2012 Payments Fraud Survey Summary of Results

Responses from Members of the Financial and Retail Protection Association, Minnesota Association for Financial Professionals, Independent Community Bankers of America, Montana Chamber of Commerce, and the Upper Midwest Automated Clearinghouse Association

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

September 17, 2012

©2012 Federal Reserve Bank of Minneapolis

Table of Contents

© 2012 Federal Reserve Bank of Minneapolis

1. Introduction

In April and May 2012, the Federal Reserve Bank (FRB) of Minneapolis' Payments Information and Outreach Office conducted research on payments-related fraud experienced by area organizations.[1,2] Members of the Financial and Retail Protection Association, Minnesota Association for Financial Professionals, Independent Community Bankers of America, Montana Chamber of Commerce, and the Upper Midwest Automated Clearinghouse Association responded to an online survey about payments fraud their organizations experienced and methods used to reduce fraud risk. Payments covered in the survey included transactions involving cash, check, debit and credit cards, automated clearinghouse (ACH), and wire transfers. The 2012 survey is similar to surveys conducted in 2010 and 2009; thus this report includes some trend analysis.[3]

2. Respondent Profile Information

There were 246 respondents. Respondents are located in all six states in the Ninth Federal Reserve District (Michigan - 5%, Minnesota - 48%, Montana - 10%, North Dakota - 13%, South Dakota - 8%, and Wisconsin - 15%).

Ninety-two percent (226 respondents) are financial institutions (FI). Eight percent (20 respondents) are split among eight other industries as shown in Table 1.[4] The total number and mix of non-FI organizations that responded to the 2012 survey differs from past surveys. Since only a small number of respondent organizations are in industries other than financial services, this should be considered when interpreting 2012 results and year-to-year changes.

[1] Questions regarding the survey summary may be directed to Claudia Swendseid (Claudia.swendseid@mpls.frb.org) or Amanda Dorphy (Amanda.dorphy@mpls.frb.org) at the Federal Reserve Bank of Minneapolis.

[2] This survey was also part of a broader survey effort sponsored by the Federal Reserve Banks of Minneapolis, Boston, Dallas, and Richmond and the Independent Community Bankers of America. Reserve Banks are publishing regional survey results and highlights of the aggregate survey results will be available from the Federal Reserve Bank of Minneapolis website.

[3] In the 2012 survey, some data collected was specific to 2011, e.g., fraud loss rates, while other information collected is as of the survey date or April 2012, e.g., mitigation services respondents currently use. To simplify year-to-year comparisons in this report, 2011 is listed in the charts and tables even though some information may reflect a respondent status as of April 2012.

[4] Recruitment of survey respondents was accomplished through website communications and emails to members of the Financial and Retail Protection Association, Minnesota Association for Financial Professionals, Independent Community Bankers of America, Montana Chamber of Commerce, and the Upper Midwest Automated Clearinghouse Association. As with many studies, recruiting was not purely at random and those who responded may not be representative of the organizations located in the Ninth Federal Reserve District or the sponsoring associations' memberships.

© 2012 Federal Reserve Bank of Minneapolis

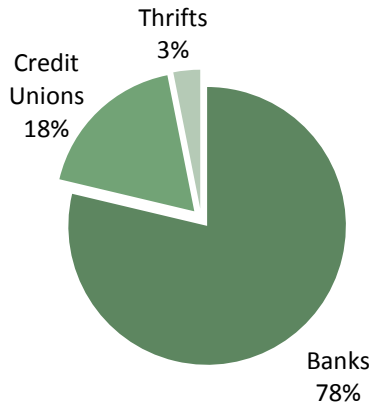
Table 1: Respondent Industry Classification by % of Respondents and Survey Year

Industry*	2012 (N=246)	2010 (N=206)	2009 (N=185)
Financial Institutions	92%	71%	74%
Government	2%	2%	3%
Manufacturing	2%	2%	8%
Health services	1%	1%	1%
Other	1%	13%	6%
Hospitality/Travel	1%	1%	1%
Other Financial Services	1%	2%	3%
Retail Trade	0.4%	6%	3%
Nonprofit	0%	3%	2%

*Percents by column exceed 100% due to rounding.

Many of the tables and charts in this report summarize survey responses of FI respondents. Banks represent the largest share (78%) of FI respondents followed by credit unions (18%) and thrifts (3%).

Chart A: Financial Institution Type



As one measure of size, all respondents were asked to categorize their organization's 2011 annual revenue, listed in Table 2. Just over half the organizations had 2011 annual revenue of less than $50 million. FI respondents were also asked their size based on total assets, as listed in Table 3. Forty-eight percent of the FI respondents are relatively small with total assets under $100 million.

© 2012 Federal Reserve Bank of Minneapolis

Table 2: Annual Revenue by % of Respondents (N=246)

Annual Revenue	2011			2010			2009
	FI	Non-FI	All Org.	FI	Non-FI	All Org.	All Org.
Under $50 million	56%	16%	53%	48%	48%	48%	40%
$50 - 99 million	12%	16%	12%	12%	2%	9%	14%
$100 - 249.9 million	9%	5%	9%	11%	8%	10%	10%
$250 - 499.9 million	5%	11%	6%	5%	6%	5%	5%
$500 - 999.9 million	2%	11%	2%	5%	6%	5%	4%
$1 - 4.9 billion	3%	21%	4%	7%	10%	8%	11%
$5 - 9.9 billion	1%	5%	1%	1%	3%	2%	1%
Over $10 billion	0%	11%	1%	3%	4%	4%	6%
Not applicable	12%	0%	11%	1%	11%	4%	10%
Don't know	1%	5%	2%	7%	2%	5%	

Table 3: Total Assets Year-End 2011 by % of Financial Institution Respondents (N=226)

Total Assets as of Year-End 2011	% of Financial Institutions
Under $50 million	24%
$50 - 99 million	24%
$100 - 249.9 million	28%
$250 - 499.9 million	12%
$500 - 999.9 million	5%
$1 - 4.9 billion	4%
$5 - 9.9 billion	3%
$10 billion or more	0.4%

© 2012 Federal Reserve Bank of Minneapolis

3. Summary of Survey Results by Questions

This section summarizes survey responses by question. Where differences are relevant, responses of FIs are reported separately from all others.

a. Payment Types Used by Non-Financial Institution Respondents

Table 4 shows the typical counterparties, businesses including government entities and/or consumers, associated with an organization's payments. Charts B and C show the different payment types accepted and used for disbursements.

Table 4: Typical Payment Counterparties Associated with Organization's Payments Volume by % of Non-Financial Institution Respondents (N=19)

Payment Counterparties	%
Payments to/from both consumers and businesses	55%
Payments primarily to/from other businesses	45%
Payments primarily to/from consumers	0%

Chart B: Payment Types Accepted by % of Non-Financial Institution Respondents (N=20)

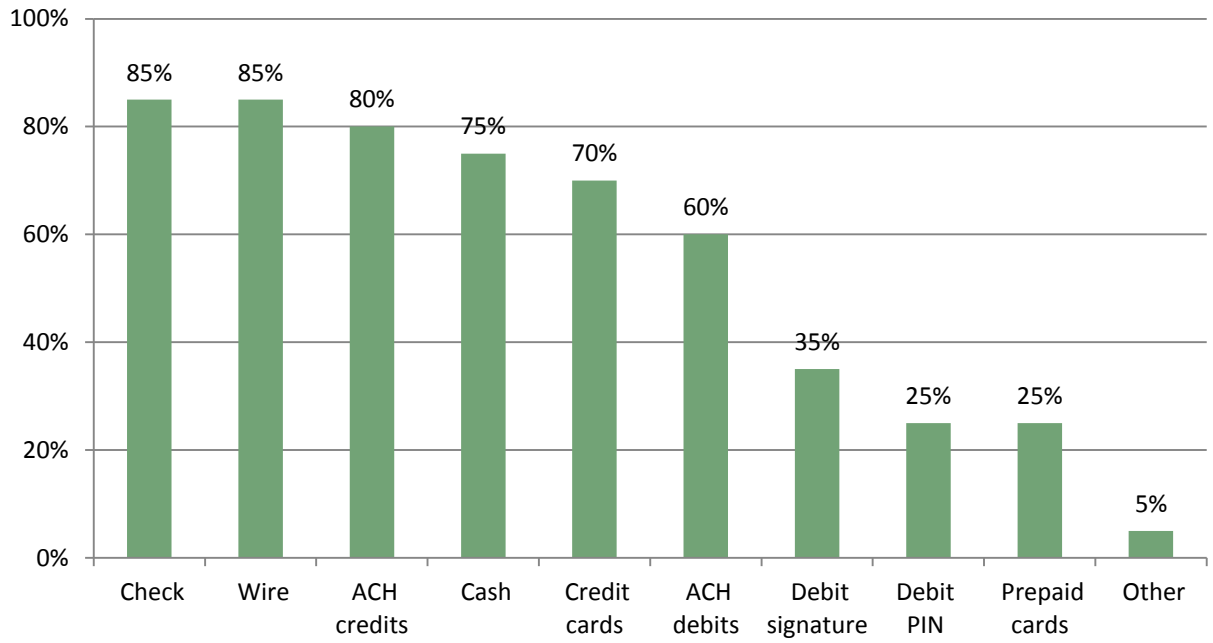
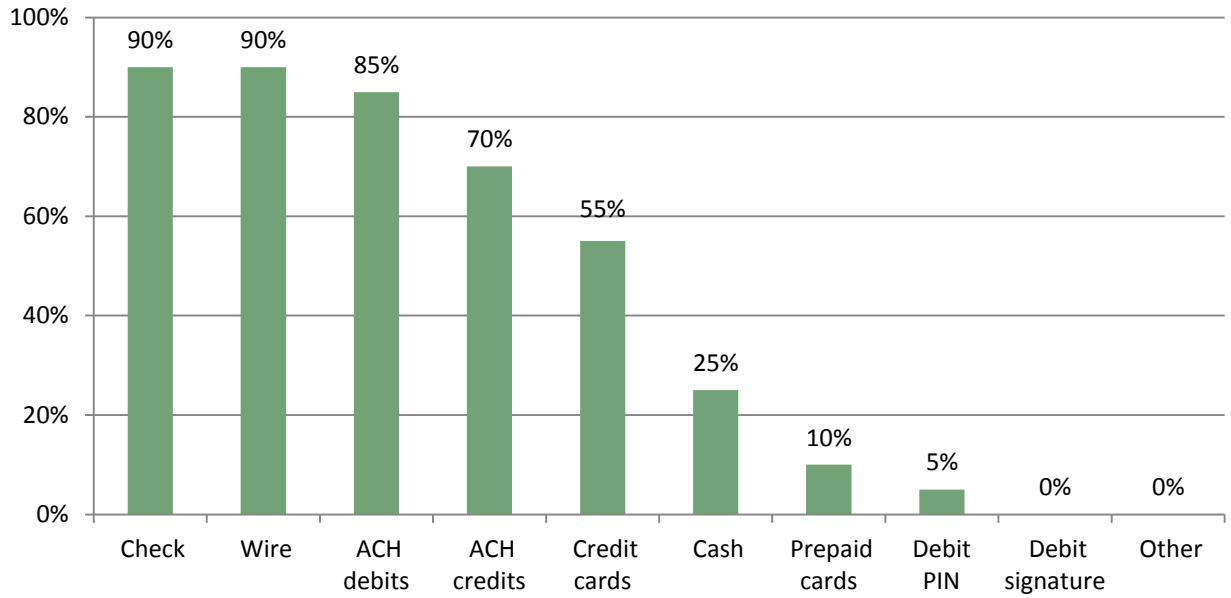


Chart C: Payment Types Used for Disbursement by % Non-Financial Institution Respondents (N=20)



b. Payment Products Offered by Financial Institution Respondents

Table 5 indicates the type of customers typically targeted by the payment products offered by FI respondents. The customer base varies by the type of financial institution with 92% of banks offering these products to both consumers and businesses, whereas 78% of credit unions primarily offer payment products to consumers only.

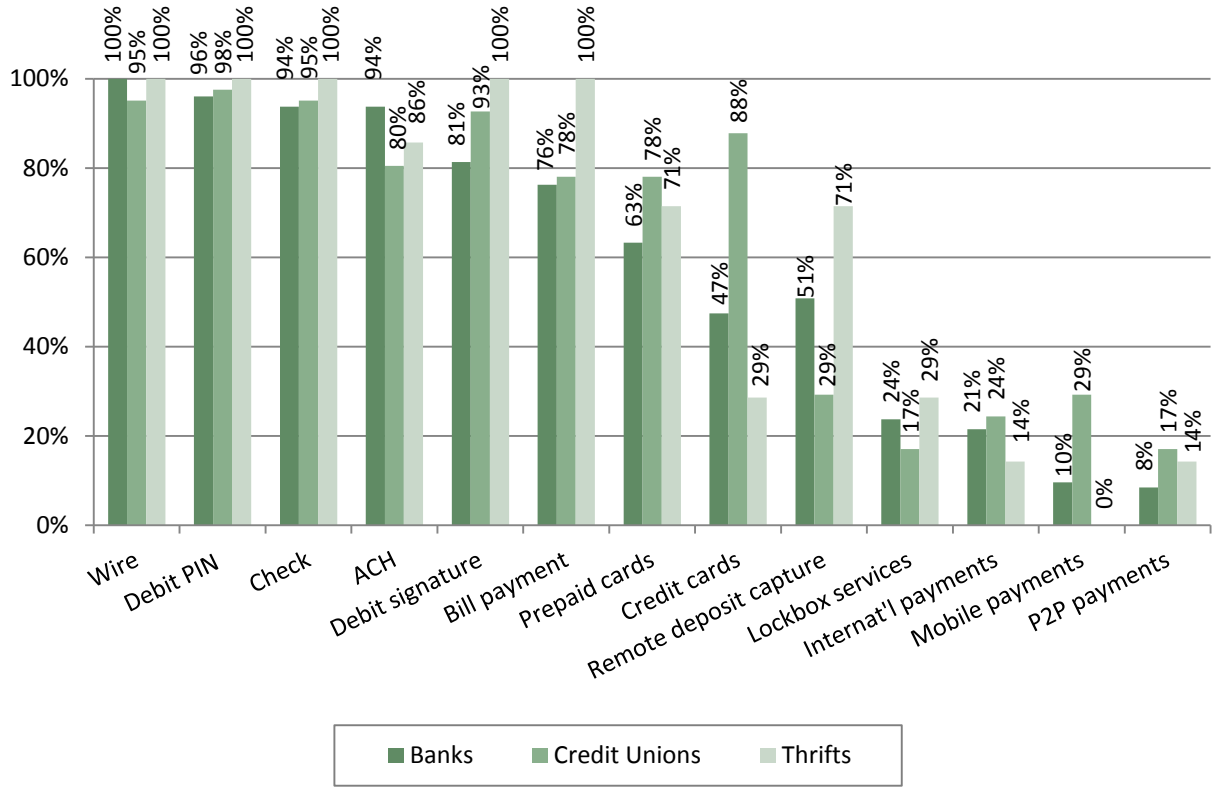
Almost all FIs offer wire transfer, PIN debit and check products as shown in Chart D. Two-thirds offer seven of the thirteen payments products. A higher percent of credit unions offer credit cards, mobile payments and prepaid cards, which may reflect their focus on consumers.

