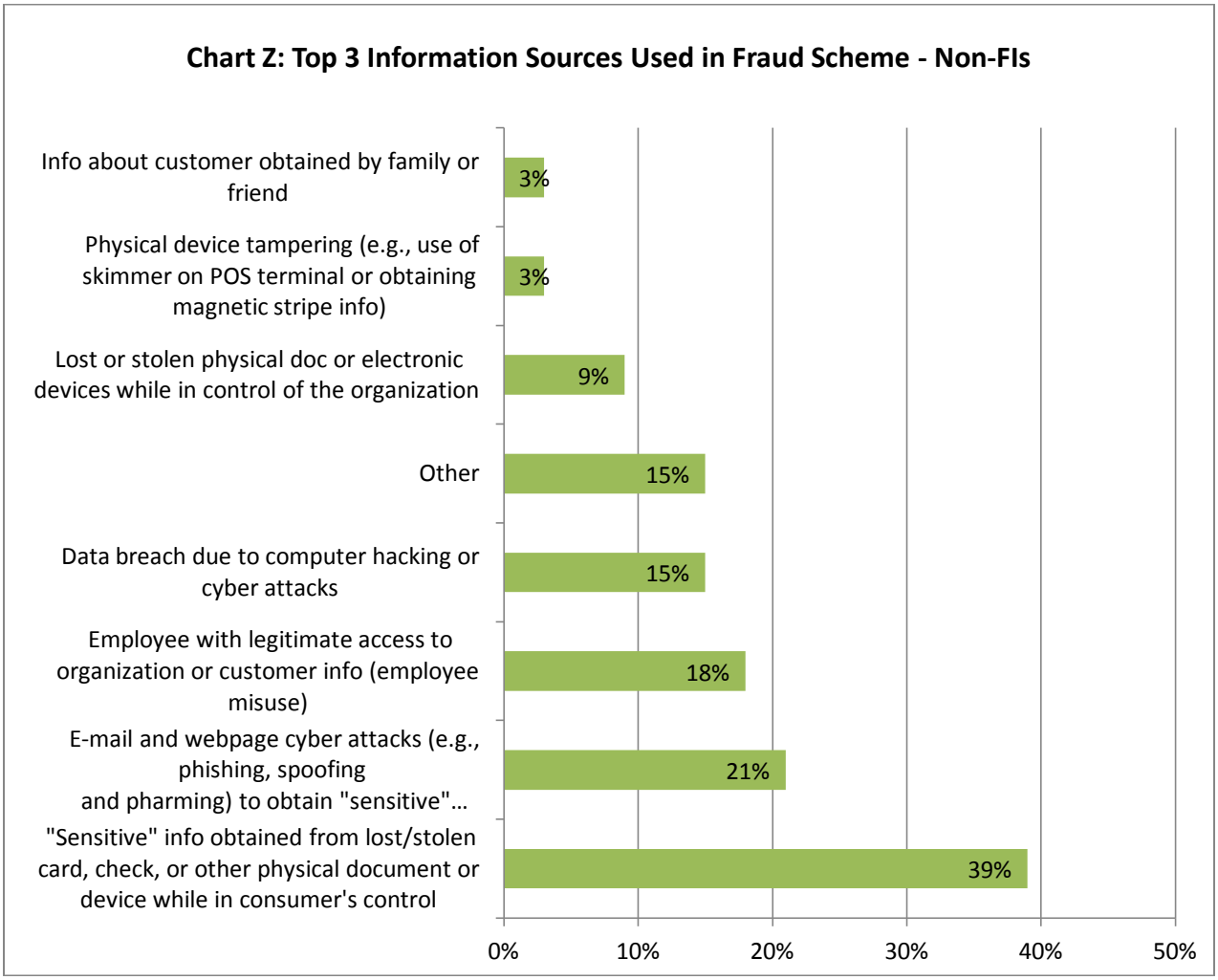
Financial institution respondents that experienced fraud against their organization's own account(s) identified counterfeit checks and unauthorized or fraudulent ACH debits as the top schemes most often used (Chart X).



Charts Y and Z list the top three sources of information used in fraud schemes, as reported by financial and non-financial institution respondents, respectively. Approximately 70% of the financial institution respondents identified “sensitive” information obtained from a lost or stolen card, check or other physical document or device while in the consumer’s control. For non-financial institution respondents, however, the organization's information was most commonly obtained from a legitimate check issued by the organization.

