2010 Payments Fraud Survey Summary of Results

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

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

April 12, 2011

©2011 Federal Reserve Bank of Minneapolis

1. Introduction

In October 2010, the Federal Reserve Bank (FRB) of Minneapolis' Payments Information and Outreach Office conducted follow-up research on payments-related fraud experienced by area organizations.[1] Members of the Financial and Retail Protection Association, Minnesota Association for Financial Professionals, Montana Bankers Association, 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.

2. Respondent Information

The survey was sent to about 2,900 organizations of which 206 participated for a response rate of 7%.[2] The share of responses by organization is shown in Table 1.

Table 1: Share of Responses by Association* (N=206)	Financial Service Org.	Other Organizations	All Organizations
Upper Midwest Automatic Clearing House Association	90%	11%	66%
Financial and Retail Protection Association	28%	16%	24%
Other organizations concerned with payments fraud	16%	27%	19%
Minnesota Association for Financial Professionals	6%	33%	15%
Montana Chamber of Commerce	1%	35%	12%
Montana Bankers Association	9%	3%	7%

* The total percent exceeds 100%, as respondent organizations are members of one or more associations.

Seventy-one percent of respondents are financial service organizations, most of which are financial institutions (FI). Retail is the next largest industry category at 6%. The remaining 23% are split among more than fourteen other industries as shown in Table 2. Respondents are also categorized by the organization's annual revenue, listed in Table 3. Almost half the organizations have annual revenues of less than $50 million.

[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] The survey sample is not representative of the organizations located in the Ninth Federal Reserve District or the sponsoring associations' membership, and neither are the results.

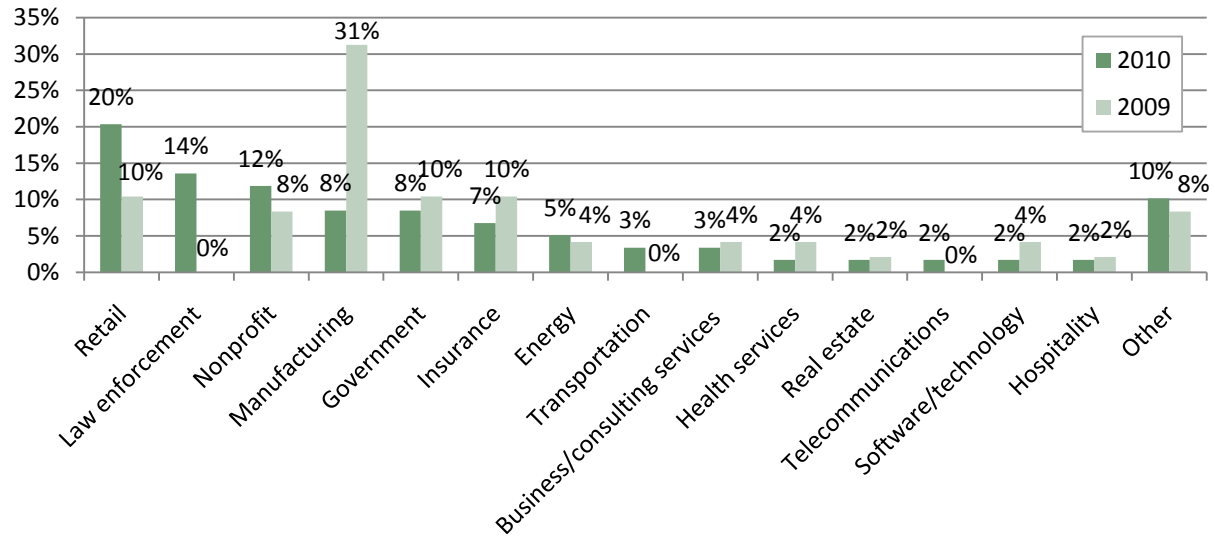
© 2011 Federal Reserve Bank of Minneapolis

Table 2: Respondents by Industry (N=206)	2010	2009
Financial services	71%	74%
Retail	6%	3%
Law enforcement	4%	0%
Nonprofit	3%	2%
Manufacturing	2%	8%
Government	2%	3%
Insurance	2%	3%
Energy	1%	1%
Transportation	1%	0%
Business services/consulting	1%	1%
Health services	.5%	1%
Real estate	.5%	1%
Telecommunications	.5%	0%
Software/technology	.5%	1%
Hospitality	.5%	1%
Other	3%	2%

Table 3: Respondents by Annual Revenue (N=206)	2010			2009
	Fin. Serv.	Other Org.	All Org.	All Org.
Under $50 million	48%	48%	48%	40%
$50 - 99 million	12%	2%	9%	14%
$100 - 249.9 million	11%	8%	10%	10%
$250 - 499.9 million	5%	6%	5%	5%
$500 - 999.9 million	5%	6%	5%	4%
$1 - 4.9 billion	7%	10%	8%	11%
$5 - 9.9 billion	1%	3%	2%	1%
$10 - 19.9 billion	1%	3%	2%	2%
Over $20 billion	2%	2%	2%	4%
Not applicable	1%	11%	4%	10%
Don't know	7%	2%	5%	

The mix of non-financial service organizations that responded to the 2010 survey differs from the 2009 mix as shown in Table 2 and Chart A. Notably, the percentage of respondents from the retail and law enforcement industries increased appreciably while those from manufacturing decreased. This provides some context in interpreting year-to-year changes.