Table 5: Type of Customers to Whom Financial Institution Typically Offers Its Payment Products and Services by % of Financial Institution Respondents

Target Customers	Banks (N=177)	Credit Unions (N=41)	Thrifts (N=7)
Both consumers and business or commercial clients	92%	22%	57%
Primarily consumers	5%	78%	43%
Primarily business or commercial clients	3%	0%	0%

© 2012 Federal Reserve Bank of Minneapolis

Chart D: Payment Products and Services Offered by % of Financial Institution Respondents



c. Payments Fraud Attempts and Financial Losses

Six percent of all respondents reported no payments fraud attempts in 2011 (4% of the FI respondents and 37% of non-FI respondents). Of those that experienced fraud attempts, four out of five FIs reported signature debit card as one of the top three payment types with the highest number of fraud attempts, followed by fraud attempts using checks, and third by PIN debit cards (Chart E). Notably, the percent of FIs reporting signature debit card fraud attempts are more than double the percent of FIs reporting PIN debit. Also, these top three payment types for fraud attempts are the same between 2010 and 2011. For non-FI respondents, check fraud attempts were highest, followed by credit cards and ACH debits as reported in Chart F. For both groups, the percent of respondents reporting ACH debit fraud attempts increased from 2010 to 2011 and decreased for ACH credits.

© 2012 Federal Reserve Bank of Minneapolis

Chart E: Top 3 Payment Types with Highest Number of Fraud Attempts by % of Financial Institution Respondents

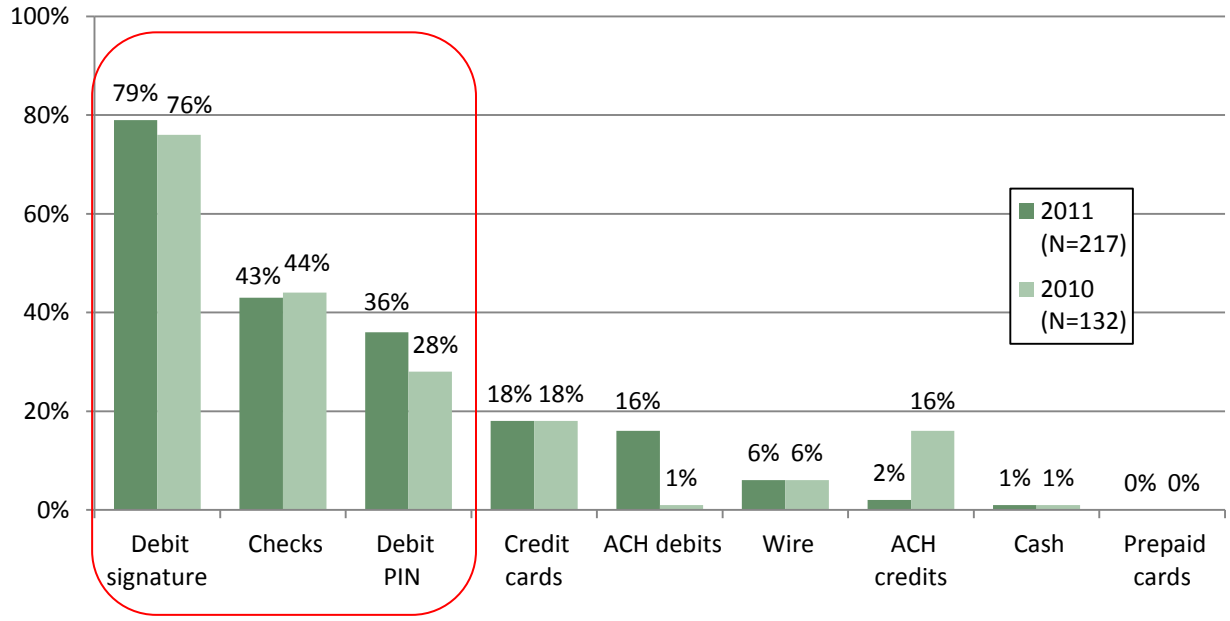
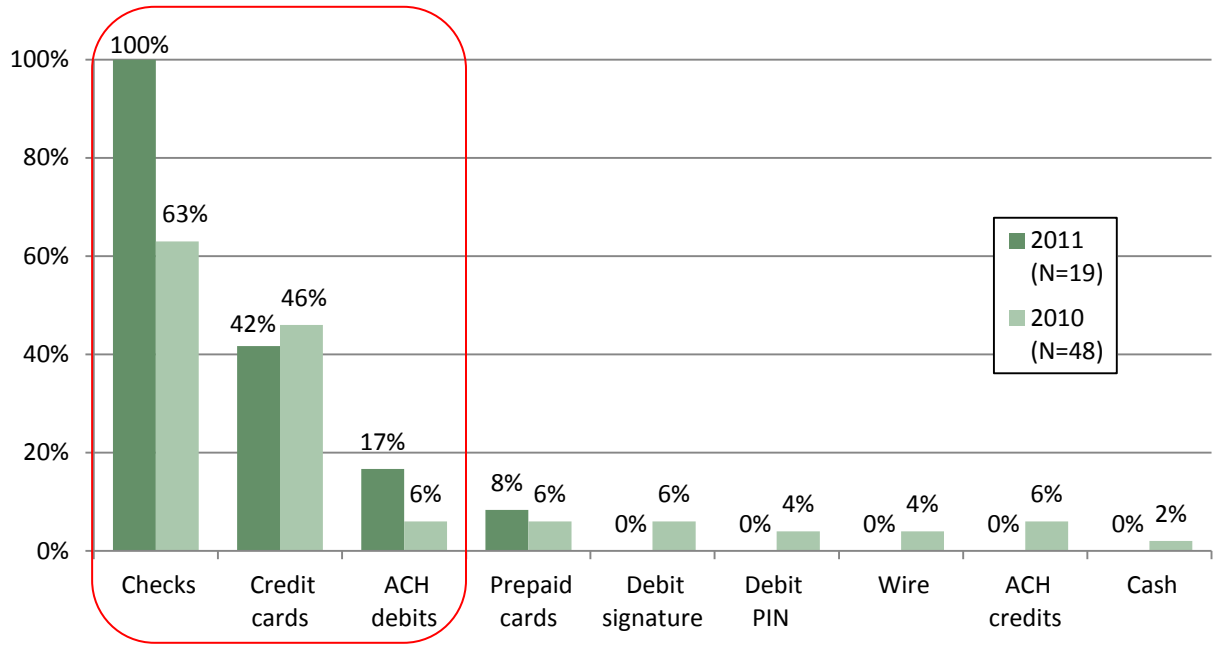


Chart F: Top 3 Payment Types with Highest Number of Fraud Attempts by % of Non-Financial Institution Respondents



Over 90% of all respondents reported dollar losses due to payments fraud in 2011. Of those that experienced fraud losses, 86% of the FI respondents identified signature debit cards among the top three payments with the highest dollar losses, followed by PIN debit cards and check reported by 38% (Chart G). In contrast, non-FI respondents identified check among the top three payments with the highest dollar losses (78% non-FIs), followed by credit cards and ACH debits as reported in Chart H.

© 2012 Federal Reserve Bank of Minneapolis

Thus, the payment types with highest dollar losses due to fraud are the same as those with the highest fraud attempts.

Chart G: Top 3 Payment Types with Highest Dollar Losses Due to Fraud by % of Financial Institution Respondents

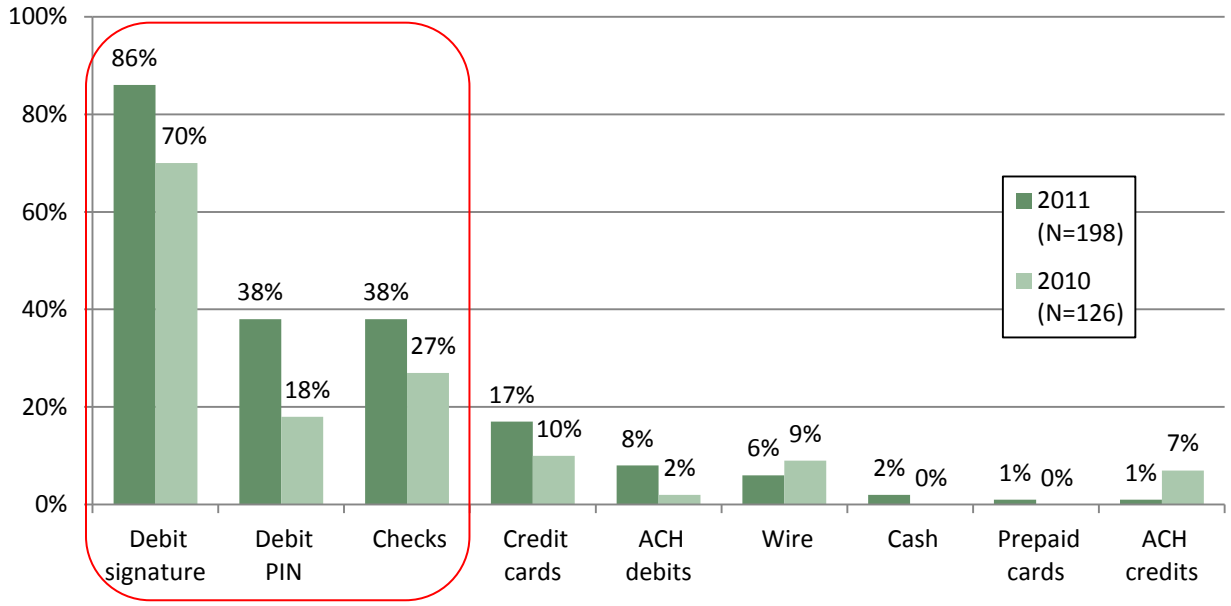
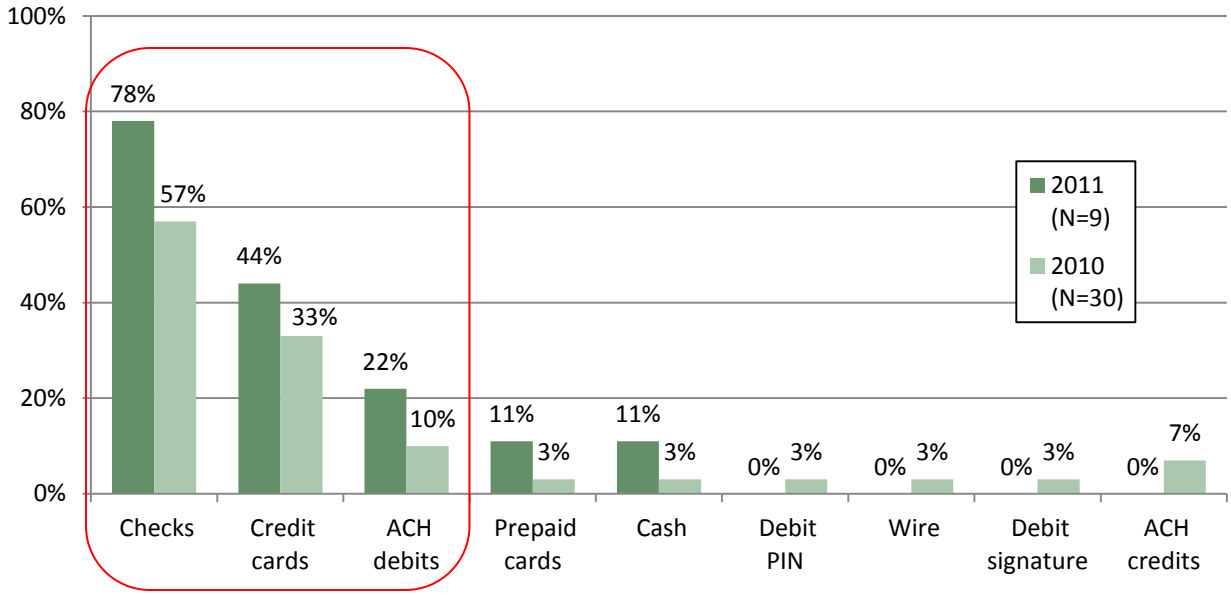


Chart H: Top 3 Payment Types with Highest Dollar Losses Due to Fraud by % of Non-Financial Institution Respondents



© 2012 Federal Reserve Bank of Minneapolis

For each payment type, respondents were asked whether fraud prevention costs or actual fraud losses were a greater expense for their organization as shown in Charts I and J. Fifty-five percent of the FIs reported actual losses on signature debit cards exceed prevention costs; likewise 40% reported the same relationship for checks and PIN debit. All three of these payment types are offered by most FIs and experienced the highest fraud attempts and losses. This seems to indicate that some FIs would benefit from increased investments in payments fraud mitigation as their losses are currently higher than prevention investments.

For non-FI respondents, actual fraud losses on prepaid cards and mobile payments exceeded expenses in fraud loss prevention. Here too, the data may suggest the need for increased investments in fraud prevention for these payment types. However, less than 30% of respondents use these payments.