Chart Y: Top 3 Information Sources Used in Fraud Schemes - FIs



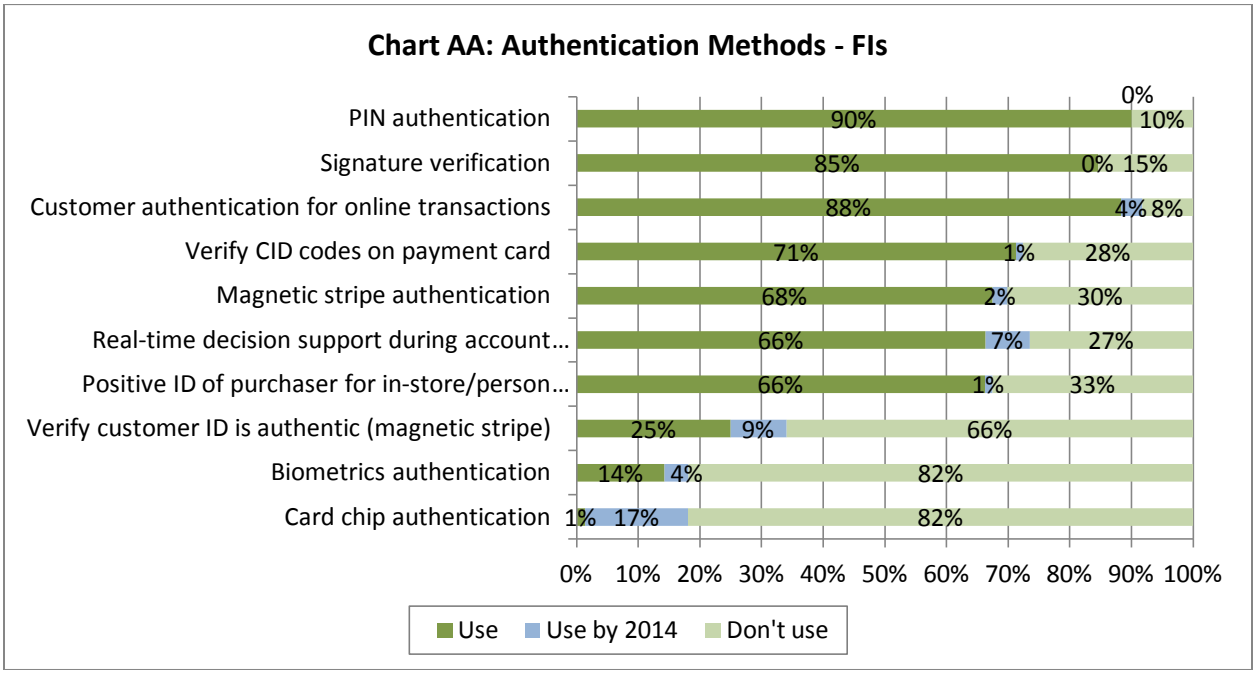


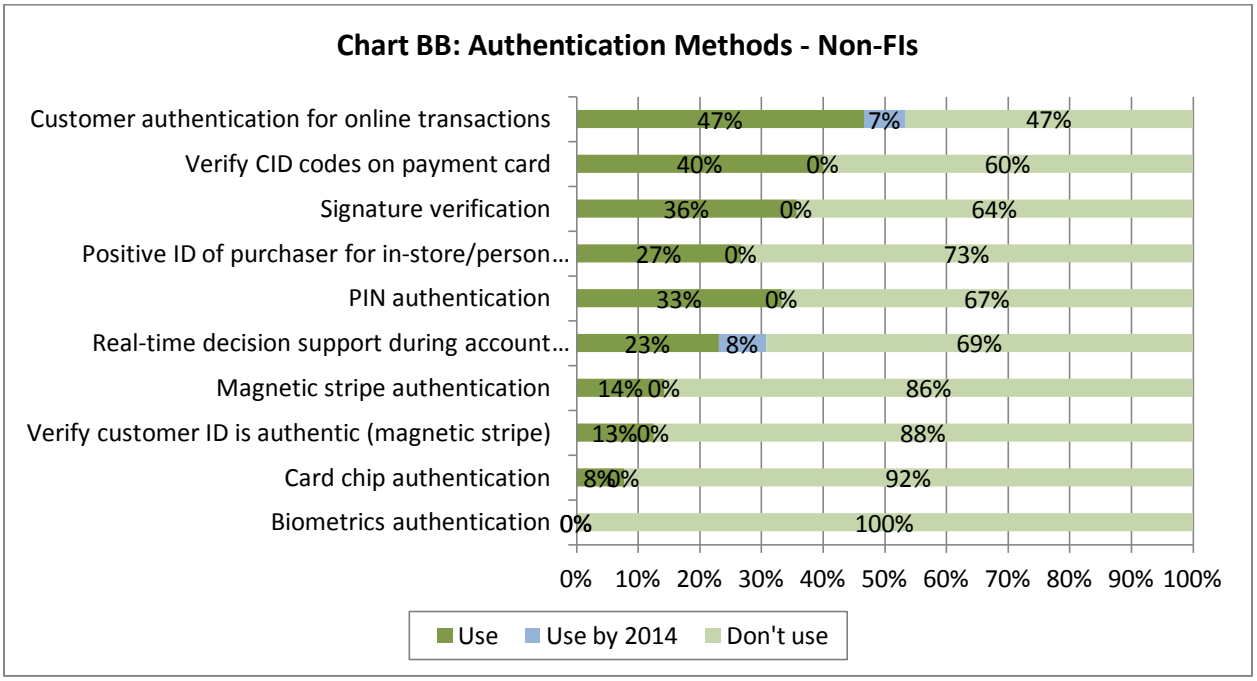
e. Payments Fraud Mitigation Methods Used

Respondents were asked about their use of—and the effectiveness of—various types of fraud mitigation methods and tools. Questions were asked in four areas: i) authentication methods, ii) transaction screening and risk management approach, iii) internal controls, and iv) risk mitigation services offered by financial institutions.

i. ***Authentication.*** Respondents were asked which authentication methods their organizations currently use or plan to use to mitigate payment risk. Responses are indicated in Charts AA and BB for financial and non-financial institution respondents, respectively. In a hopeful sign for the growth in adoption of the EMV standards[3] for card processing, some 17% of FI respondents indicated that they plan to use chip card authentication by 2014.

[3] EMV® is a global standard for credit and debit card transactions based on chip card technology. Though widely adopted in other developing countries, the United States is only beginning to move away from magnetic ("mag') stripe technology to the EMV standards. The standard is commonly referred to as "chip-and-PIN," although in the U.S. implementation—as led by the card associations Visa, MasterCard, Discover and American Express—both the option of "chip-and-PIN" and "chip-and-signature" will be allowed.





Respondents who indicated that their institutions use the various types of authentication methods shown above were then asked to rate the effectiveness of those authentication methods. Overall, both categories of respondents indicate that the processes they have in place are effective (Charts CC and DD). For financial institutions using signature verification, it was the authentication method most often thought to be "somewhat ineffective" (11%), while non-

financial institution respondents using magnetic stripe authentication more often chose that method as "somewhat ineffective" (50%), though the limited number of respondents to this question may make it hard to draw a broad conclusion.