Chart A: Non-Financial Services Industries by Respondents 2010 versus 2009



© 2011 Federal Reserve Bank of Minneapolis

3. Summary of Survey Results by Questions

Section 3 summarizes survey responses by question. Where differences are relevant, responses of financial institutions are reported separately from all others.

a. Payment Types Used by Respondent Organizations

Charts B through E show the different payments types accepted and used for disbursements for business-to-business (B2B), consumer-to-business (C2B), and business-to-consumer (B2C) payments.

Chart B: Payment Types Accepted for B2B Payments by % of Respondents

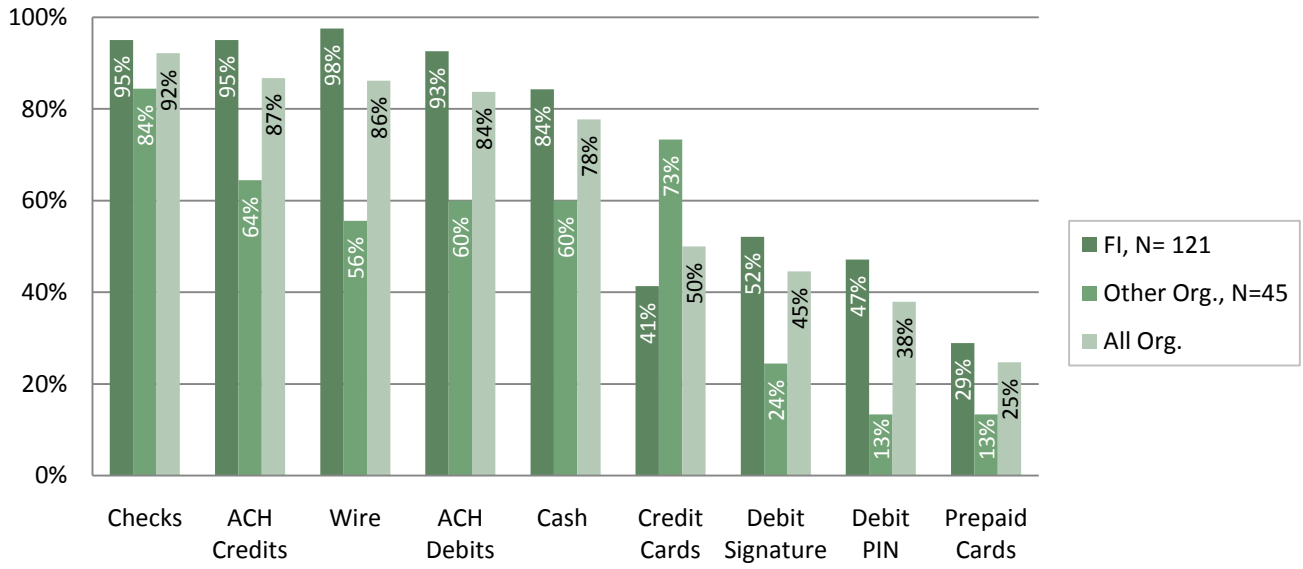
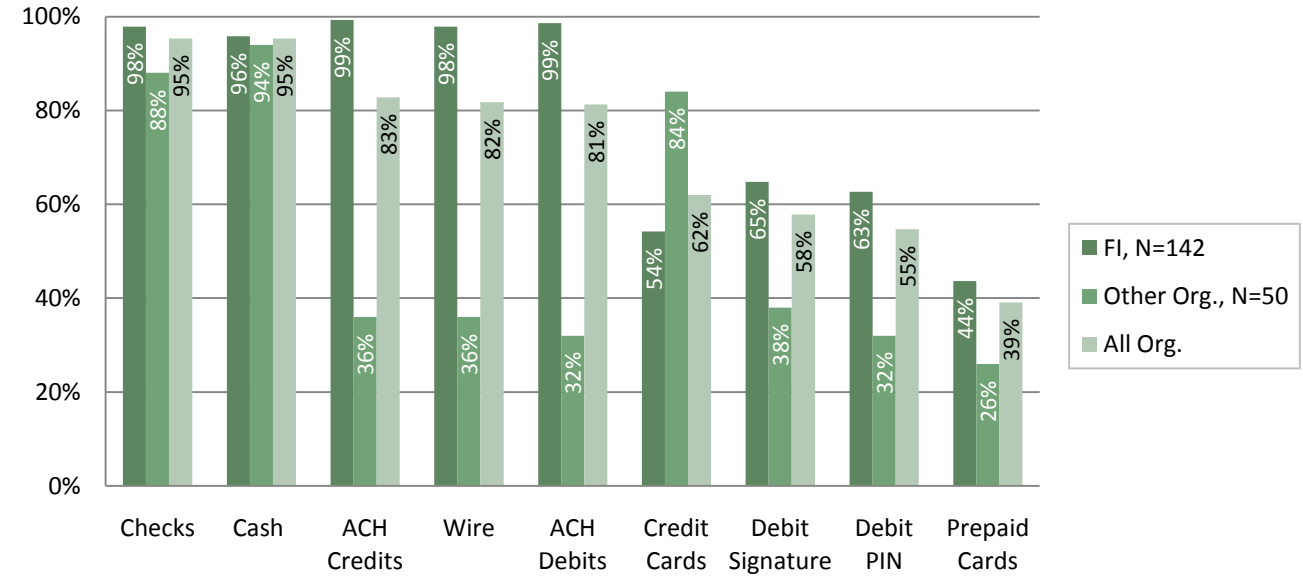