Chart I: Fraud Prevention Costs Versus Actual Fraud Losses by % of Financial Institution Respondents (N=202)

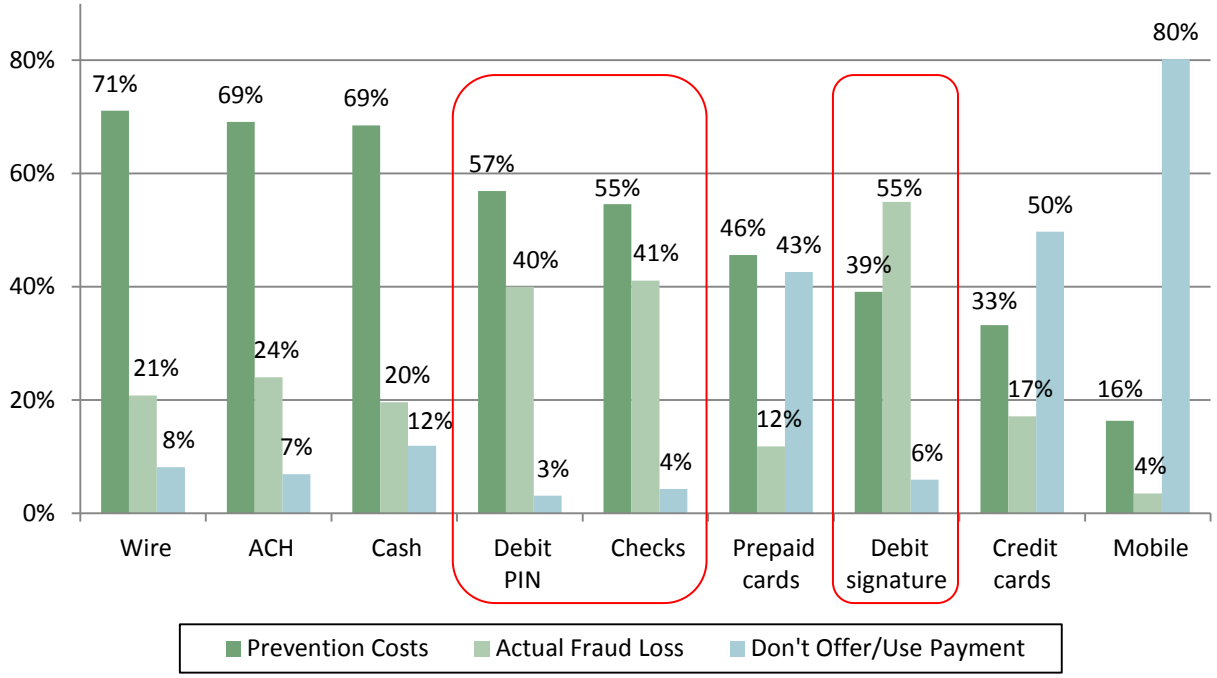
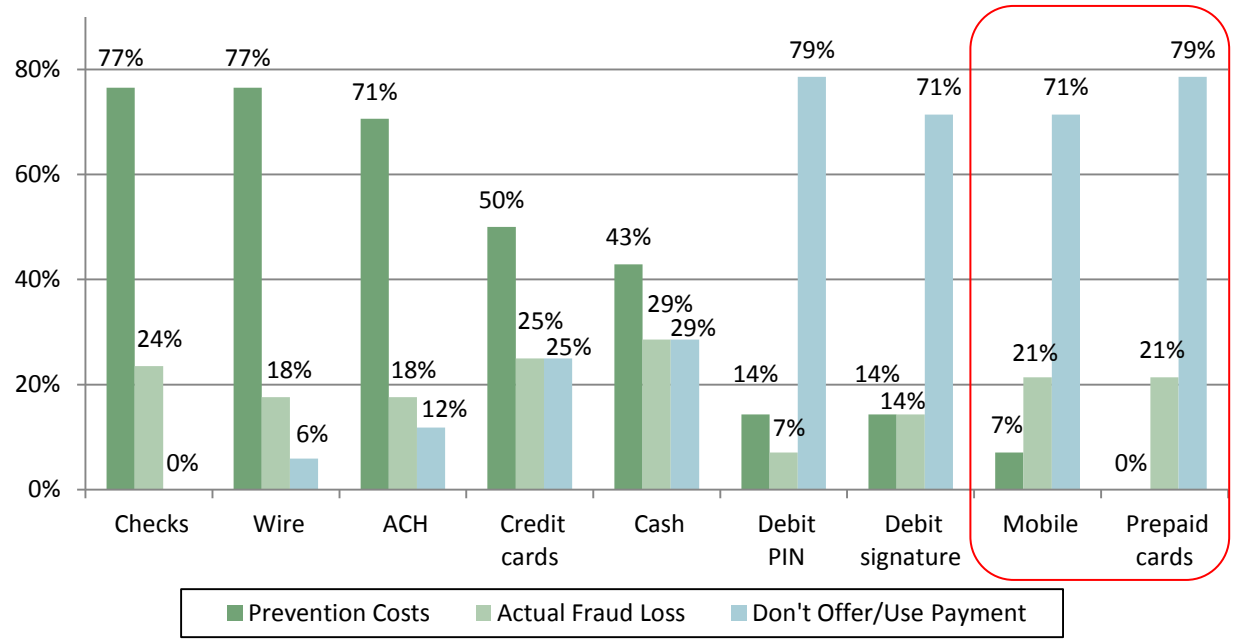


Chart J: Fraud Prevention Costs Versus Actual Fraud Losses by % of Non-Financial Institution Respondents (N= 17)



Bottom line, payment fraud attempts and losses remain widespread in 2011, particularly against financial institutions. Thus, investments in fraud prevention also remain important, but are not likely to eliminate fraud losses all together. Prevention investments should be considered within a benefit/cost framework that weighs the cost of investment against the cost of fraud losses.

For organizations that experienced fraud losses, over 90% estimated losses as 0.5% or less of their annual revenue (Table 6) and about 80% selected the lowest range of loss, or less than 0.3% of annual revenues. No respondents reported 2011 losses in the highest loss range or over 5%.

Table 6: Payments Fraud Financial Losses by % of Respondents Incurring Losses

Loss Range as a Percent of Annual Revenue	Financial Institutions		Non-Financial Institutions		All Respondents	
	2011 (N=194)	2010 (N=120)	2011 (N=9)	2010 (N=28)	2011 (N=203)	2010 (N=148)
>0% - .3%	79%	82%	67%	75%	78%	80%
.3% - .5%	14%	11%	0%	11%	13%	11%
.6% - 1%	5%	3%	11%	4%	5%	3%
1.1% - 5%	2%	3%	22%	7%	3%	4%
Over 5%	0%	2%	0%	4%	0%	2%

© 2012 Federal Reserve Bank of Minneapolis

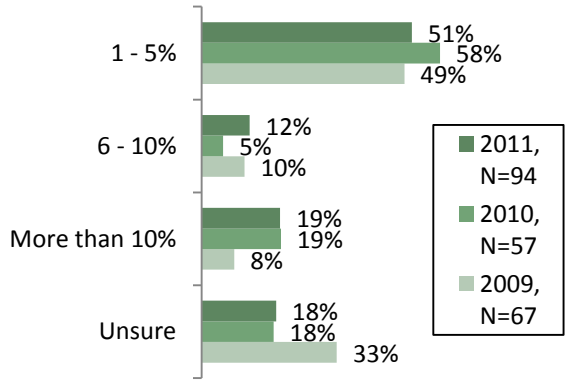
Forty-three percent of respondents reported an increase in fraud losses in 2011 compared to 2010 (Table 7). Improvements in year-to-year changes in fraud losses differed between FIs and non-FIs. FI percentages remained about the same over the last three years in terms of those reporting an increase in financial loss due to payments fraud (~46%), no change (~41%), or a decrease (~13%). Changes to fraud losses experienced by non-FI respondents seems to show some improvement compared to prior years. Zero percent of non-FIs reported an increase in their 2011 financial losses versus 2010, which continues a decline since 2009; 72% stayed about the same, and the rest (28%) reported a decrease.[5]

Table 7: Change in Payments Fraud Losses Compared to Previous Years by % of Respondents

% of Respondents	FI Respondents			Non-FI Respondents			All Respondents		
	2011 N=208	2010 N=131	2009 N=137	2011 N=18	2010 N=53	2009 N=38	2011 N=226	2010 N=184	2009 N=185
Increased	46%	45%	50%	0%	11%	27%	43%	35%	44%
Stayed the same	41%	42%	41%	72%	79%	50%	44%	53%	43%
Decreased	13%	13%	9%	28%	9%	23%	14%	12%	12%

FIs that reported an increase in 2011 fraud losses were asked to estimate the percentage increase in their fraud loss rate (Chart K). Over half cited an increase of 1% to 5% and about 20% estimated an increase of 10% or more. Note, however, that despite these increases, the total loss estimated as a percentage of revenues remains relatively low for the vast majority of respondents.

Chart K: Percent Increase in Loss Rate by % of Financial Institutions with Increased Losses

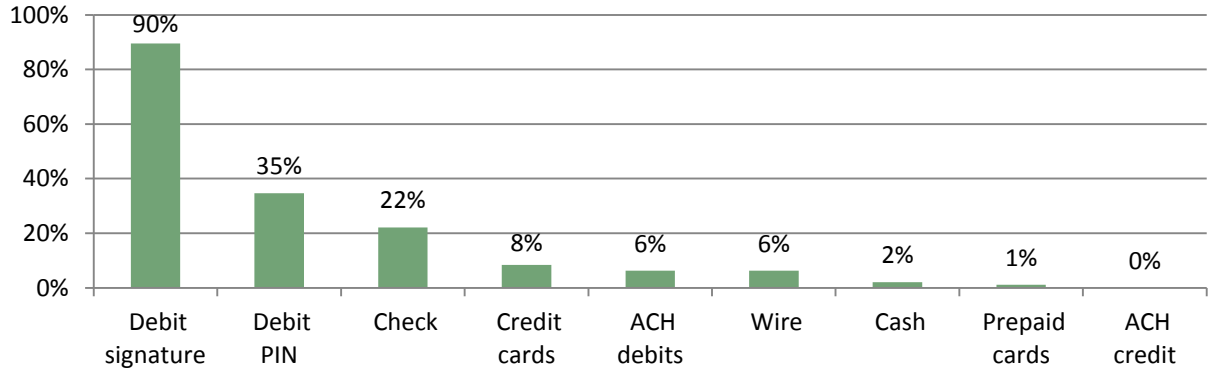


FIs with an increase in 2011 fraud losses were also asked to identify one or more payment types associated with the increased loss (Chart L). Ninety percent of FIs attributed increased losses to signature debit cards, compared to a third that identified PIN debit cards, and 20% that identified checks. These same payment types were reported by FIs as having the highest number of fraud attempts and losses.

[5] As noted above, the number of non-FI respondents in the survey is small at 20 organizations.

© 2012 Federal Reserve Bank of Minneapolis

Chart L: Payment Types Attributed to 2011 Fraud Loss Increase by % of Financial Institutions with Increased Losses (N=95)



Respondents that experienced a decrease in fraud losses in 2011 compared to 2010 (14%) were asked to estimate the percentage decrease in their loss rate (Charts M and N). About half estimated a 1% to 5% reduction in fraud losses and another 40% were unsure about the size of the decrease.

Chart M: Percent Decrease in Loss Rate by % of Financial Institutions with Decreased Losses

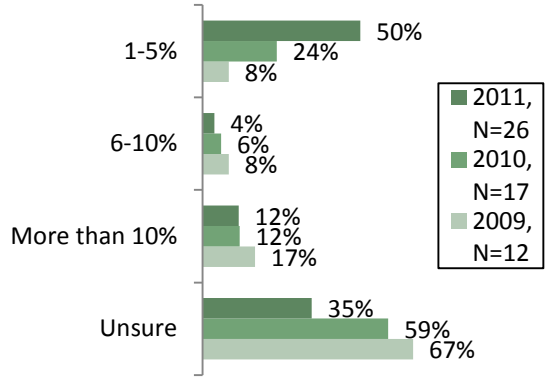
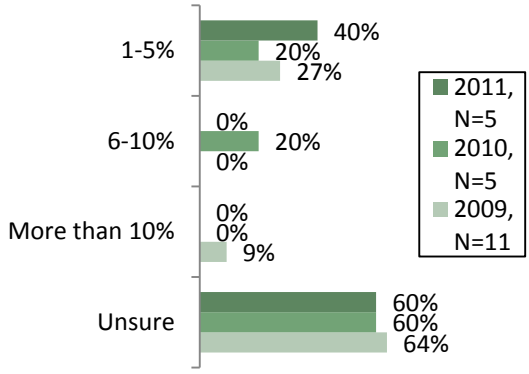


Chart N: Percent Decrease in Loss Rate by % of Non-Financial Institutions with Decreased Losses



These same respondents identified one or more payment types associated with the decrease in fraud losses (Charts O and P). Seventy-five percent of the FIs identified signature debit cards and about a third identified PIN debit cards. Non-FI respondents attributed their decrease in losses to credit cards and ACH debit payments. Although check is among the top three payment types for fraud losses, only 13% of the respondents (12% of FIs and 20% of non-FIs) attributed their decrease in losses to check.

© 2012 Federal Reserve Bank of Minneapolis

Chart O: Payment Types Attributed to 2011 Fraud Loss Decrease by % of Financial Institutions with Decreased Losses (N=25)

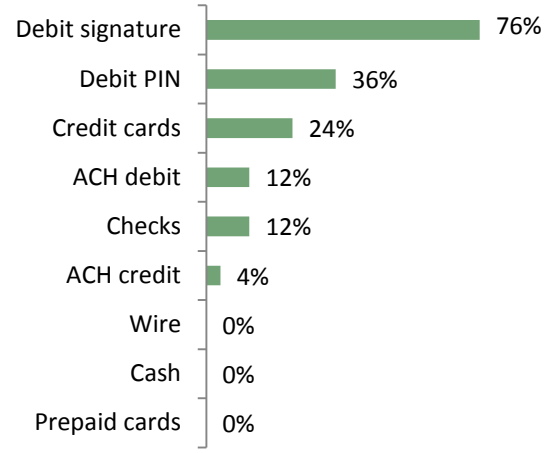
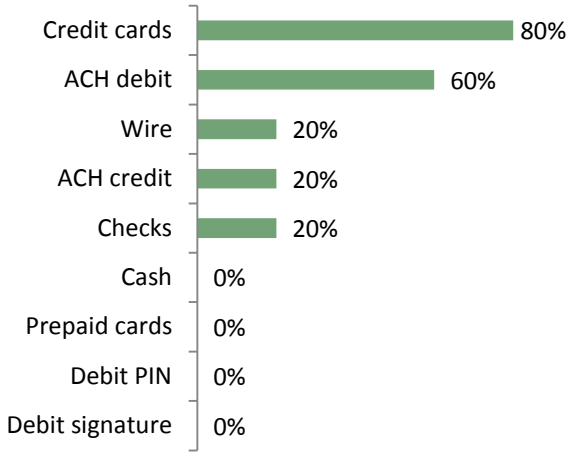


Chart P: Payment Types Attributed to 2011 Fraud Loss Decrease by % of Non-Financial Institutions with Decreased Losses (N=5)



Sixty-one percent of the respondents with a decrease in 2011 fraud losses attribute this to changes in payments risk management practices (Table 8). Two-thirds of these respondents identified enhanced fraud monitoring systems and staff training and education as among the risk management changes they made to reduce fraud losses (Table 9). This may suggest an opportunity for all organizations interested in reducing fraud losses to consider implementing similar measures.