Chart CC: Effectiveness of Authentication - FIs

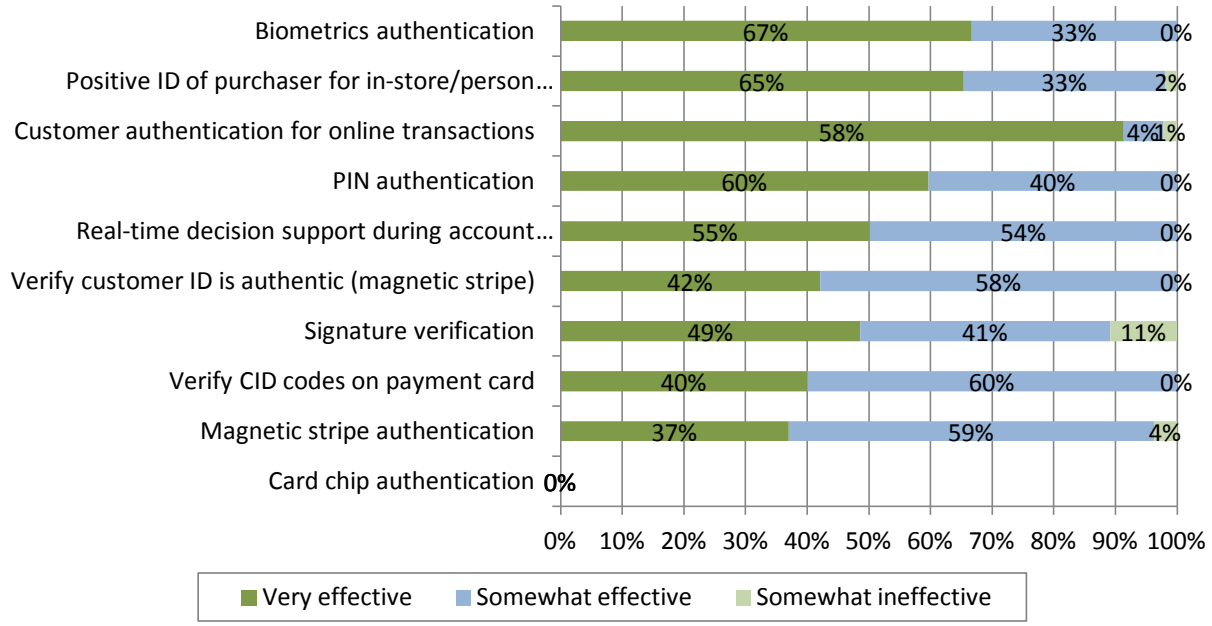
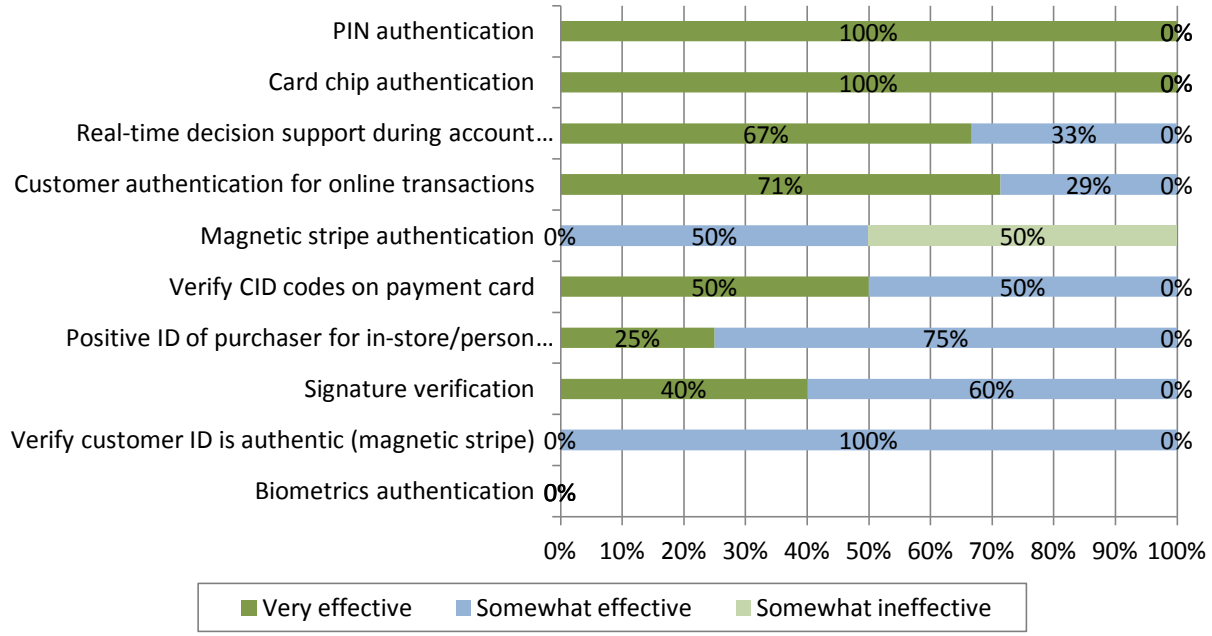
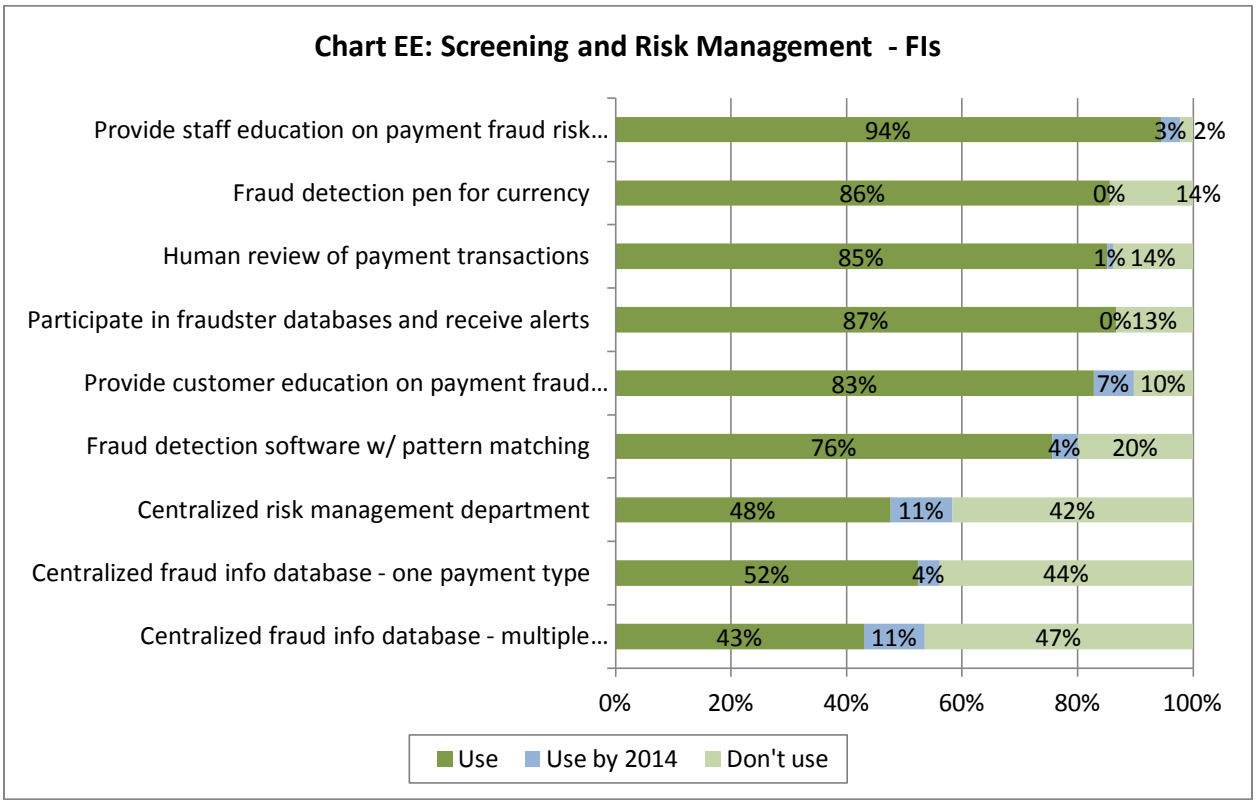
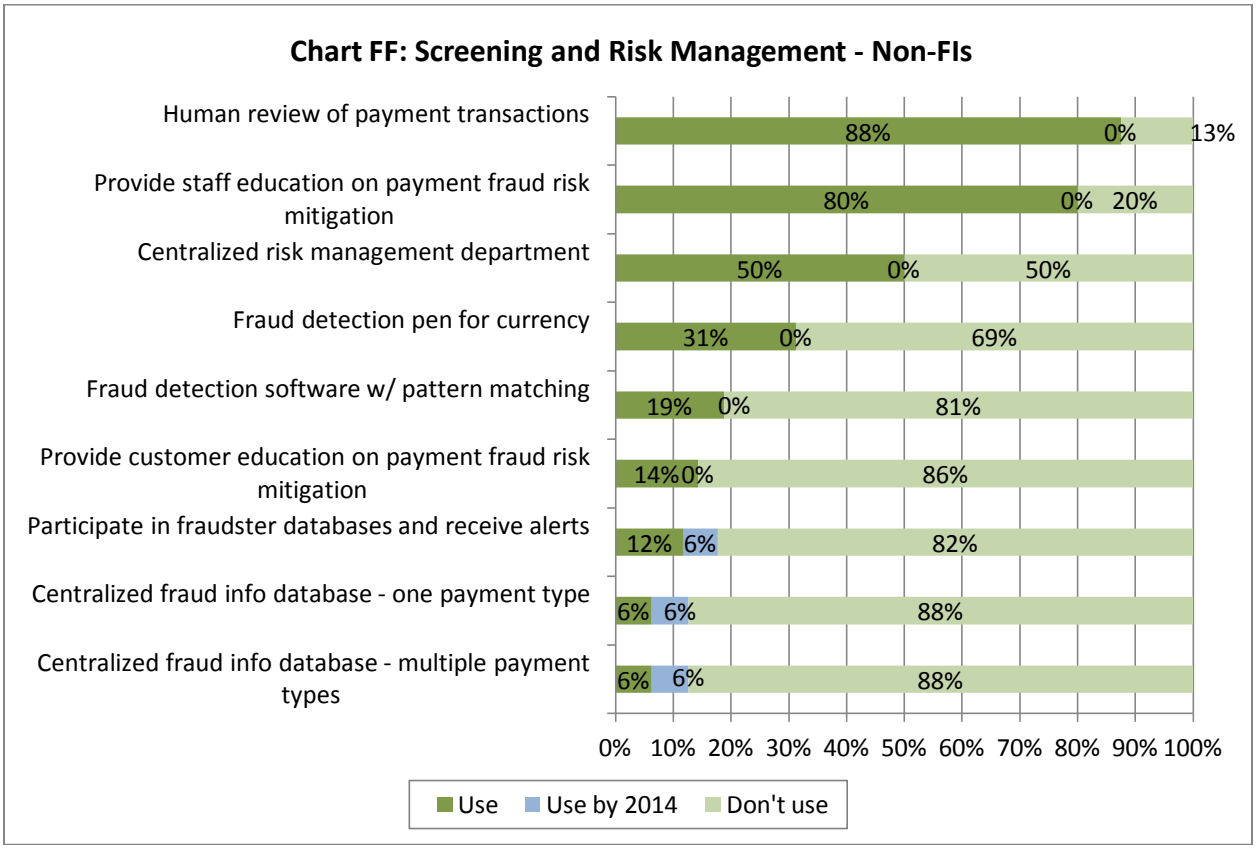


Chart DD: Effectiveness of Authentication - Non-FIs



ii. *Transaction Screening and Risk Management Approach.* Use of different methods to screen transactions and apply centralized risk management varied significantly in overall adoption between FIs and other organizations (Charts EE and FF). While both financial and non-financial institution respondents rely on human review of payment transactions, a larger percent of FI respondents have adopted or plan to adopt centralized fraud information databases (for either one or multiple payment types) and participate in fraudster databases/receive alerts.





Respondents who indicated that they use certain screening and risk management processes were also asked to report on their sense of the effectiveness of those processes. Their responses are indicated in Charts GG and HH. As with the effectiveness of their authentication processes in the section above, in the case of transaction screening and risk management processes, both categories of respondents indicate that the processes they have in place are effective. For non-financial institution respondents, "participate in fraudster databases and receive alerts" was the only method deemed by any respondent(s) to be "somewhat ineffective," though, again, the limited number of respondents to this question may make it hard to draw a broad conclusion there.