Chart C: Payment Types Accepted for C2B Payments by % of Respondents



© 2011 Federal Reserve Bank of Minneapolis

Chart D: Payment Types Used for B2B Disbursements by % of Respondents

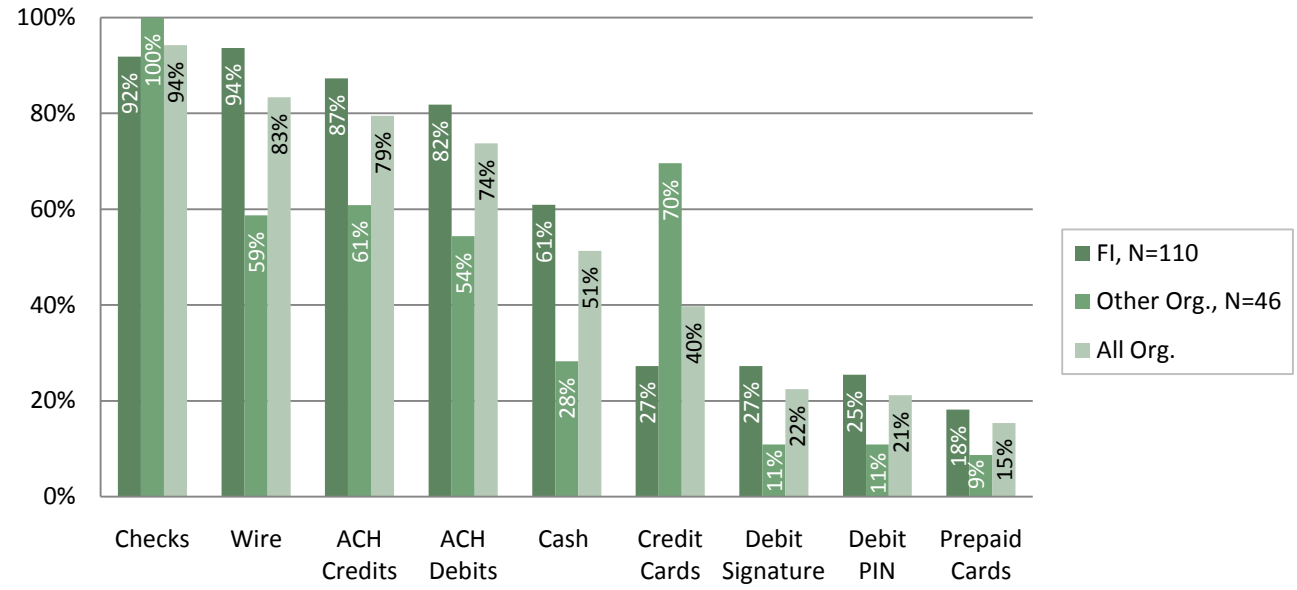
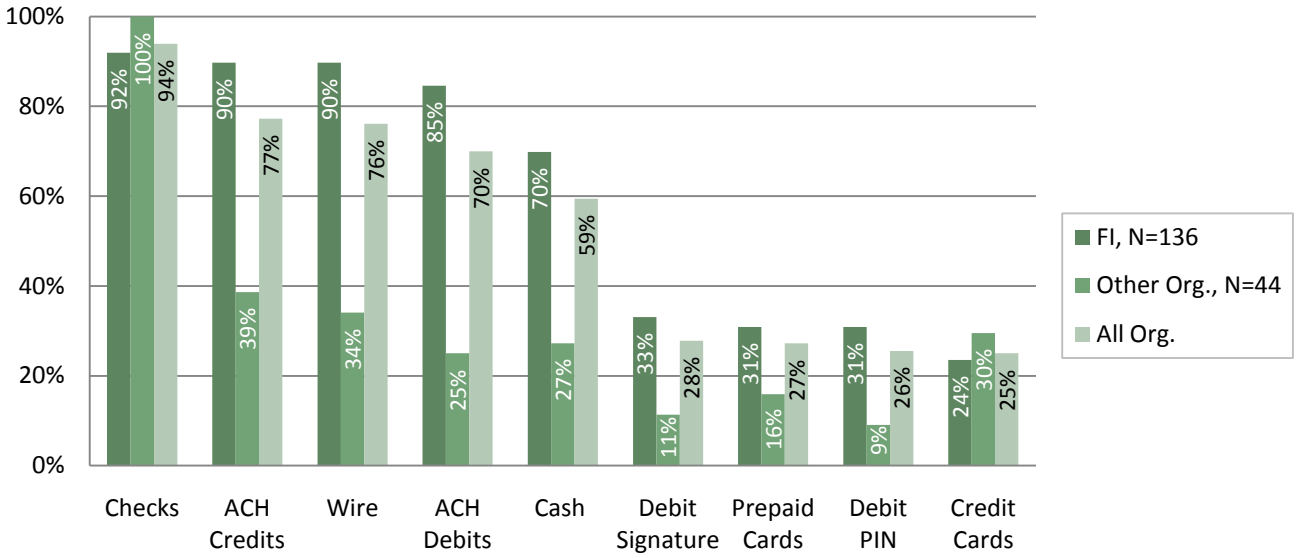