Table 8: Implemented Changes to Payment Risk Management Leading to a Decrease in Fraud Losses by % of Respondents with Decreased Losses

Changes in Risk Management Practices Led to Fraud Loss Decrease	Financial Institutions N=26	Non-Financial Institutions N=5	All Respondents N=31
Yes	62%	60%	61%
No	39%	40%	39%

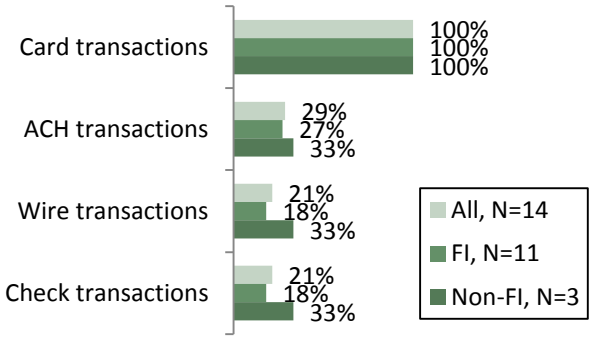
Table 9: Key Changes Made to Payment Risk Management Practices by % of Respondents

Areas of Change	Financial Institutions N=16	Non-Financial Institutions N=3	All Respondents N=19
Enhanced fraud monitoring system	69%	100%	74%
Staff training and education	63%	100%	68%
Enhanced internal controls and procedures	38%	100%	47%
Adopted/increased use of risk management tools offered by organization's financial institution or financial service provider	38%	100%	47%
Enhanced method to authenticate customer and/or validate customer account	13%	100%	26%

© 2012 Federal Reserve Bank of Minneapolis

All respondents that enhanced their fraud monitoring systems applied these to monitoring card transactions (Chart Q). Two-thirds that made these enhancements applied them exclusively to card transactions.

Chart Q: Payments to Which Enhanced Fraud Monitoring Applies



d. Perpetrators Involved in Successful Payments Fraud

Respondents reported that external parties were most often responsible for successful fraud attempts (Table 10); with 52% of respondents attributing all successful fraud attempts to external parties—a decrease of 12% compared to 2010 survey results. Consistent with 2010, another 14% of respondents could not determine the type of perpetrators involved in any of the successful fraud attempts. However, frauds involving internal parties increased. In total, 8% of respondents reported that all successful fraud involved internal parties (4%) and internal with external parties (4%) compared to a total of 2% in 2010. Finally, about 25% of respondents blamed a mix of perpetrators. Again respondents reporting some portion of fraud involved internal parties increased in 2011.

Table 10: Successful Fraud by Perpetrators Involved by % of Respondents (N=207)

Portion of Successful Payments Fraud by Perpetrators Involved					
Perpetrators	**100%**	**76-99%**	**51-75%**	**26 - 50%**	**1-25%**
Internal Only	4%	3%	3%	5%	3%
Internal w/External	4%	0%	1%	6%	4%
External Only	52%	7%	2%	4%	5%
Could Not Determine	14%	1%	1%	2%	8%

75% of respondents attributed all successful fraud to a single perpetrator category.

25% of respondents attributed a portion of successful fraud to more than one perpetrator category.

© 2012 Federal Reserve Bank of Minneapolis

e. Most Common Fraud Schemes

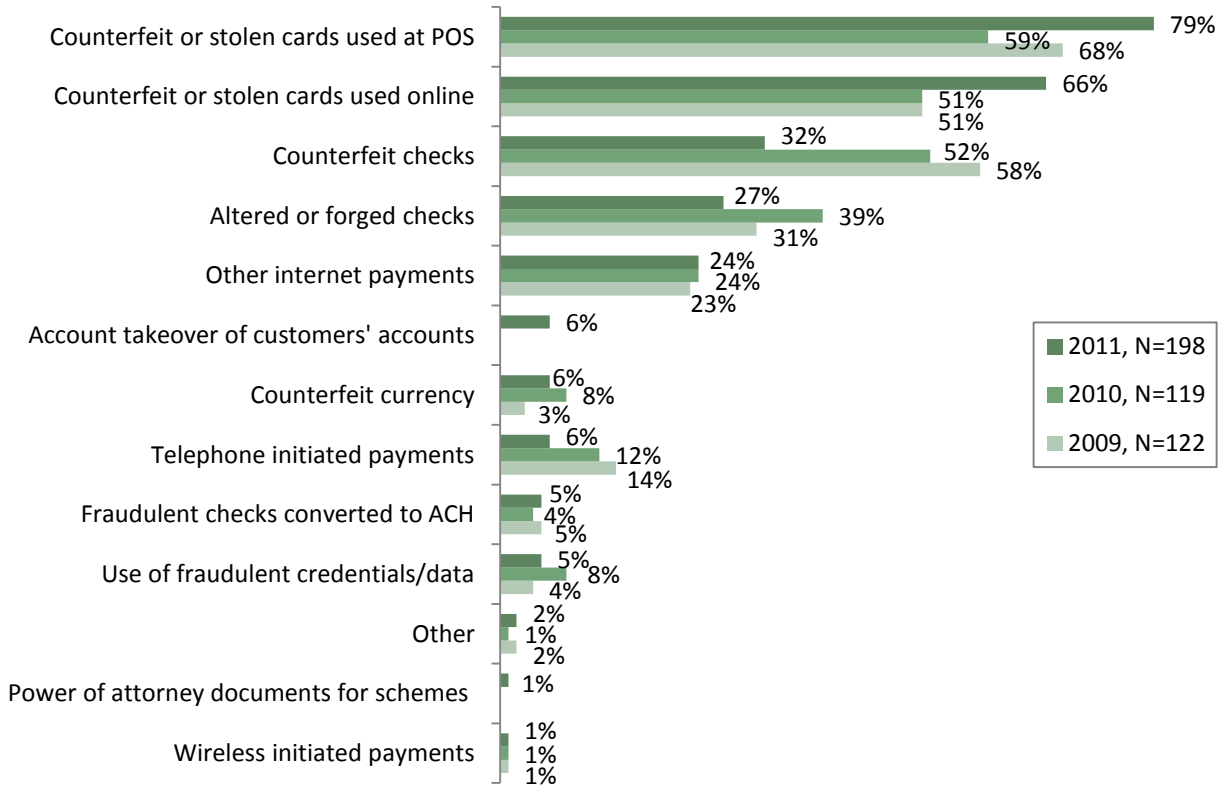
Questions were asked about the top three schemes most often used to initiate payments fraud in three areas:

- payments by or on behalf of FIs' customers (Chart R),
- payments received/accepted by non-FIs (Chart S), and
- payments against the respondent's own banking accounts (Charts T and U).

For the third consecutive survey, FIs identified counterfeit and stolen cards used at both the point-of-sale (POS) and online and counterfeit checks in general as the top three fraud schemes used involving payments by or on behalf of the FIs' customers. Over two-thirds of the FIs reported the former two schemes and a third reported counterfeit checks as the most used scheme. Notably, the total percentage that reported counterfeit checks as a most common scheme declined in 2011 and 2010.

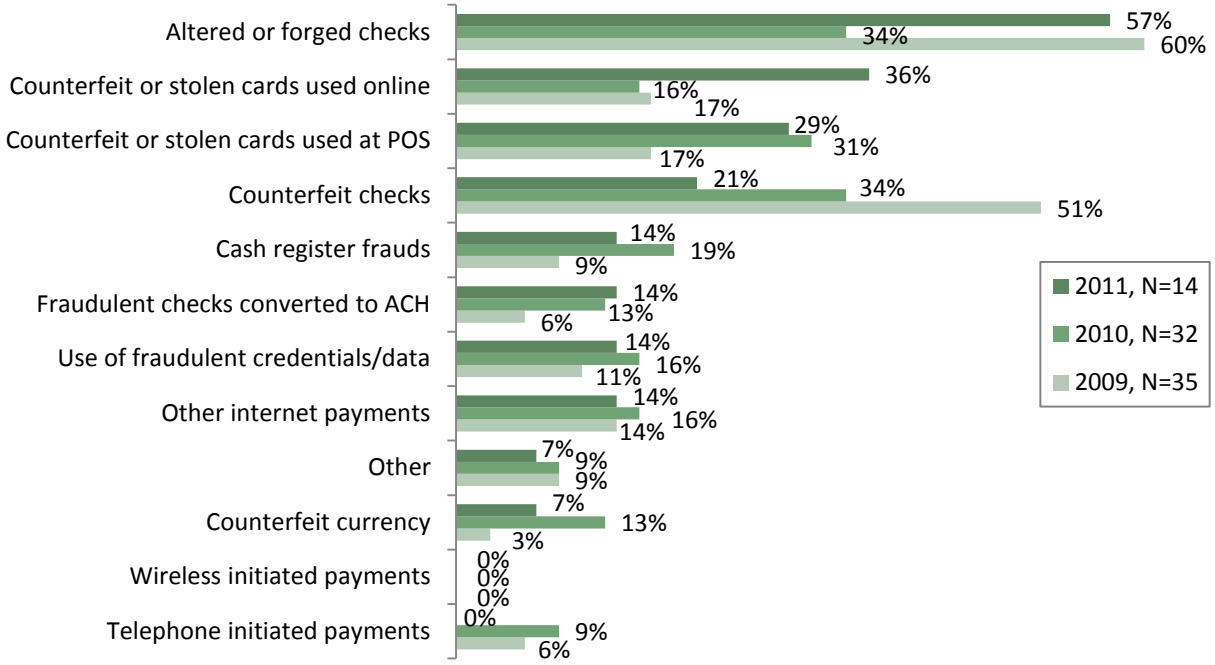
Fifty-seven percent of non-FI respondents reported altered or forged checks in the top three schemes most often used involving payments received or accepted, followed by counterfeit or stolen cards used online (36%) and at POS (29%). Similar to FIs, non-FIs report a 30% decline in counterfeit checks in 2011 compared to 2009 (Chart S).

Chart R: Top 3 Current Fraud Schemes Most Often Used Involving Payments by or on Behalf of Financial Institutions' Customers by % of Financial Institution Respondents



© 2012 Federal Reserve Bank of Minneapolis

Chart S: Top 3 Current Fraud Schemes Most Often Used Involving Payments Received/Accepted by % of Non-Financial Institution Respondents



Thirty-one percent of respondents (33% of FIs and 8% of non-FIs) reported no fraud attempts against their organizations own banking accounts. This is an improvement over 2009, when 11% of FI respondents and 3% of non-FI respondents reported no fraud against their organization's own accounts.

Respondents that reported fraud against their own accounts identified the most used schemes as fraudulent or unauthorized ACH debits, altered or forged checks, and counterfeit checks (Charts T and U). For FIs, the percent of respondents reporting altered or forged checks and counterfeit checks in the top three schemes declined between 2010 and 2011 from 48% to 38% and from 51% to 34%, respectively (Chart T).

As shown in Chart U, non-FI respondents continued to report check-related fraud in the top three schemes used against the organization's own accounts. The percent of non-FIs reporting fraudulent or unauthorized ACH debits and card transactions as most used schemes, declined between 2010 and 2011 from 31% to 27% and from 38% to 27%, respectively. Nine percent of non-FI respondents identified most used schemes as a breach of access or other security controls to their payment processes, including account takeovers, an increase over the 2010 level of 3%.

© 2012 Federal Reserve Bank of Minneapolis

Chart T: Fraud Schemes Involving Organization's Own Accounts by % of Financial Institution Respondents

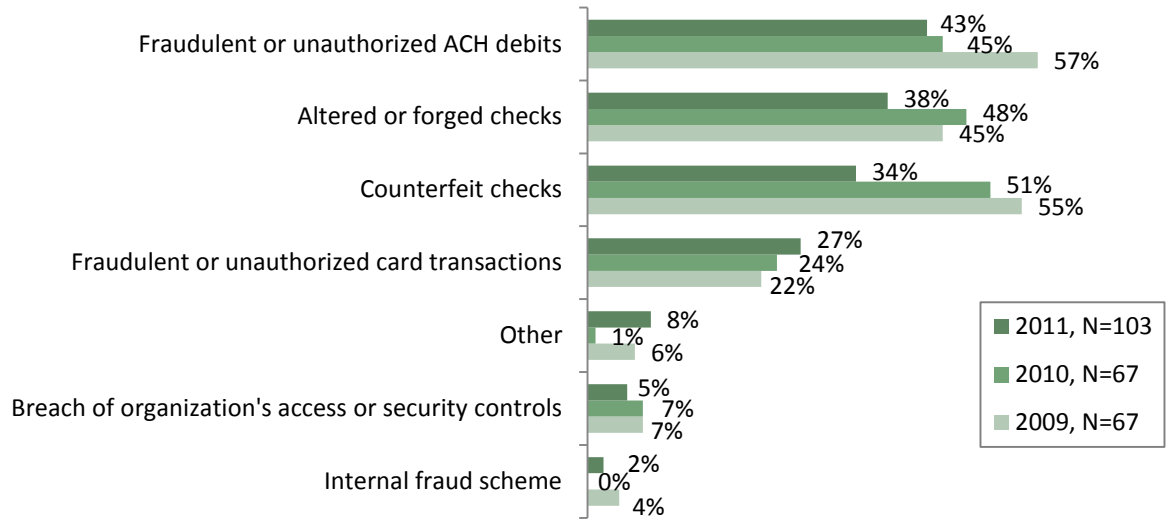


Chart U: Fraud Schemes Involving Organization's Own Accounts by % of Non-Financial Institution Respondents

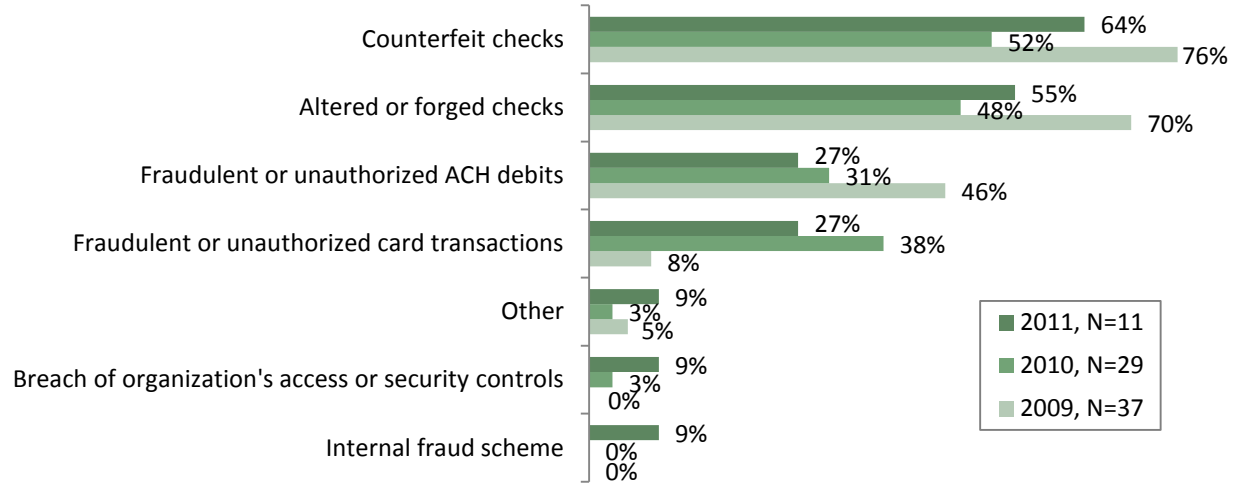


Table 11 lists the top three sources of information used in the most common fraud schemes. Nearly two-thirds of respondents identified "sensitive" information obtained from a lost or stolen card, check or other physical document or device while in the consumer's control. About a third of respondents reported physical device tampering and email or webpage cyber attacks as the source of information used to commit payments fraud.