Chart GG: Effectiveness of Transaction Screening and Risk Mgmt. - FIs

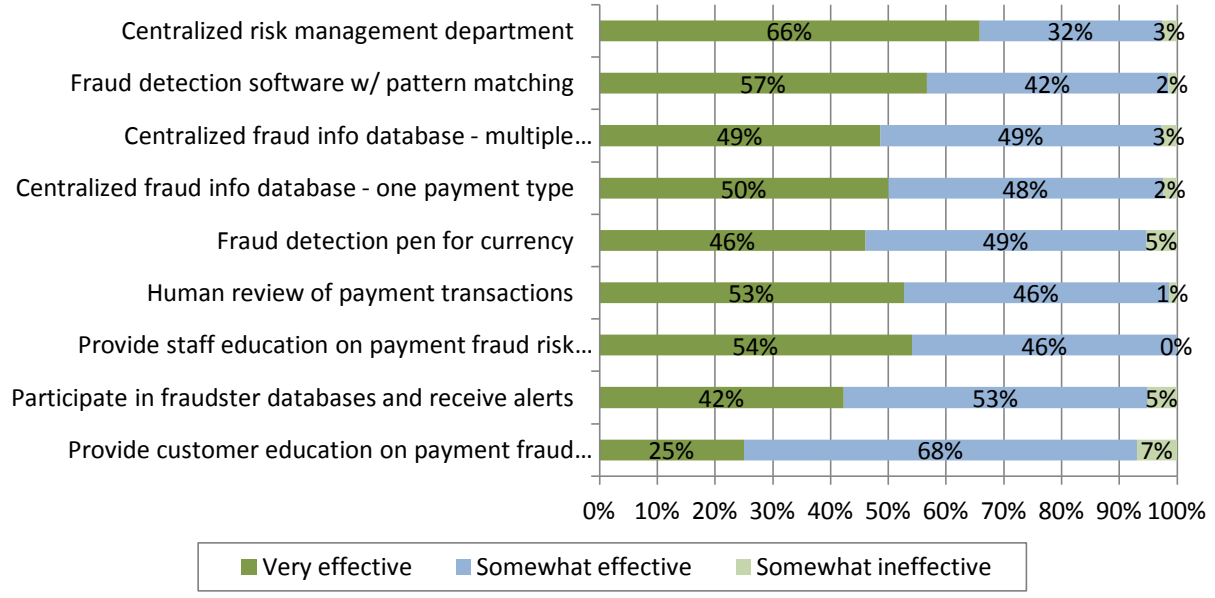
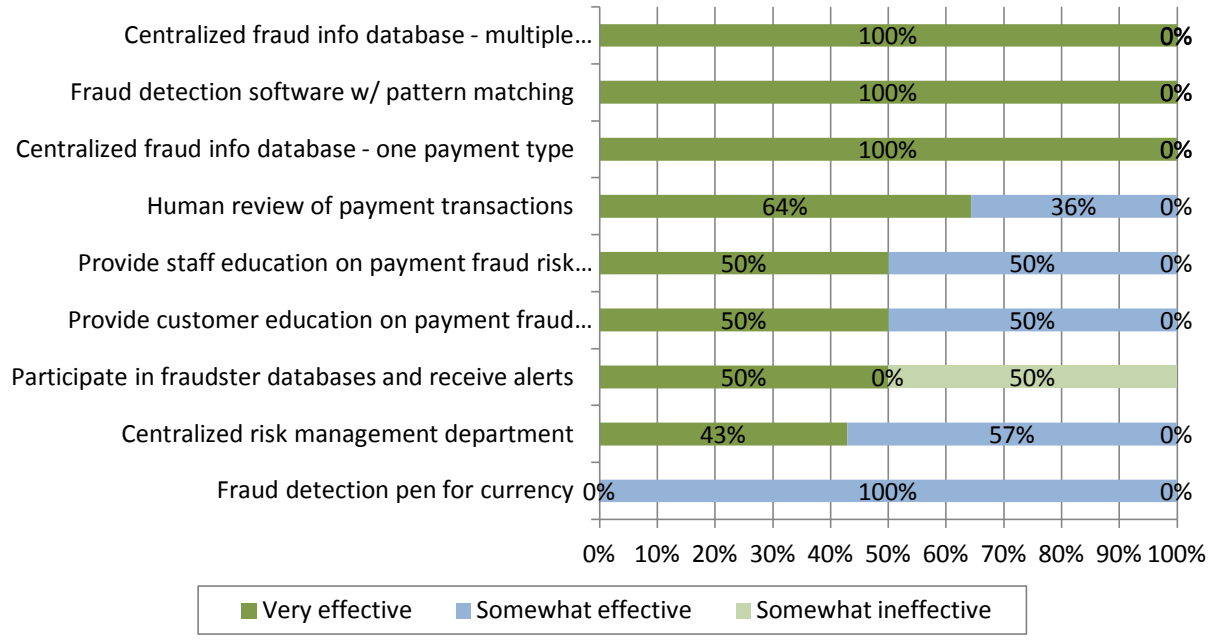
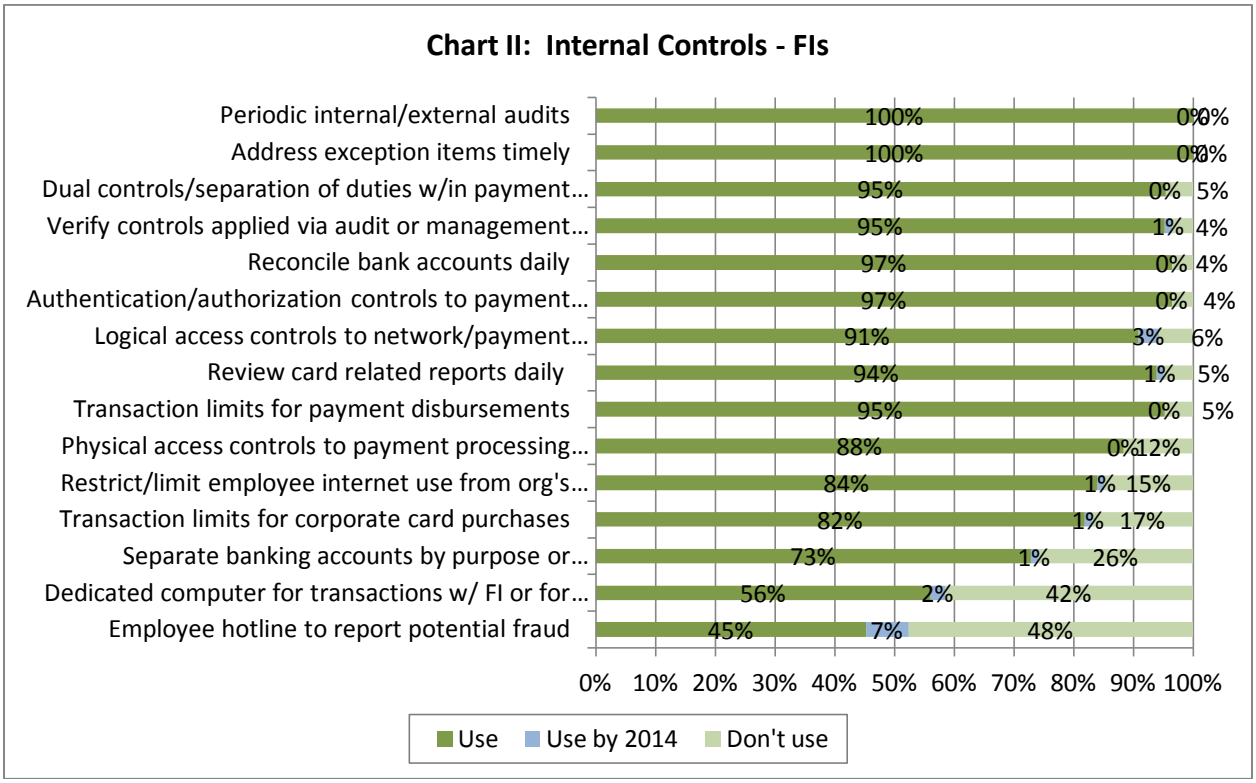


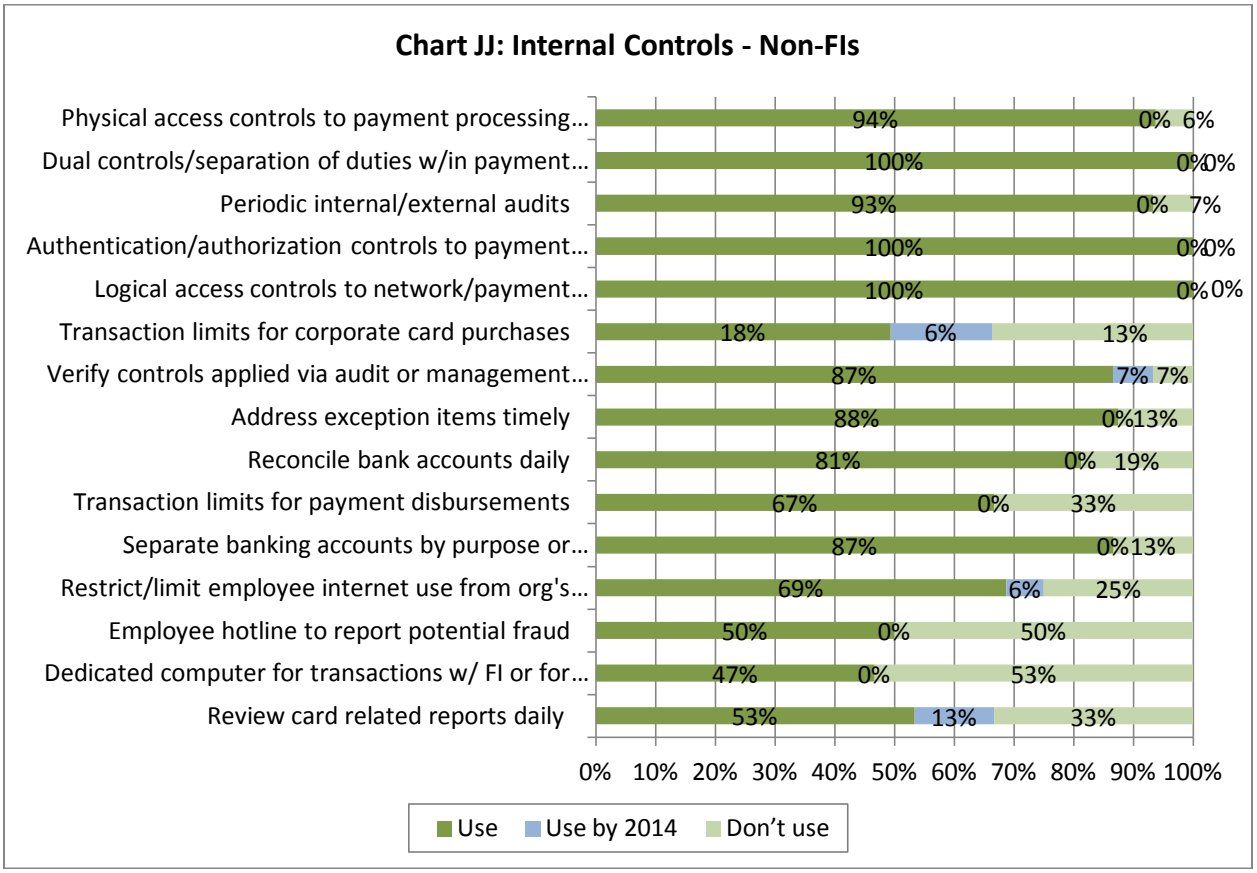
Chart HH: Effectiveness of Transaction Screening and Risk Mgmt. - Non-FIs



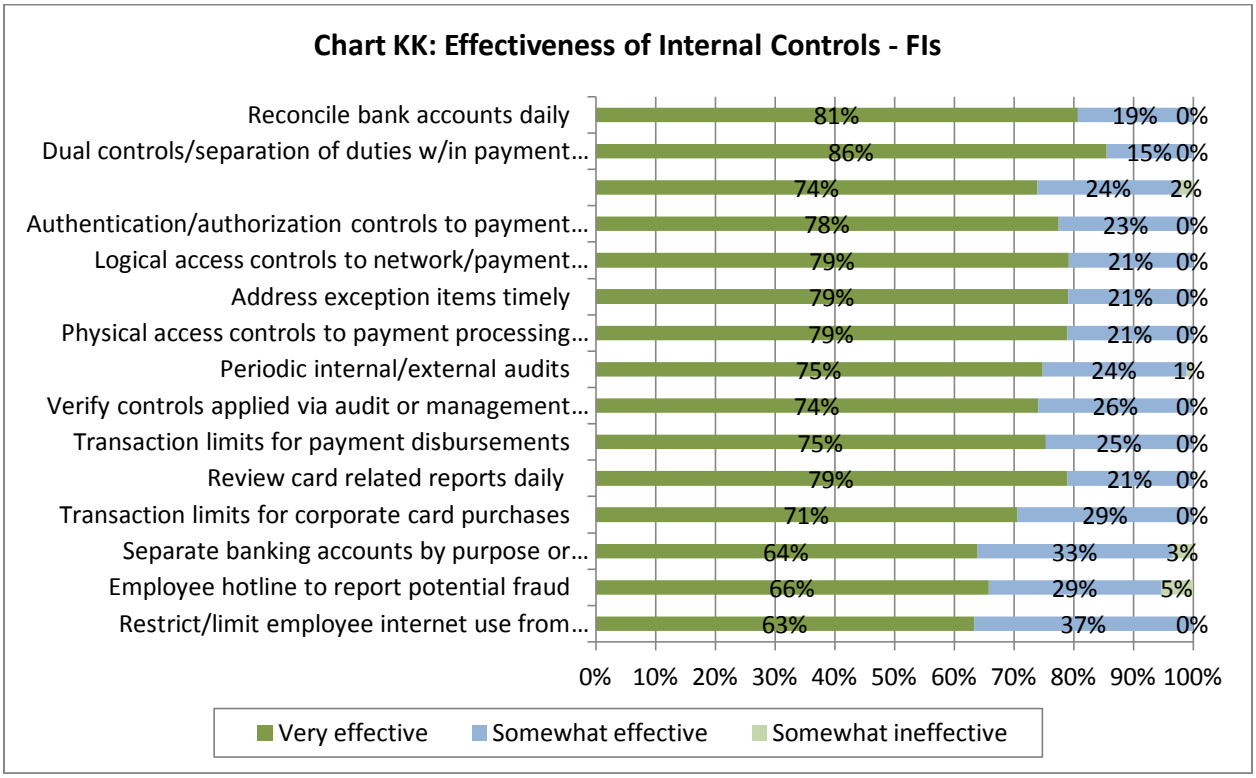
iii. *Internal Controls*. Respondents were asked which internal controls and procedures their organizations currently use or plan to use (Charts II and JJ). Ninety-seven percent of financial

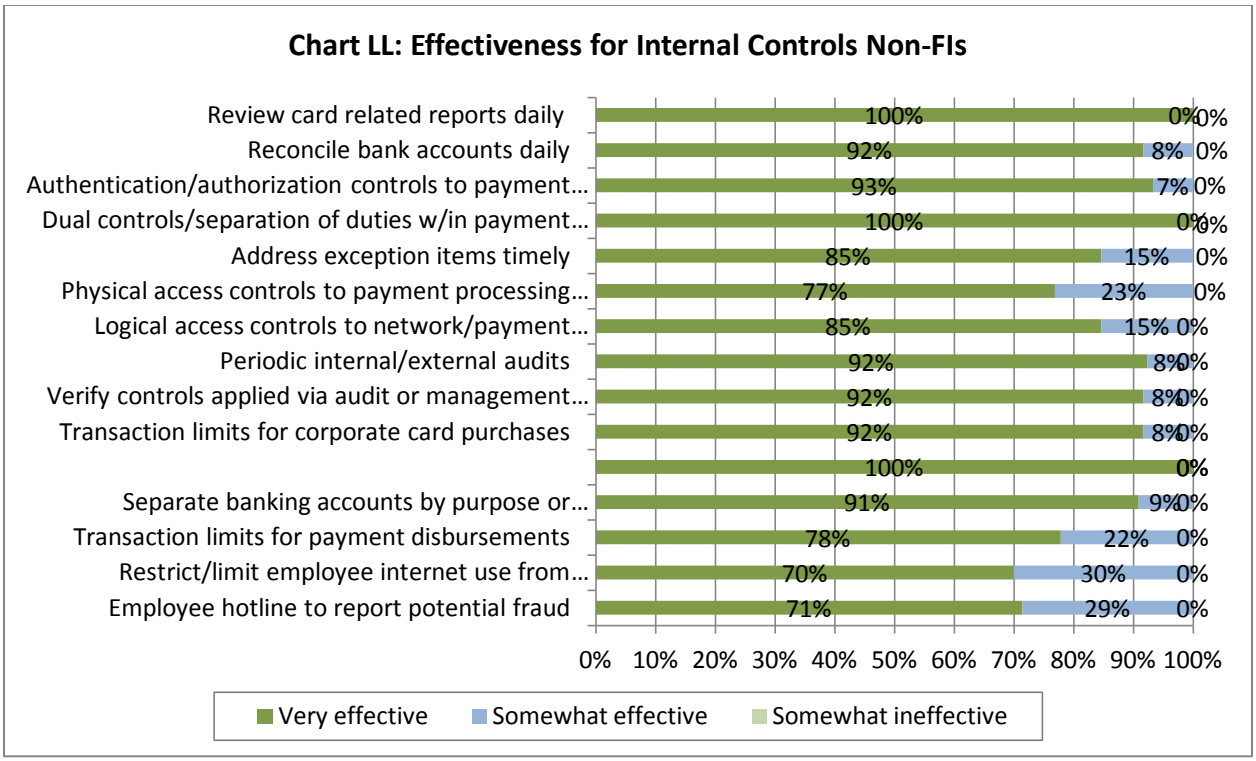
institution respondents reconcile bank accounts daily, but only 81% of non-financial institutions do so. Non-financial institution respondents seem to show a strong preference for use of separate accounts for different types of payments. Non-financial institution respondents seem to be more focused on card-related solutions, as by 2014 a number of respondents plan to set transaction limits for corporate card purchases and to review card-related reports daily.