© 2012 Federal Reserve Bank of Minneapolis

Table 11: Top 3 Information Sources Used in Fraud Schemes

Information Sources	FI 2011 N=181	FI 2010 N=107	Non-FI 2011 N=13	Non-FI 2010 N=30	All 2011 N=194	All 2010 N=137
"Sensitive" information obtained from lost or stolen card, check, or other physical document or device while in consumer's control	60%	54%	62%	30%	62%	49%
Physical device tampering, e.g., use of skimmer on POS terminal or obtaining magnetic stripe information	35%	41%	8%	3%	34%	33%
Email/webpage cyber attacks, e.g., phishing, spoofing and pharming, to obtain "sensitive" customer info.	31%	49%	31%	17%	32%	42%
Information about customer obtained by family/friend	27%	19%	0%	20%	26%	19%
Data breach due to computer hacking or cyber attacks	23%	6%	0%	3%	22%	5%
Organization's information obtained from a legitimate check issued by your organization	15%	22%	69%	53%	19%	29%
Lost or stolen physical documentation or electronic devices while in control of the organization	4%	8%	8%	0%	5%	7%
Employee with legitimate access to organization or customer information (employee misuse)	1%	1%	8%	23%	2%	6%

f. Payments Fraud Mitigation Strategies

Respondents were asked about their use and the effectiveness of various types of fraud mitigation methods and tools in four areas: i) internal controls and procedures, ii) customer authentication methods, iii) transaction screening and risk management methods, and iv) risk mitigation services offered by FIs. Strategies to detect and prevent fraud effectively require the use of various mitigation methods and tools. However, the most frequently used methods were not necessarily the most effective.

i. ***Internal Controls and Procedures.*** Internal controls and procedures are the fraud mitigation methods most used by respondents. Over 80% of respondents use nine or more of the 15 internal controls and procedures listed on Charts V and W below. The effectiveness of internal controls is rated highly by users, with over 95% of respondents rating each method as very or somewhat effective and 70% of respondents rating the majority as very effective.

   Change in use rates by FIs since 2009 are small for most of the procedures and controls. Increased use of over 5% was reported for "reconcile bank accounts daily," "use of an employee

© 2012 Federal Reserve Bank of Minneapolis

hotline to report potential fraud" and "set transaction limits for corporate card purchase," up 7%, 10% and 18%, respectively.

Use rates by non-FIs remained relatively consistent between 2009 and 2011. More variability is reported between 2010 and 2011, which likely reflects the difference in the number of survey respondents and the smaller size of the organizations responding in 2010.

Chart V: Use Internal Controls and Procedures by % of Financial Institution Respondents (N=171 to 181)

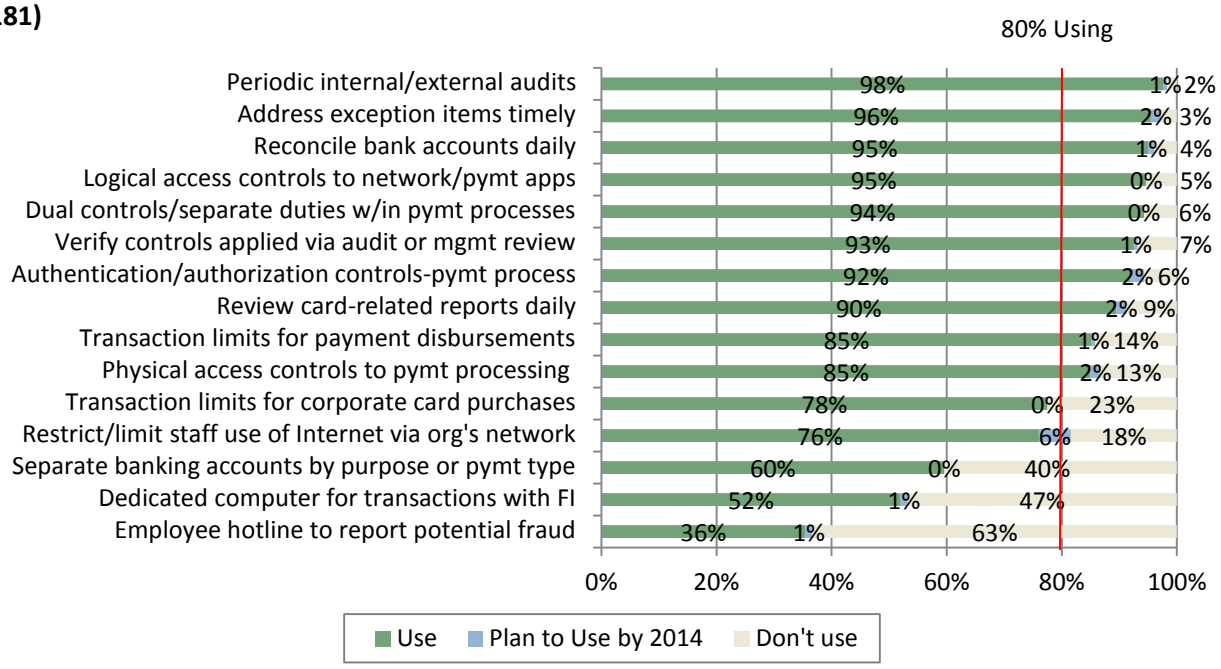
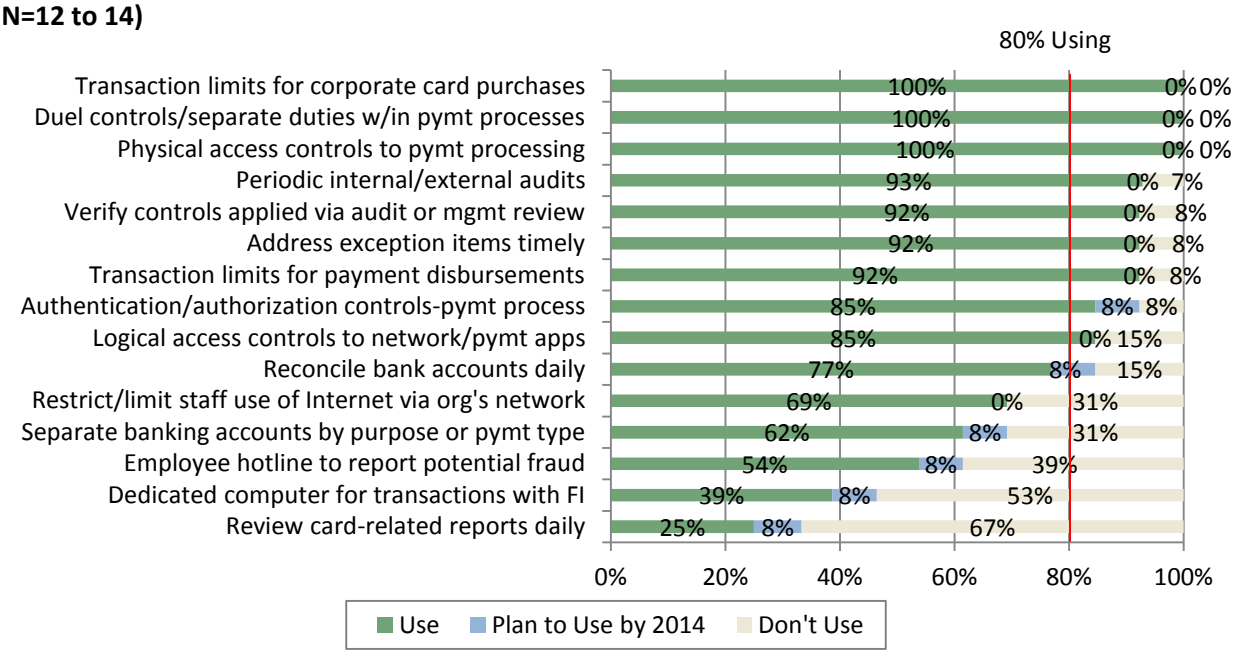


Chart W: Use of Internal Controls and Procedures by % of Non-Financial Institution Respondents (N=12 to 14)



© 2012 Federal Reserve Bank of Minneapolis

Chart X: Effectiveness of Internal Controls and Procedures by % of Financial Institution Respondents Using It (N=60 to 175)

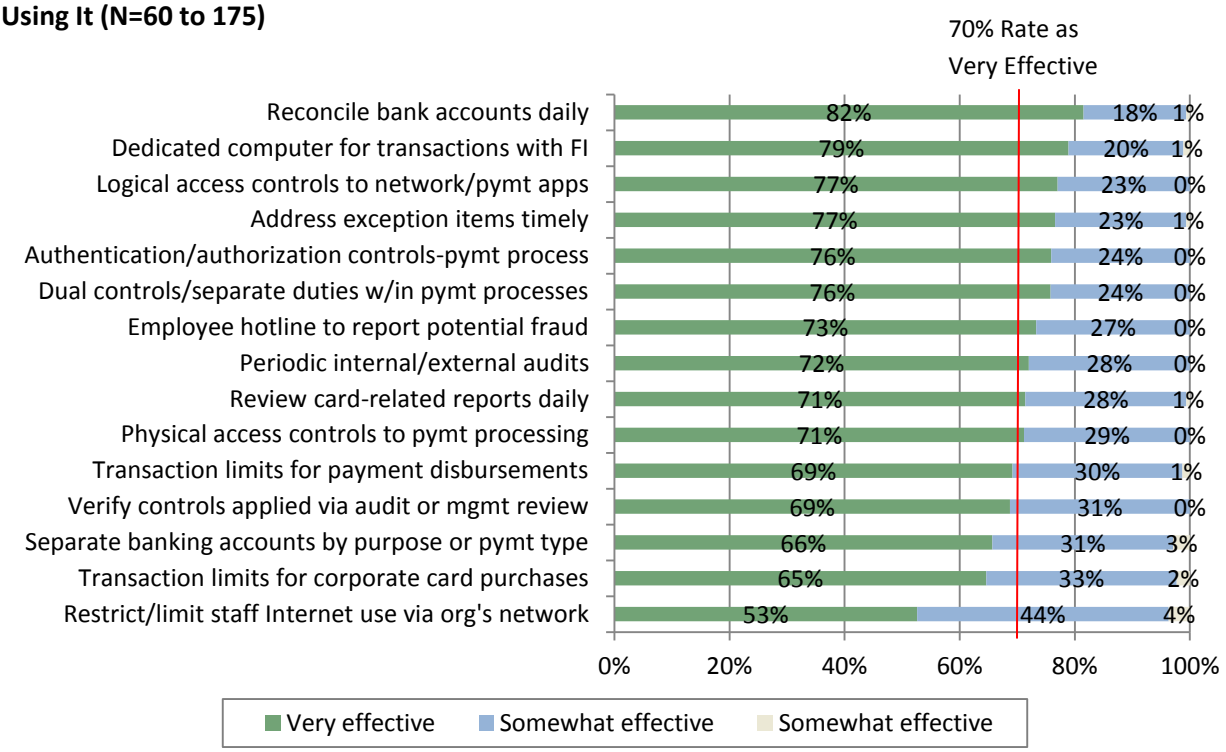
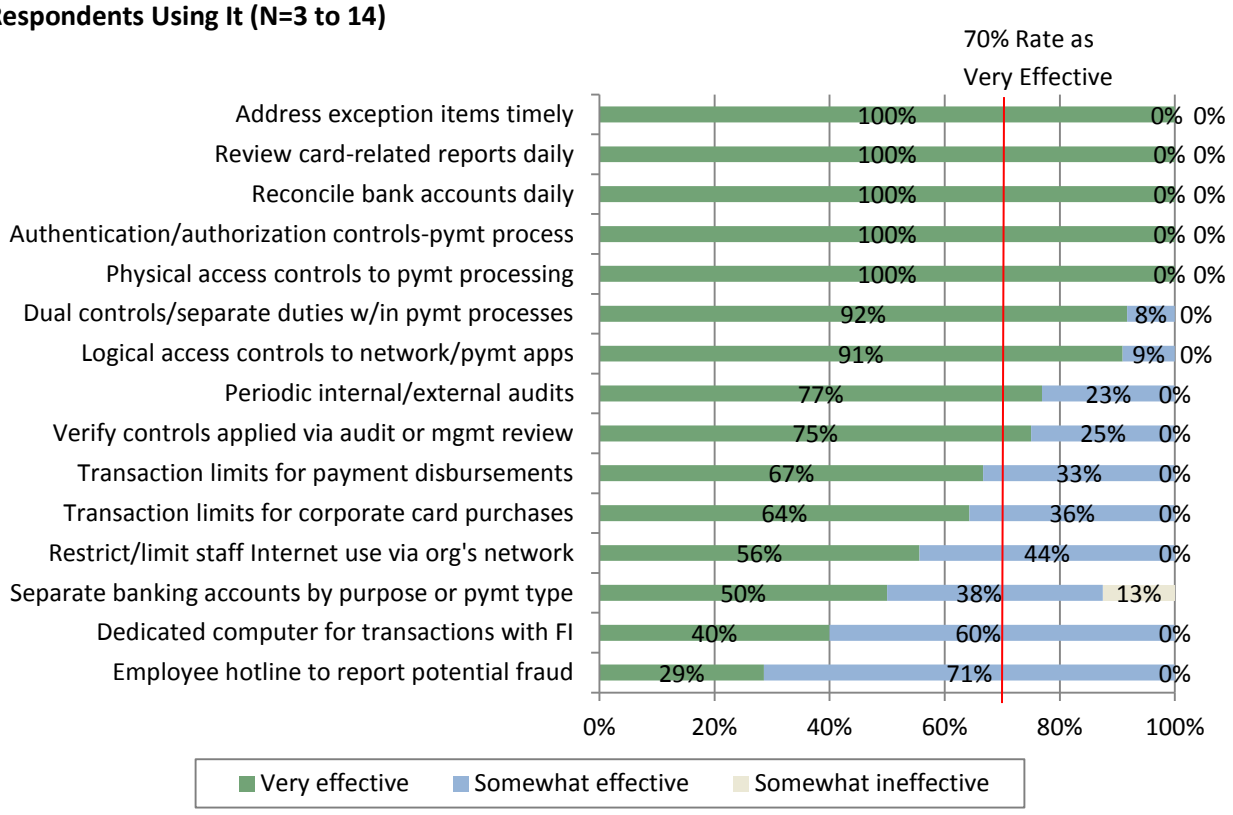