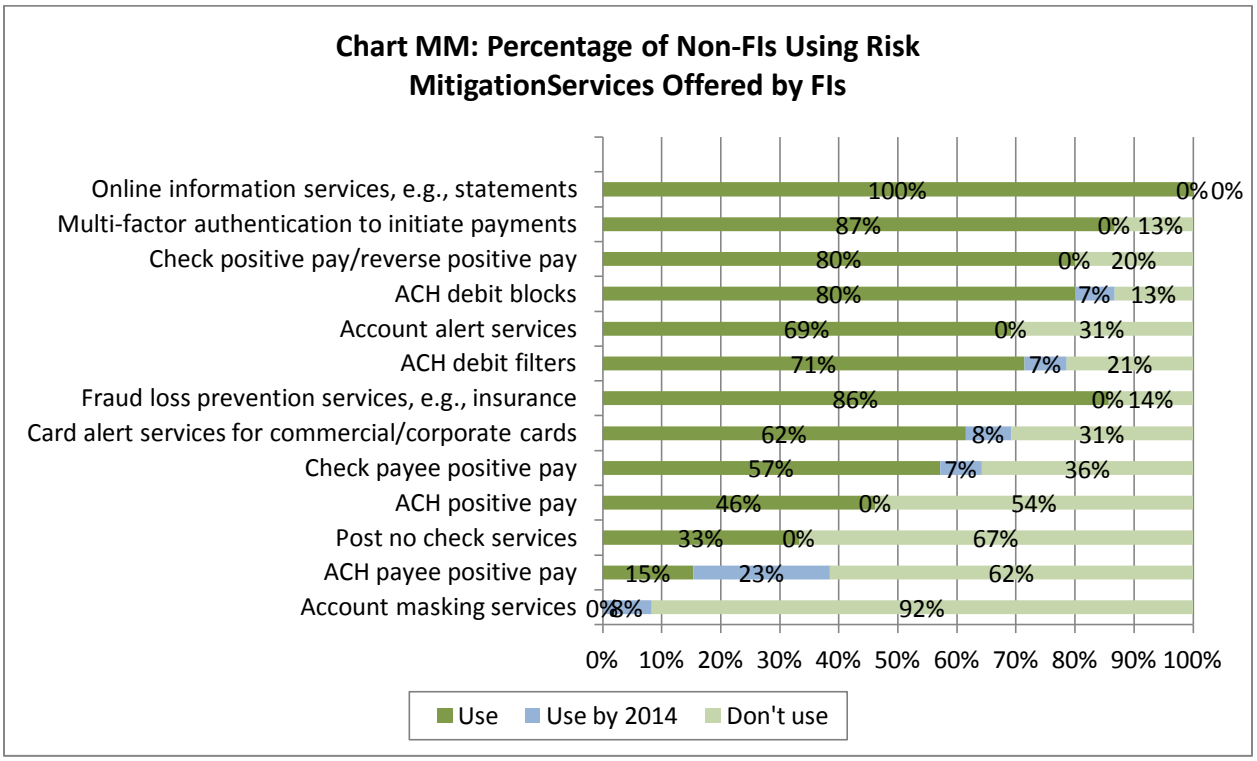
Respondents who indicated they used the types of internal controls as shown above were also asked to report on the effectiveness of those controls. Their responses are indicated in Charts KK and LL. As with the effectiveness of both their authentication processes and in the transaction screening and risk management processes (in the sections above), in the case of internal controls, both categories of respondents indicate that the processes they have in place are effective.





iv. ***Risk Mitigation Services Offered by Financial Institutions.*** Of the various risk mitigation services offered by financial institutions, the top five used by non-financial institution

respondents as reported in Chart MM are: online information services (e.g. statements), multi-factor authentication to initiate payments, fraud loss prevention insurance, check positive pay/reverse positive pay, and ACH debit blocks. Based on the responses as to which services FIs plan to use by 2014, there appears to be significant planned growth in the ACH area, with the use of ACH payee positive Pay (23%) and ACH debit blocks (7%) and debit filters (7%) on the horizon.



When it comes to the effectiveness of these services offered by financial institutions, non-financial institution respondents (users of the services) overall indicated positive responses (Chart NN). The one exception was fraud loss prevention services (e.g., insurance). It is possible that financial institution respondents see insurance as less effective as it does not prevent fraud; it is really only a solution for after fraud has already occurred.

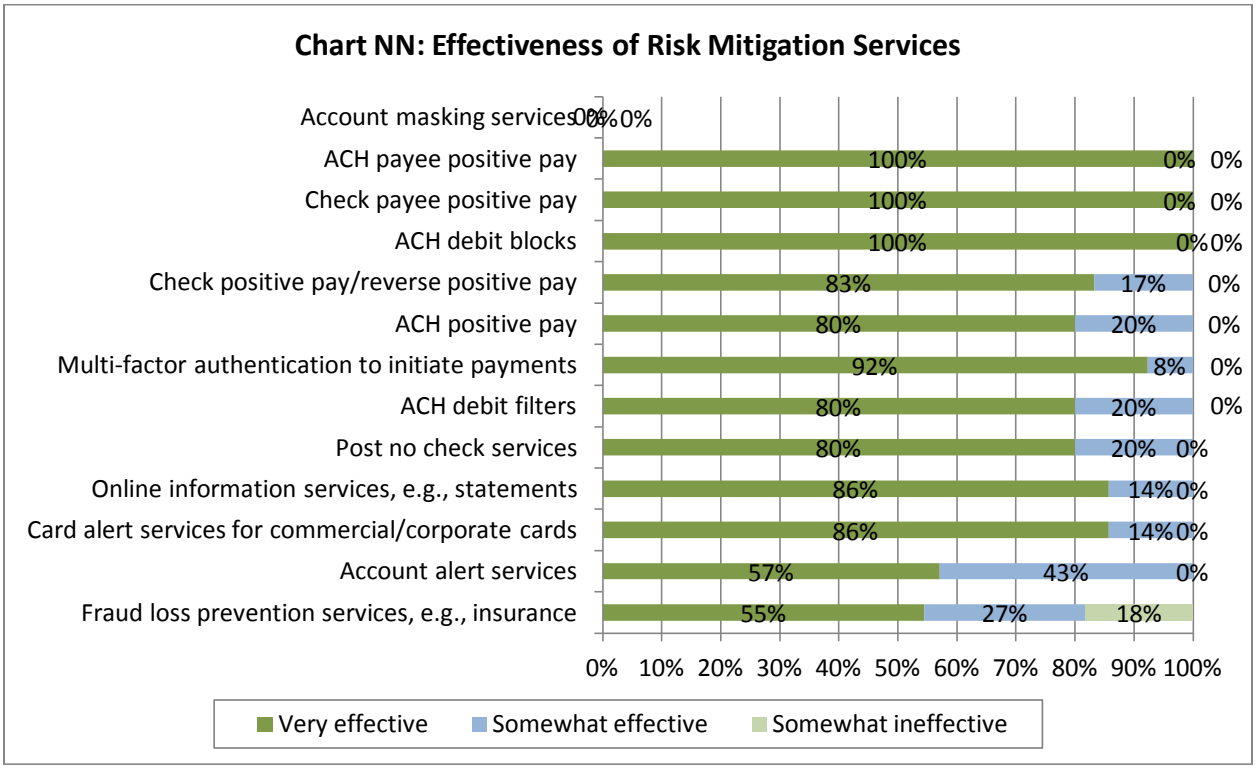
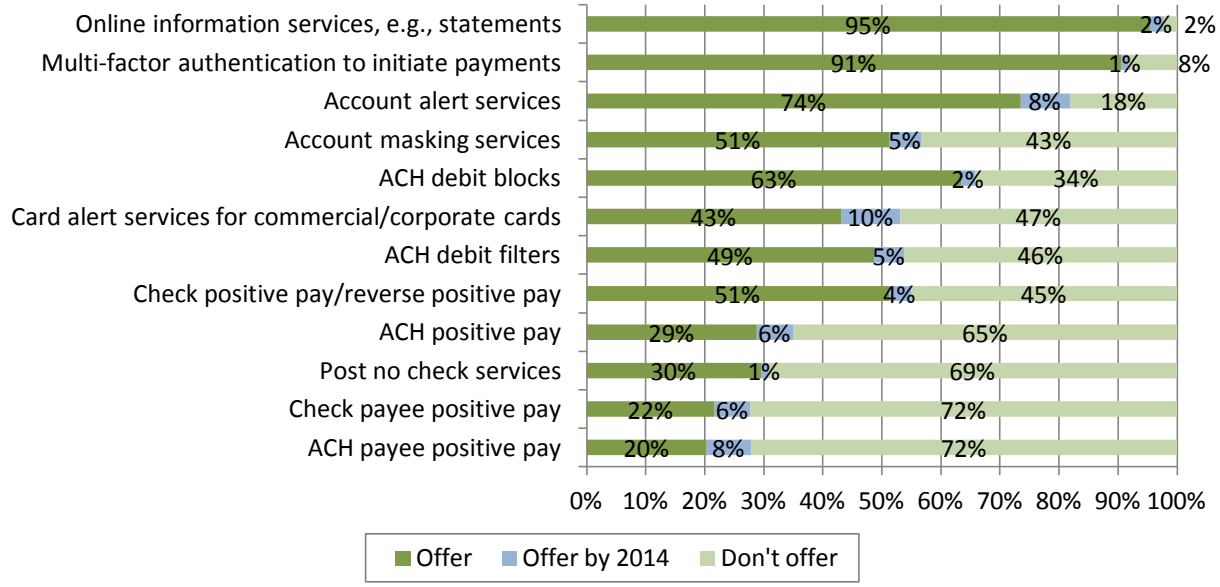


Chart OO provides a view of the various risk mitigation services that are being offered by financial institution respondents. A large majority of respondents are offering services such as online statements to their corporate customers and have implemented multifactor authentication requirements for the initiation of payments. As one moves down the list of service offerings to more complex products, such as positive pay/reverse positive pay and payee positive pay (for both check and ACH), the percentage of financial institution respondents offering those services decreases significantly. It is possible that community bank respondents either cannot offer some of these more sophisticated services or they do not have a commercial customer base that has yet expressed a need for them. In addition, because the financial institution respondents include all types of FIs – both banks and credit unions – the number of respondents may reflect some credit unions that traditionally support individual members, as opposed to corporate customers, and may not need to offer such services to their retail customer base.

Chart OO: Percentage of FI/Svc. Provider Respondents Offering Risk Mitigation Services

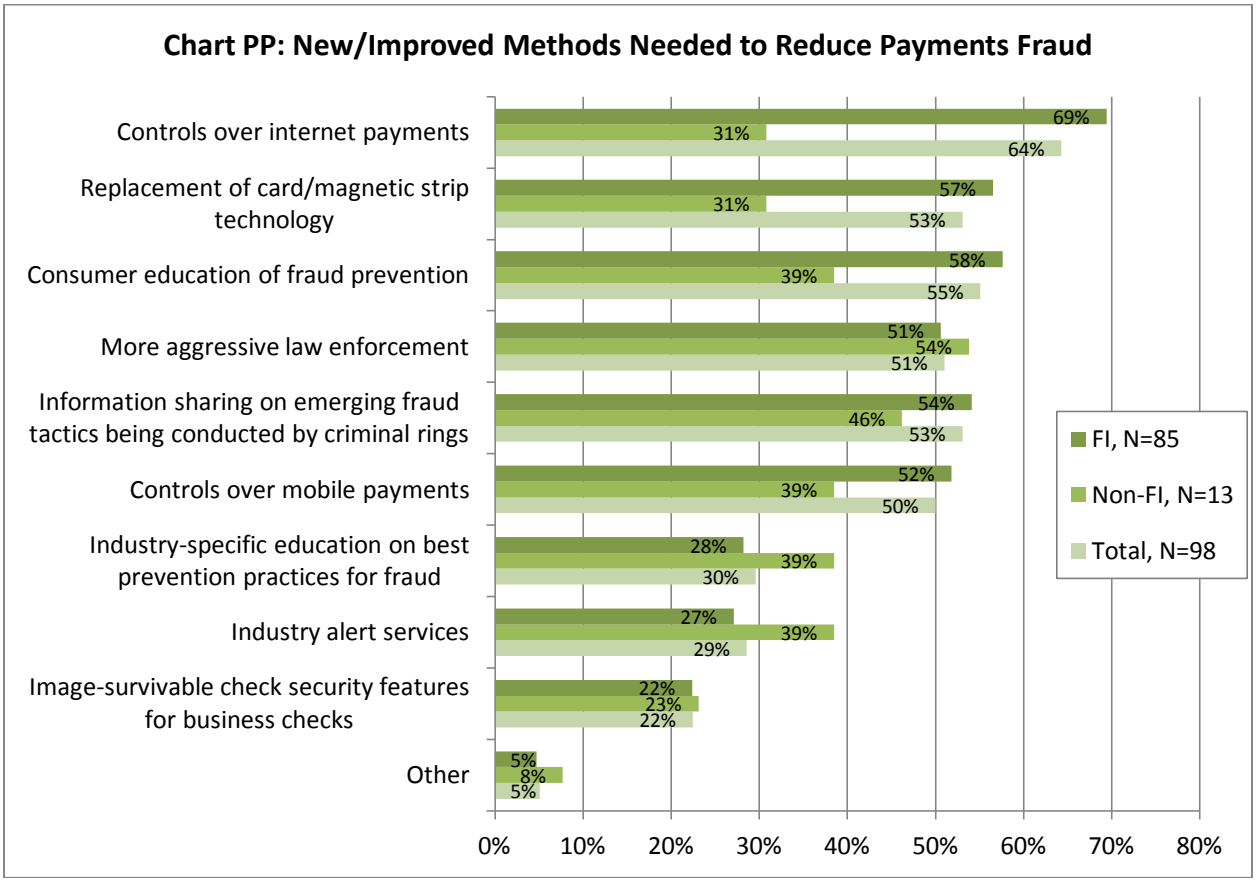


f. Opportunities to Reduce Payments Fraud

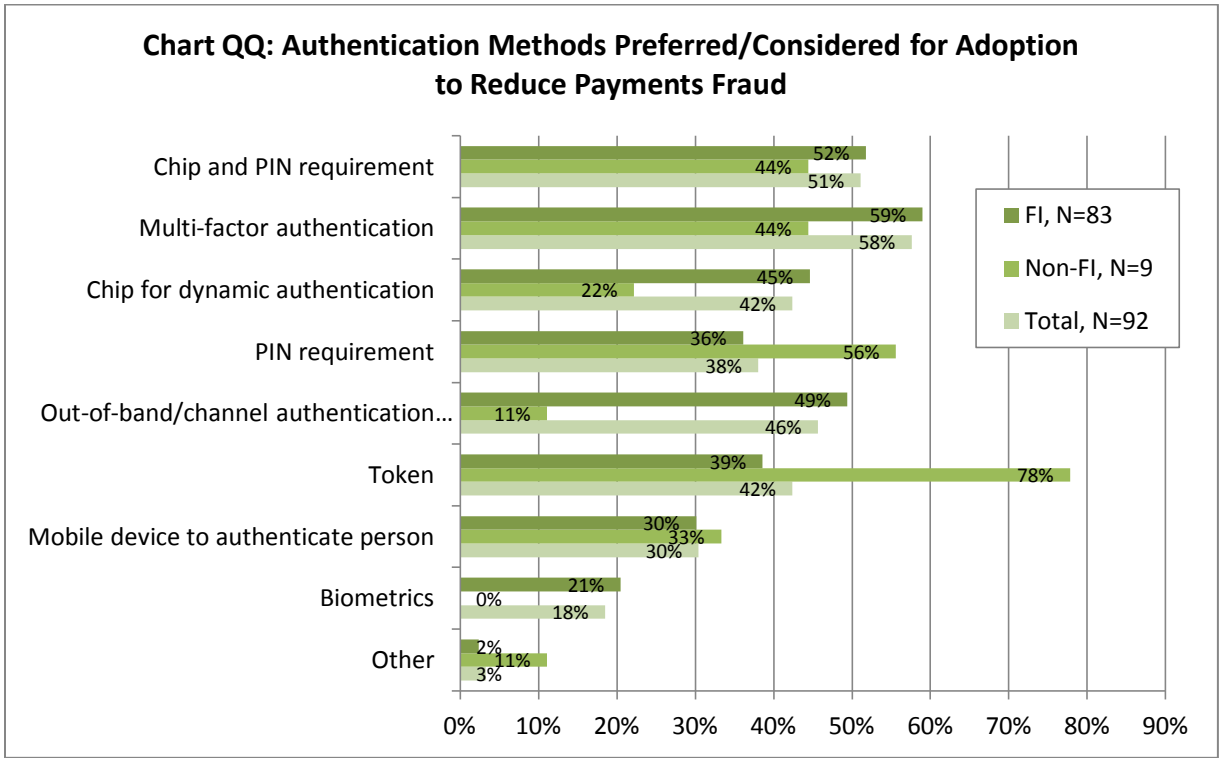
Respondents reported on opportunities to reduce fraud in three areas: i) organizational actions, ii) barriers to reducing payments fraud, and iii) legal and regulatory changes.