Chart Y: Effectiveness of Internal Controls and Procedures by % of Non-Financial Institution Respondents Using It (N=3 to 14)



© 2012 Federal Reserve Bank of Minneapolis

ii. ***Customer Authentication Methods.*** In 2012, respondents were asked about 10 different customer authentication methods. Usage varied significantly in overall adoption between FIs and non-FI respondents (Charts Z and AA). Over 60% of the FIs use seven of the 10 methods, while only 25% of the non-FIs use six of the 10 methods. Differences in usage may be explained partly by differences in payment instruments used or offered and the typical payment counterparties or target customers. For example, nearly all FIs offer debit cards and target both consumer and business customers. Only 70% of non-FIs accept card payments and 45% reported that payment counterparties are primarily other businesses.

Card chip authentication had the highest percent of respondents that are planning to use it by 2014 (11% of FIs and 25% of non-FIs). This is not surprising given recent announcements by the major card brands to migrate U.S. card payments to chip-enabled cards.

Five of the authentication methods were rated as very effective by those that use them (Charts BB and CC), whereas magnetic stripe authentication was rated less effective (12% of FIs and 33% of non-FIs). Signature verification was also rated lower with 13% of FIs rating it somewhat effective.

Chart Z: Use of Customer Authentication Methods by % of Financial Institution Respondents (N=169 to 181)

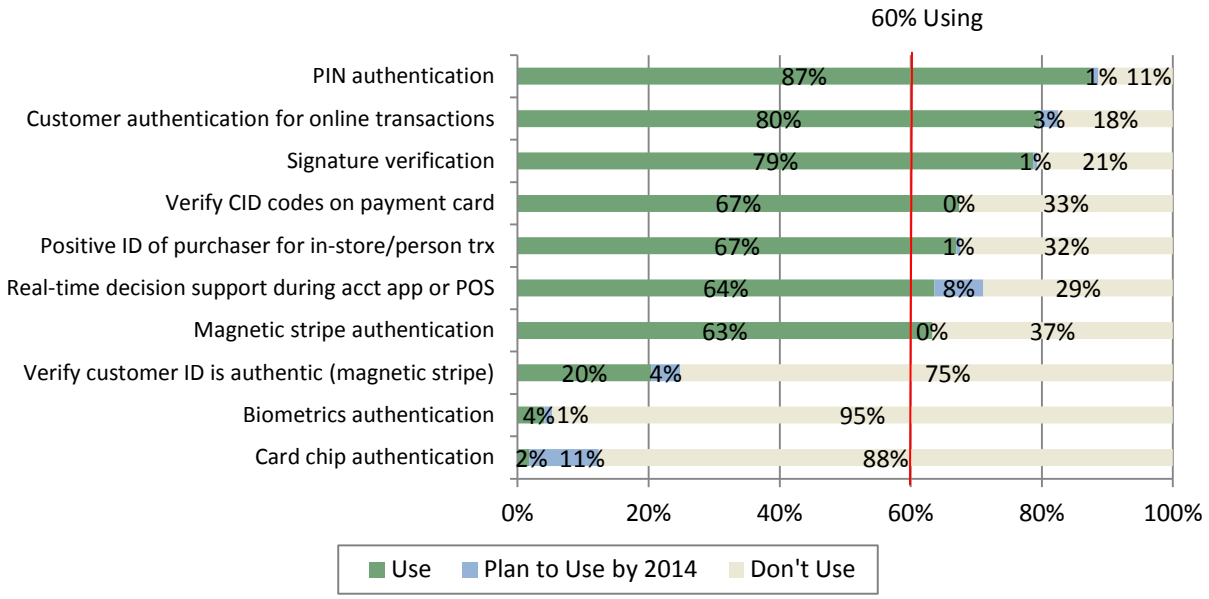


Chart AA: Use of Customer Authentication Methods by % of Non-Financial Institution Respondents (N=12 to 14)

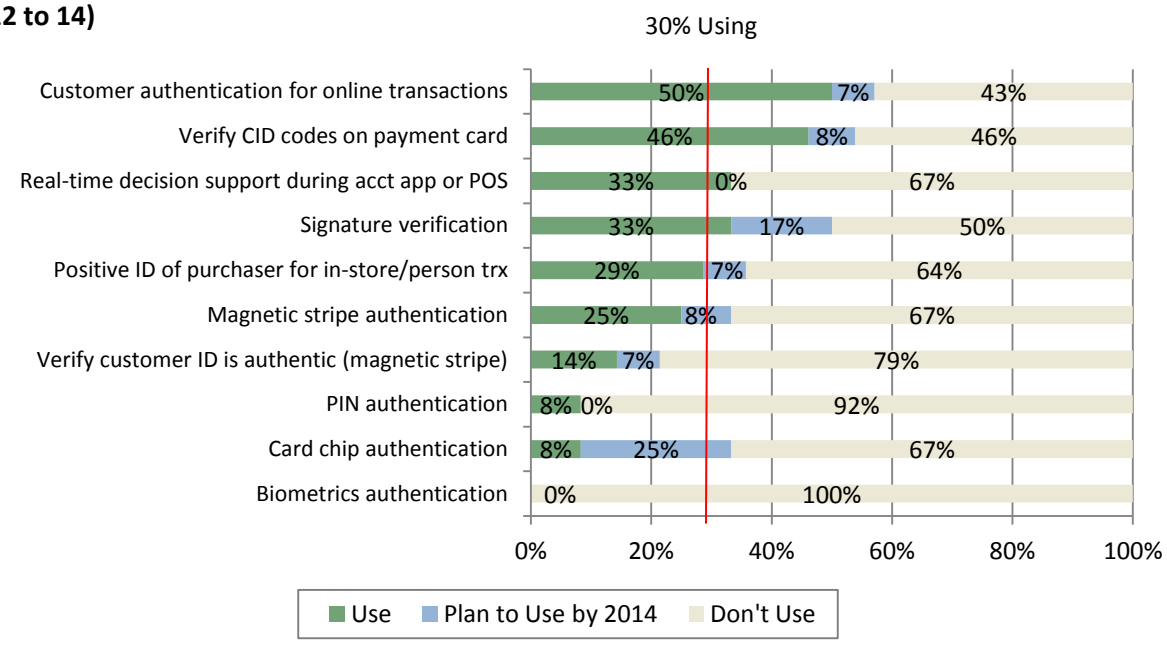
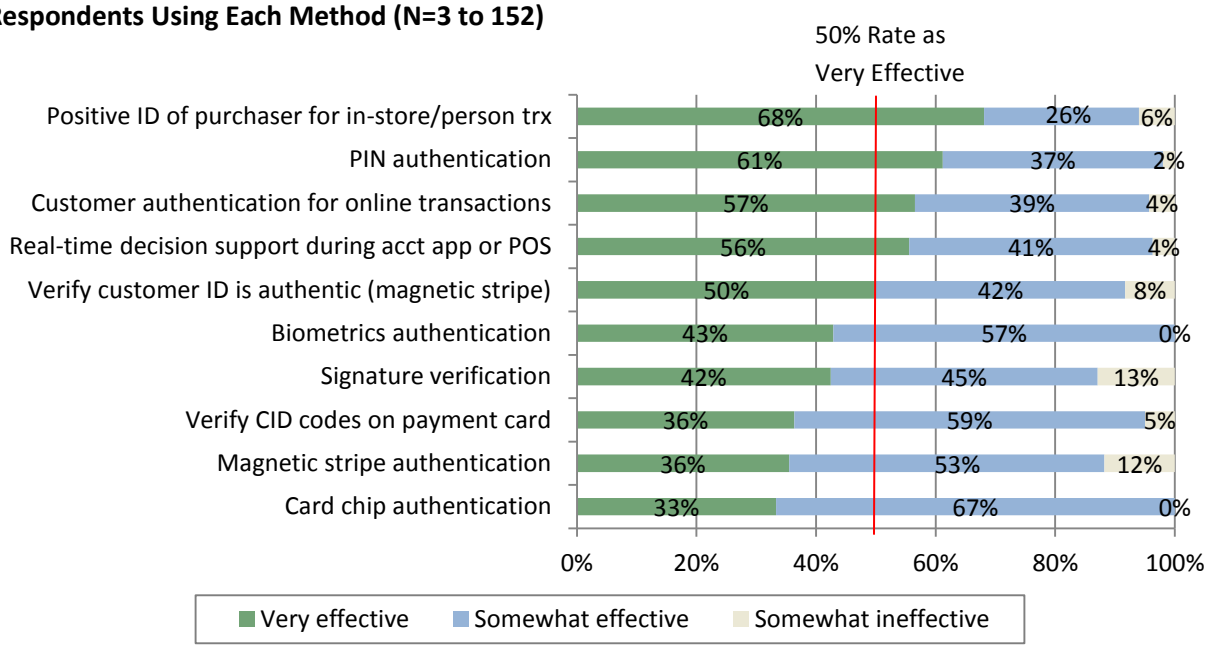
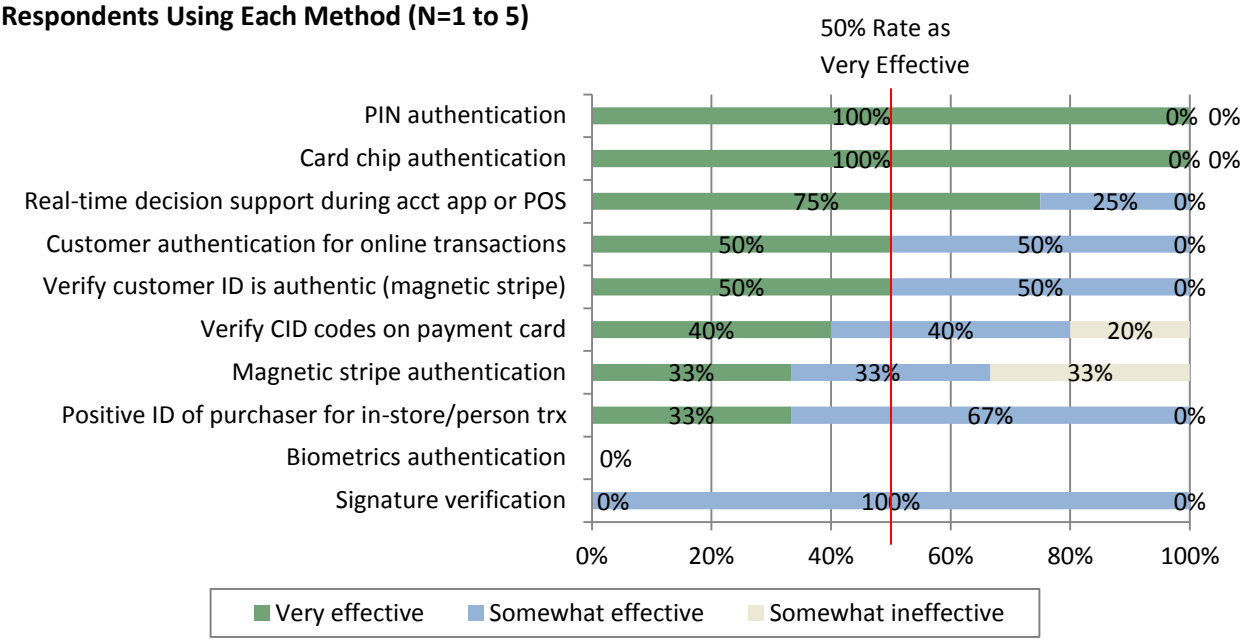


Chart BB: Effectiveness of Customer Authentication Methods by % of Financial Institution Respondents Using Each Method (N=3 to 152)



© 2012 Federal Reserve Bank of Minneapolis

Chart CC: Effectiveness of Customer Authentication Methods by % of Non-Financial Institution Respondents Using Each Method (N=1 to 5)



iii. ***Transaction Screening and Risk Management Methods.*** Use of transaction screening and risk management methods varied in use between FIs and non-FIs (Charts DD and EE). Methods with the highest use were staff education and training on payment risk management, use of fraud detection pen for currency, and human review of payment transactions. Methods with the lowest use were centralized fraud information database for one or multiple payment types.

More respondents plan to provide customer education on payments fraud risk mitigation by 2014 (14% of FIs and 17% of non-FIs). Nine percent of the FIs also plan to implement software that detects fraud through pattern matching, predictive analytics or other indicators. These plans make sense in view of the information in Section C. Two-thirds of respondents reduced their fraud losses by enhancing fraud monitoring systems and providing more staff education and training.

All of the transaction screening and risk management methods were rated as effective by most users, with over half of respondents rating the majority of methods as very effective.

© 2012 Federal Reserve Bank of Minneapolis

Chart DD: Use of Transaction Screening and Risk Management Methods by % of Financial Institution Respondents (N=169-182)

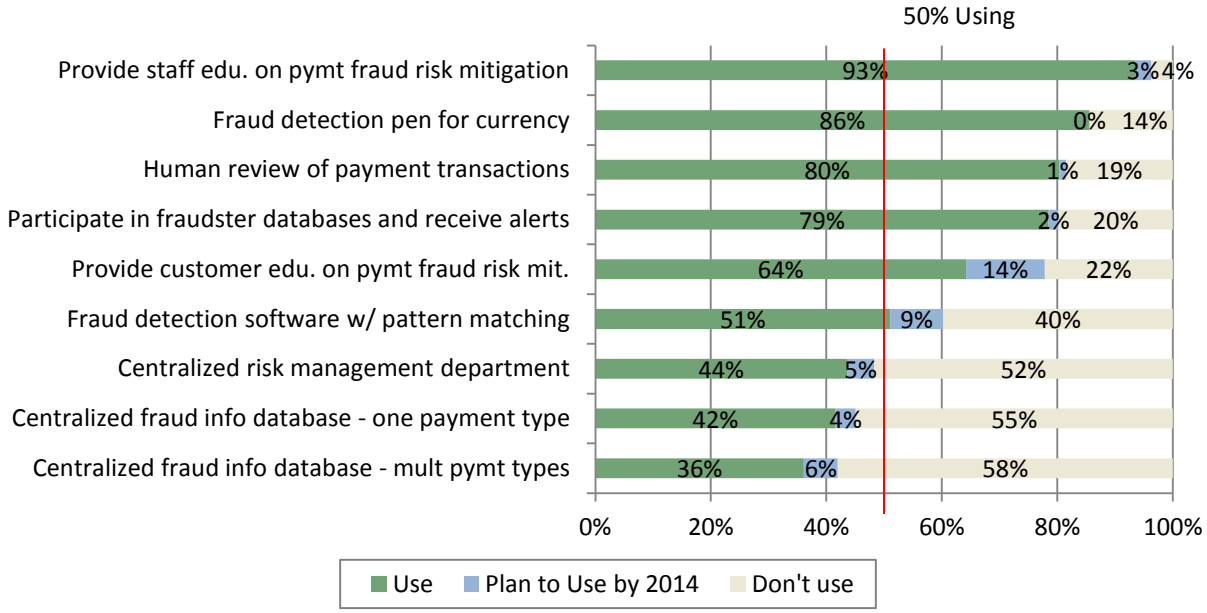


Chart EE: Use of Transaction Screening and Risk Management Methods by % of Non-Financial Institution Respondents (N=12 to 14)

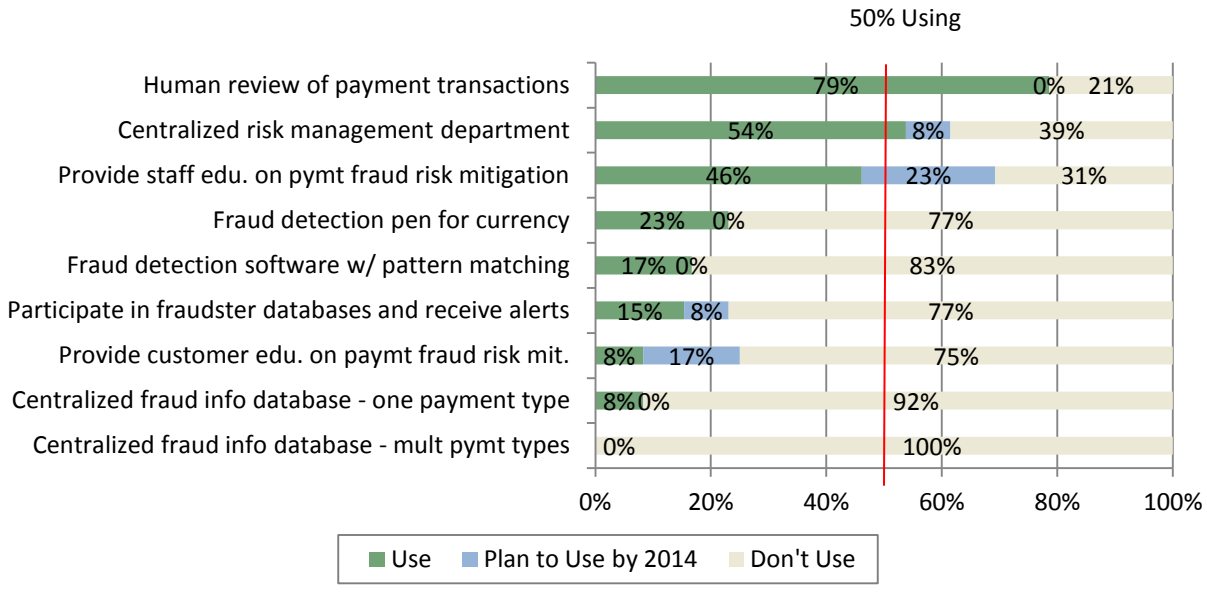


Chart FF: Effectiveness of Transaction Screening and Risk Management Methods by % of Financial Institution Respondents Using Each Method (N=58 to 168)

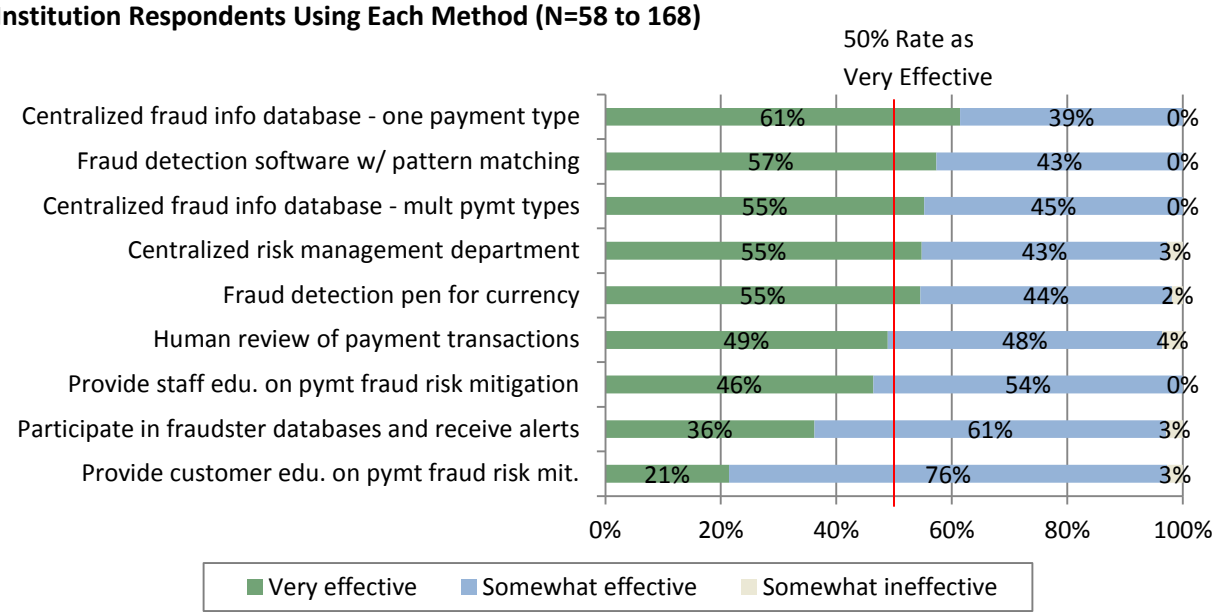
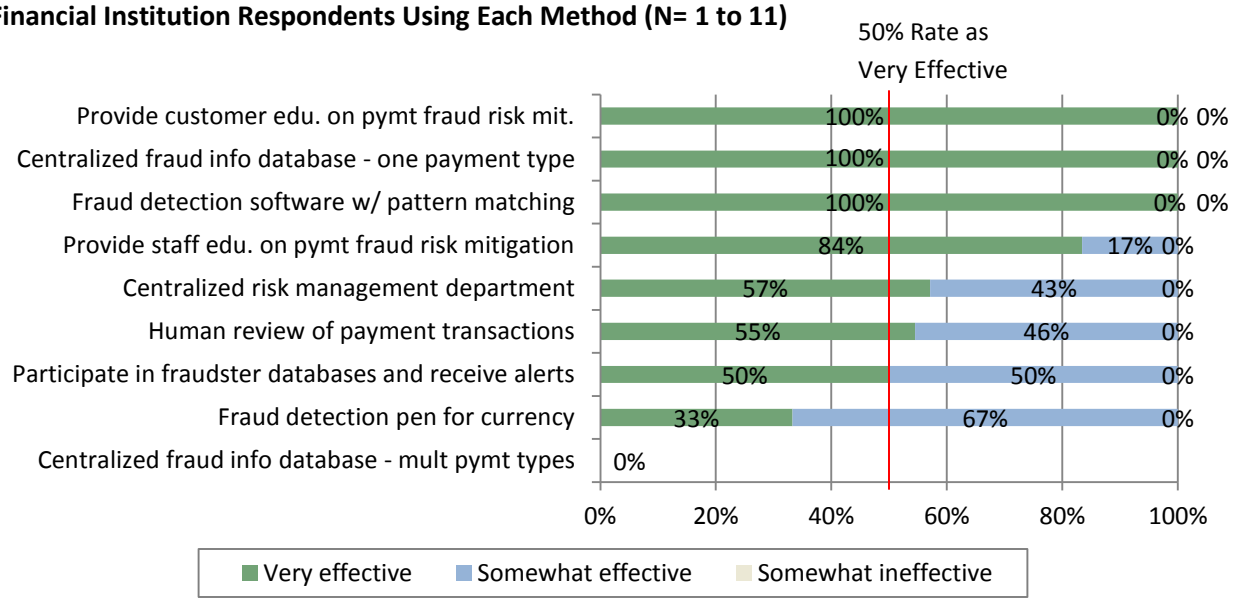


Chart GG: Effectiveness of Transaction Screening and Risk Management Methods by % of Non-Financial Institution Respondents Using Each Method (N= 1 to 11)



iv. ***Risk Mitigation Services Offered by Financial Institutions.*** The top six methods used by non-FI respondents are reported in Chart HH: online information services, multi-factor authentication to initiate payments, check positive pay/reverse positive pay, account alert services, ACH debit blocks, and ACH filters. Five of the six services identified as most used were similarly reported in the 2010 and 2009 surveys. However, for most of the services, 2010 use is materially lower than reported in 2011 and 2009. This might be explained by the change in respondent mix relative to size of annual revenue—i.e., a higher share of small organizations responded to this question in 2010. In the 2011 and 2009, five services reflected use rates of 70% or more.

© 2012 Federal Reserve Bank of Minneapolis

Non-FI respondents identified four new risk mitigation services they plan to add by 2014. These are ACH payee positive pay with 15% planning to use it, check payee positive pay (8%), ACH positive pay (8%), and card alert services for commercial/corporate cards (7%). In the 2010 survey, non-FI respondents identified the same four services plus account masking as services they would add in the next two years.

Eight of the risk mitigation services were rated as very effective by over 80% of the organizations that use them (Chart II). Services that provide information to help identify potential fraudulent transactions and fraud loss prevention services were viewed as somewhat effective by 40% to 50% of the users.

The top two services based on use, i.e., online information services and multi-factor authentication to initiate payments, are offered by over 80% of the FI respondents (Chart JJ). Most FIs also offer account alert services. Other services with high usage are offered by less than half of the FIs. Highest among services that FIs plan to offer in the future were check and ACH positive pay/payee positive pay with 7% to 8% of FIs planning to offer these services by 2014. These data seem to suggest that more opportunity may exist for FIs to respond to demand by non-FIs for fraud risk mitigation services.

Chart HH: Use of Risk Mitigation Services Offered by Financial Institutions by % of Non-Financial Institution Respondents

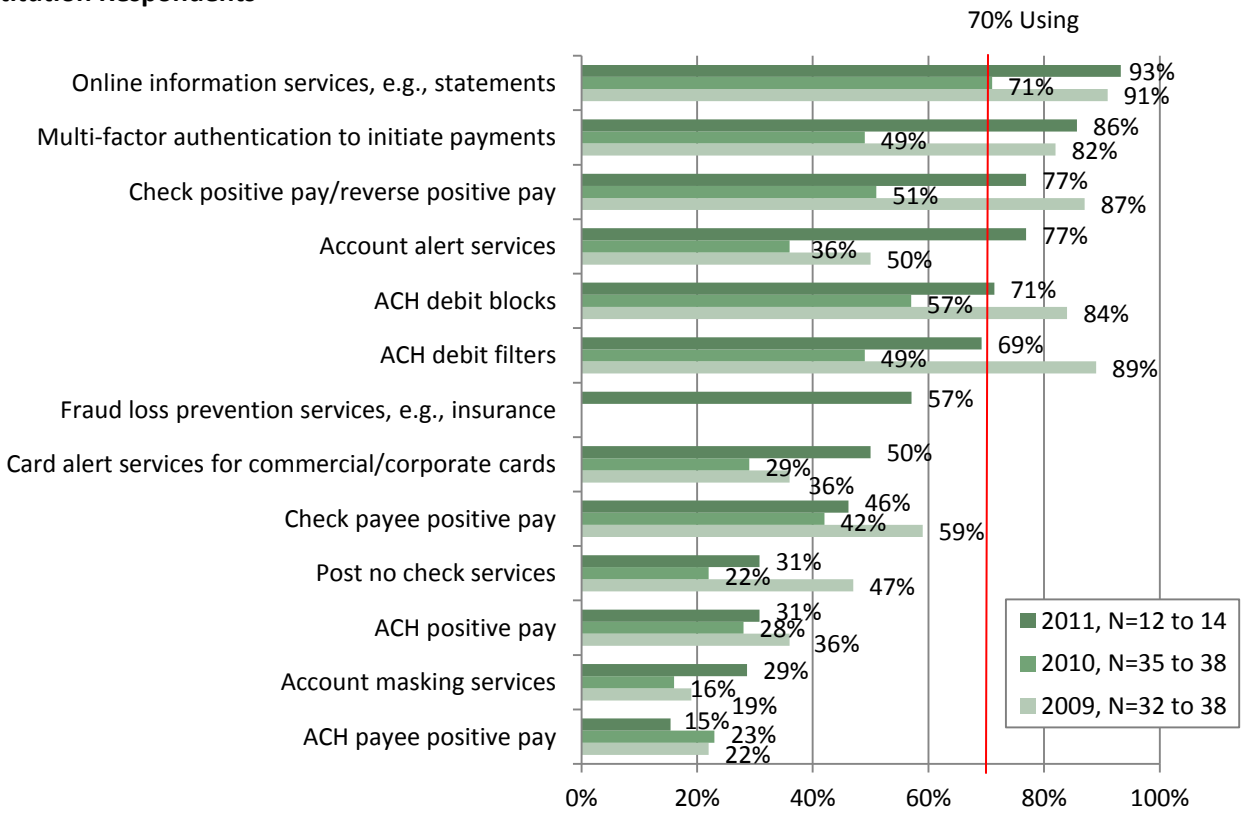


Chart II: Effectiveness of Risk Mitigation Services Offered by Financial Institutions by % of Non-Financial Institution Respondents Using the Service (N=2 to 12)