i. *Organizational Actions.* Respondents were asked what new or improved methods are most needed to reduce payments fraud (Chart PP). Nearly two-thirds of the respondents said their organizations should apply controls over Internet payments, while more than half of all respondents are in favor of replacement of card/magnetic stripe technology. The latter bodes well for the coming adoption of the EMV standards for card transactions in the U.S.[4]

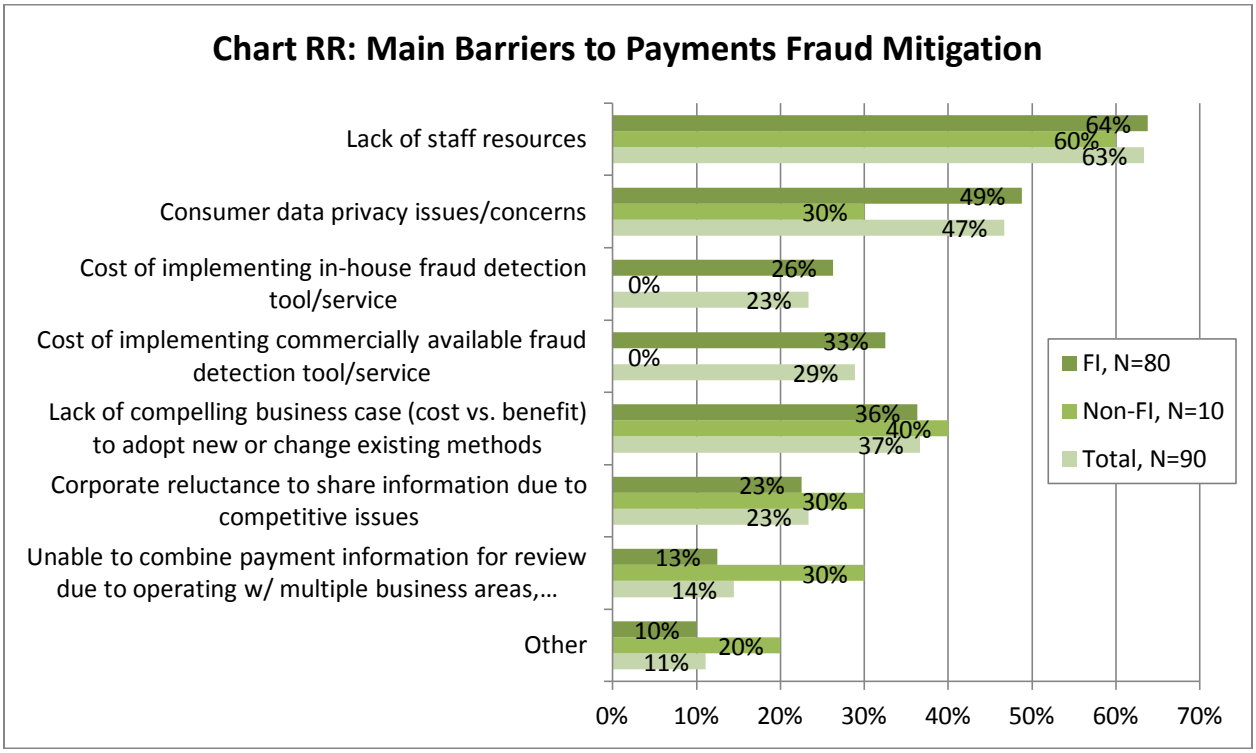
[4] See page 19.



When asked what authentication methods their organizations might prefer or consider adopting to help reduce payments fraud, the adoption of tokens led the way among non-financial institution respondents, while multifactor authentication was the top method among financial institution respondents. When viewed in total, approximately 58% of respondents were in favor of multifactor authentication (Chart QQ).



ii. Barriers to Reducing Payments Fraud. Respondents reported on barriers to further reducing payments fraud. Most identified a version of "cost" as the main barrier, citing lack of staff resources, implementation costs and lack of compelling business case as the main barriers. A complete summary is listed in Chart RR.



iii. ***Legal or Regulatory Changes.*** Respondents were also asked to offer views on legal and regulatory changes that would help reduce payments fraud. Many respondents would like to see increased penalties for fraud and more likely prosecution. Topping the list for FI respondents was placing more responsibility for fraud mitigation with—and shifting liability for fraudulent card payments to—the entity that initially accepts the card. This is interesting in light of the planned liability shifts that are part of the EMV "roadmaps" of all the major card associations (MasterCard, Visa, Discover and American Express). Table 2 lists these and other considerations.

Table 2: Legal and Regulatory Considerations by Percentage of Respondents

Legal and Regulatory Changes	FI (N=86)	FI (%)	Non-FS (N=13)	Non-FS (%)	Total (N=99)	Total (%)
Place responsibility to mitigate fraud and shift liability for fraudulent card payments to the entity that initially accepts the card payment	67	78%	3	23%	70	71%
Increase penalties for fraud and attempted fraud	63	73%	9	69%	72	73%
Place more responsibility on consumers and customers to reconcile and protect their payment data	63	73%	5	39%	68	69%
Assign liability for fraud losses to the party most responsible for not acting to reduce the risk of payment fraud	60	70%	5	39%	65	66%
Strengthen disincentives to committing fraud through stiffer penalties and more likely prosecution	49	57%	10	77%	59	60%
Improve law enforcement cooperation on domestic and international payments fraud and fraud rings	48	56%	8	62%	56	57%
Focus future legal or regulatory changes on data breaches to where breaches occur	44	51%	3	23%	47	47%
Align Regulation E and Regulation CC to reflect changes in check collection systems' use of check images and conversion of checks to ACH	39	45%	4	31%	43	43%
Assign responsibility for mitigating fraud risk to the party best positioned to take action against fraud	41	48%	2	15%	43	43%
Establish new laws/regs or change existing ones in order to strengthen the management of payments fraud risk	27	31%	5	39%	32	32%

h. Conclusions

Considered as a whole, the results of our 2012 payments fraud survey suggest the following:

- Both financial institutions and corporations of all sizes in the district continue to be concerned about payments-related fraud.

- Most problematic is fraud that affects checks and debit cards because these are the payment types that were most often attacked by fraud schemes and that sustained the highest losses as a result. These findings are generally consistent with fraud surveys conducted by national industry associations such as the Association for Financial Professionals (AFP).[5]

- Although fraud involving "corporate account take-over" has been highlighted in the press recently as a major problem, it was not cited as a significant scheme that affected respondents to this survey.

- Most financial institutions and other corporations report total fraud losses that represent less than .3% of their annual revenues. While any loss due to fraud is undesirable, by this measure these levels are relatively small.

[5] See http://www.afponline.org/fraud/

- Organizations are using various internal controls and procedures to mitigate payments fraud risk. Transaction monitoring, authentication, and risk services offered by financial institutions are also used.

- Lack of staff resources is the primary barrier cited by a majority of organizations when considering additional options for mitigating payments fraud risk.