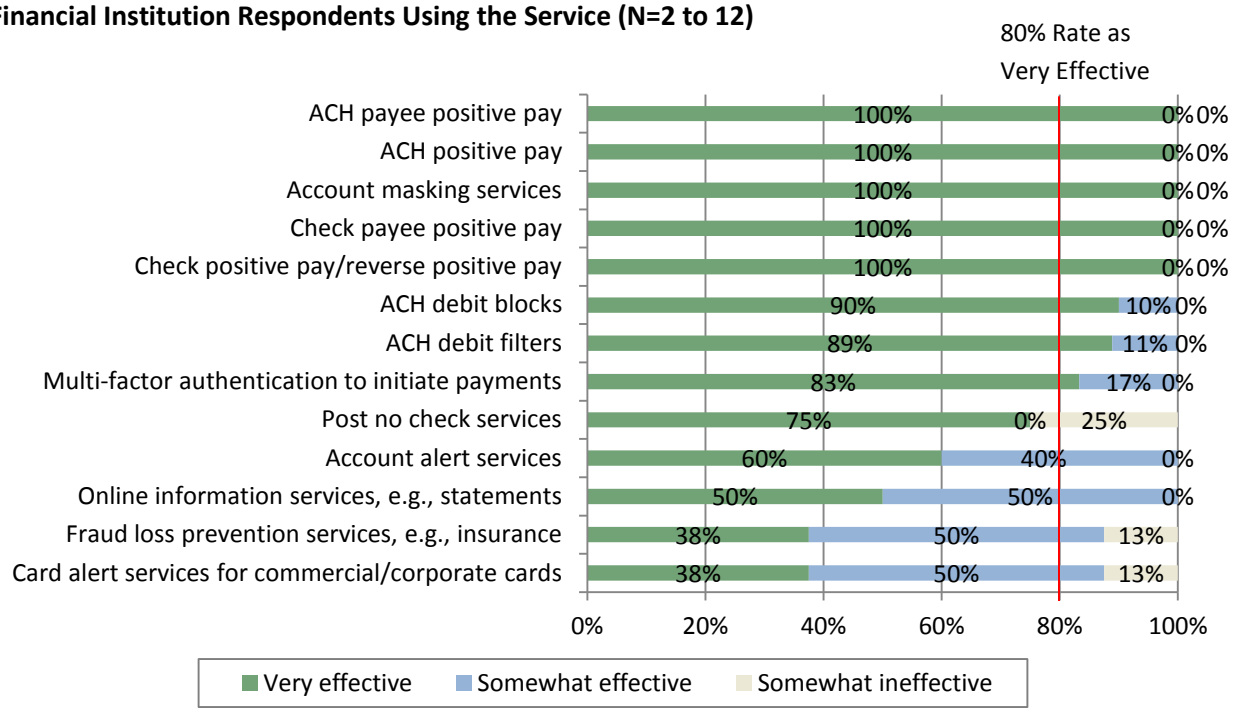
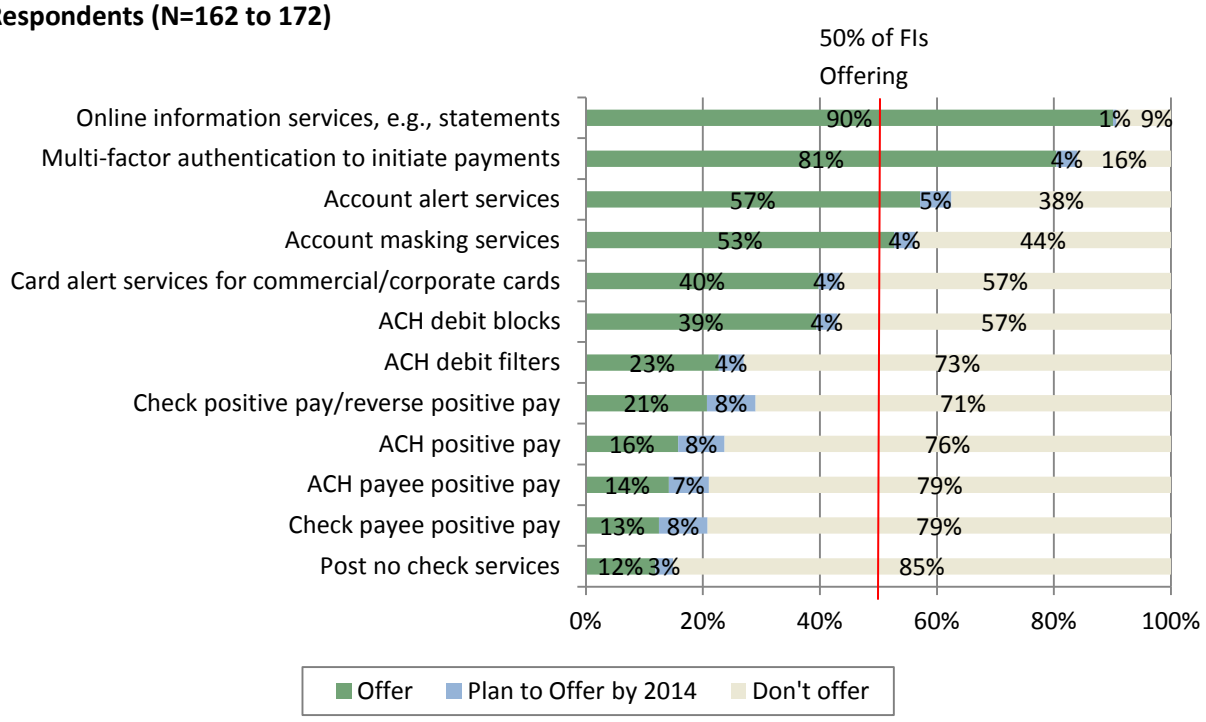


Chart JJ: Risk Mitigation Services Offered by Financial Institutions by % of Financial Institution Respondents (N=162 to 172)



© 2012 Federal Reserve Bank of Minneapolis

g. Barriers to Reduce Payments Fraud

Respondents reported on barriers to further reducing payments fraud. Most identified some aspect of "cost" as the main barrier. Examples included the lack of resources, implementation costs, and a lack of a compelling business case. A complete summary is listed in Table 12. This emphasis on cost as a barrier to further fraud mitigation efforts is consistent with survey responses in 2009 and 2010.

Table 12: Main Barriers to Payments Fraud Mitigation by % of Respondents

Barriers	Financial Institutions			Non-Financial Institutions		
	2011 (N=163)	2010 (N=92)	2009 (N=91)	2011 (N=12)	2010 (N=34)	2009 (N=29)
Lack of staff resources	56%	54%	56%	75%	53%	52%
Cost of implementing in-house fraud detection tool/service	50%	52%	62%	8%	38%	48%
Cost of implementing commercially available fraud detection tool/service	39%	48%	57%	17%	41%	52%
Lack of compelling business case (cost vs. benefit) to adopt new or change existing methods	38%	47%	36%	75%	35%	55%
Consumer data privacy issues/concerns	33%	38%	37%	33%	41%	34%
Unable to combine payment information for review due to operating w/ multiple business areas, states or banks	12%	4%	5%	17%	6%	24%
Corporate reluctance to share information due to competitive issues	11%	9%	5%	25%	3%	10%

h. Opportunities to Reduce Payments Fraud

Respondents identified opportunities to reduce fraud in three areas: i) new methods needed, ii) authentication methods, and iii) legal and regulatory changes.

i. ***New or Improved Methods Most Needed.*** The majority of respondents identified controls over Internet payments, consumer education on payments fraud prevention and replacement of card/magnetic stripe technology as the new or improved methods most needed to help reduce payments fraud (Table 13). Eighty percent of the non-FIs identified the new or improved methods most needed as information sharing on emerging fraud tactics.

© 2012 Federal Reserve Bank of Minneapolis

Table 13: New Methods Needed by % of Respondents

New Methods Needed	Financial Institutions (N=173)	Non-Financial Institutions (N=14)	All Respondents (N=187)
Controls over Internet payments	66%	57%	65%
Consumer education on fraud prevention	61%	71%	62%
Replacement of card/magnetic stripe technology	58%	29%	56%
More aggressive law enforcement	47%	36%	46%
Controls over mobile payments	40%	36%	40%
Information sharing on emerging fraud tactics, e.g., those being conducted by criminal rings	40%	79%	43%
Industry-specific education on best prevention practices for fraud	36%	21%	35%
Industry alert services	23%	29%	24%
Image survivable check security features for business checks	10%	14%	11%

ii. ***Authentication Methods***. Respondents were asked what authentication methods their organizations would prefer to adopt to help reduce payments fraud. Half of the FIs identified a "Chip and PIN requirement" and two-thirds of the non-FIs identified tokens (Table 14).

Table 14: Preferences for Adoption of Authentication Methods

Authentication Methods Preferences	Financial Institutions (N=161)	Non-Financial Institutions (N=12)	All Respondents (N=173)
Chip and PIN requirement	55%	25%	53%
Multi-factor authentication	49%	42%	49%
PIN requirement	43%	42%	43%
Chip for dynamic authentication	34%	25%	34%
Token	29%	67%	31%
Out-of-band/channel authentication to authorize payment	29%	17%	28%
Biometrics	23%	17%	23%
Mobile device to authenticate person	22%	25%	22%

iii. ***Legal or Regulatory Changes.*** Respondents were also asked to offer views on legal and regulatory changes that would help reduce payments fraud. Increased penalties for fraud and attempted fraud were identified by many. FI respondents suggested placing more responsibility on customers to reconcile and protect their payments data, and shifting more liability for fraudulent payments to the entity that initially accepts the card payments. Non-FI respondents also identified the need for increased penalties for fraud and attempted fraud as well as

© 2012 Federal Reserve Bank of Minneapolis

strengthening disincentives to committing fraud through stiffer penalties and more likely prosecution and establishing new or changing existing laws/regulations to strengthen the management of payments fraud risk. Table 15 summarizes all responses regarding legal and regulatory changes.

Table 15: Legal and Regulatory Considerations by % of Respondents

Legal and Regulatory Changes	Financial Institutions		Non-Financial Institutions		All Respondents	
	2011 (N=117)	2010 (N=104)	2011 (N=13)	2010 (N=39)	2011 (N=130)	2010 (N=143)
Increase penalties for fraud and attempted fraud	68%	70%	69%	67%	68%	69%
Place more responsibility on consumers and customers to reconcile and protect their payments data	68%	79%	15%	26%	65%	64%
Place responsibility to mitigate fraud and shift liability for fraudulent card payments to the entity that initially accepts the card payment	67%	79%	31%	18%	65%	62%
Assign liability for fraud losses to the party most responsible for not acting to reduce the risk of payment fraud	52%	47%	8%	26%	49%	41%
Strengthen disincentives to committing fraud through stiffer penalties and more likely prosecution	47%	59%	62%	72%	48%	62%
Improve law enforcement cooperation on domestic and international payments fraud and fraud rings	45%	38%	54%	69%	46%	46%
Align Regulation E and Regulation CC to reflect changes in check collection systems' use of check images and conversion of checks to ACH	37%	52%	31%	26%	36%	45%
Focus future legal or regulatory changes on data breaches to where breaches occur	35%	30%	31%	15%	35%	26%
Assign responsibility for mitigating fraud risk to the party best positioned to take action against fraud	31%	40%	23%	26%	30%	36%
Establish new laws/regs or change existing ones in order to strengthen the management of payments fraud risk	24%	18%	69%	28%	27%	21%

© 2012 Federal Reserve Bank of Minneapolis

4. Conclusions

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

- Payments-related fraud remains a significant concern of FIs and other corporations in the region, including very small organizations. Nearly all respondents experienced some number of payments fraud attempts (94%) and most incurred payments fraud losses (91%).
- For FIs, signature debit card is the payment instrument most vulnerable to fraud attempts and losses, a trend that continues from 2010. For non-FIs, check continues to be the payment instrument most vulnerable to fraud attempts and losses.
- Over half of FIs reported that signature debit card losses from fraud exceeded their investment in mitigation methods to prevent such fraud. This seems to suggest a cost-effective opportunity to increase these fraud prevention investments.
- Corporate account take-over fraud can result in significant losses, but it was not identified as a significant fraud scheme that affected a high percentage of respondents to this survey. However, corporate account take-over fraud may be increasing. Nine percent of non-FIs identified most often used fraud schemes involving a breach of access or other data security controls, which included account takeovers. This is an increase over 2010 level of 3%.
- Most FIs and other corporations report total fraud losses that represent less than 0.3% of their annual revenues. This is consistent with 2010 and 2009 survey results. While any fraud losses are undesirable, by this measure fraud loss levels appear relatively low.
- Strategies to detect and prevent fraud effectively require the use of various mitigation methods and tools. Internal controls and procedures are the main fraud mitigation methods used by most organizations. Transaction monitoring, transaction authentication, and other risk management services offered by FIs are also used by a majority of non-FI organizations. Finally, the most frequently used methods were not necessarily the most effective**.**
- Two-thirds of the respondents that reduced their fraud losses in 2011 attributed this to changes made to enhance fraud monitoring systems and employee education and training. This may suggest an opportunity for all organizations interested in reducing fraud losses to consider implementing.
- Cost is the primary barrier cited by the majority of respondents that prevents them from investing in additional options for mitigating payments fraud. Similar results were reported in 2010 and 2009. This may be short sighted in view of reports that for some payment types fraud losses exceed the cost of investments in fraud prevention.

© 2012 Federal Reserve Bank of Minneapolis

- Organizations are focused now on the need for alternatives to magnetic stripe authentication technology to secure card payments. Chip adoption by 2014 was identified by respondents as among the top three most needed methods to reduce fraud in the future. This is a new priority compared to survey results in 2009 and 2010.

© 2012 Federal Reserve Bank of Minneapolis