Chart E: Payment Types Used for B2C Disbursements by % of Respondents

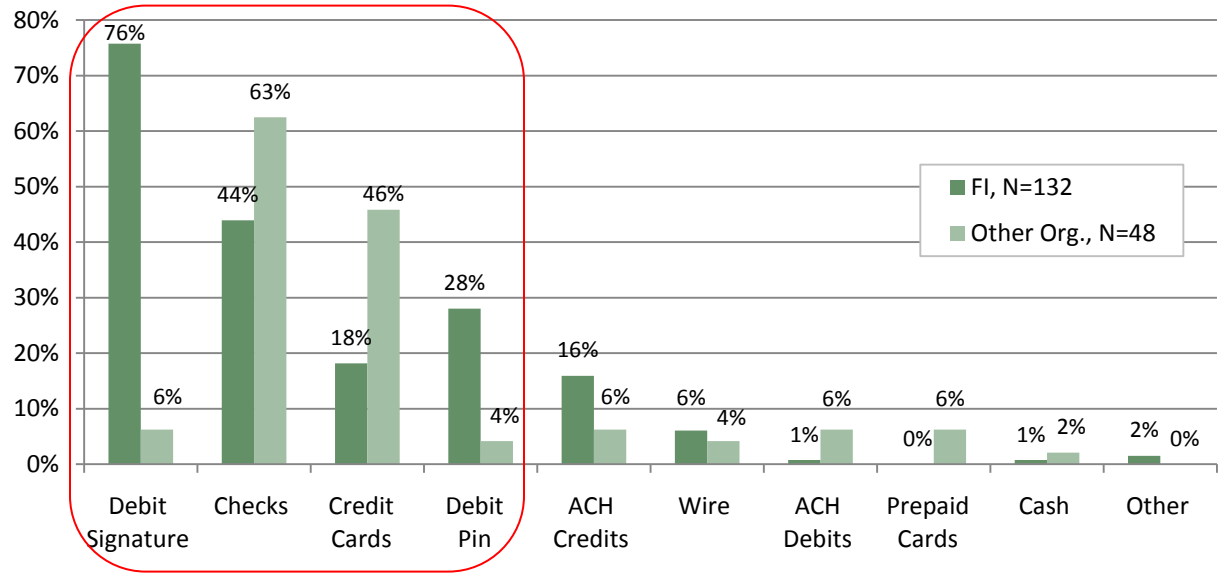


© 2011 Federal Reserve Bank of Minneapolis

b. Payments Fraud Attempts and Financial Losses

Seven percent of all respondents reported no payments fraud attempts (2% of the FI respondents and 17% of all other organization). Of those that experienced fraud attempts, respondents were asked which payment types have the highest number of attempts as reported in Chart F. Signature debit card attempts were the highest at 76%, but among FIs only. Check fraud attempts were next highest among non-FI organizations at 63%, followed by credit cards among these organizations (46%). FIs also reported relatively high numbers of check fraud attempts at 44%, followed by PIN debit cards at 28%, credit cards at 18%, and ACH credits at 16%.

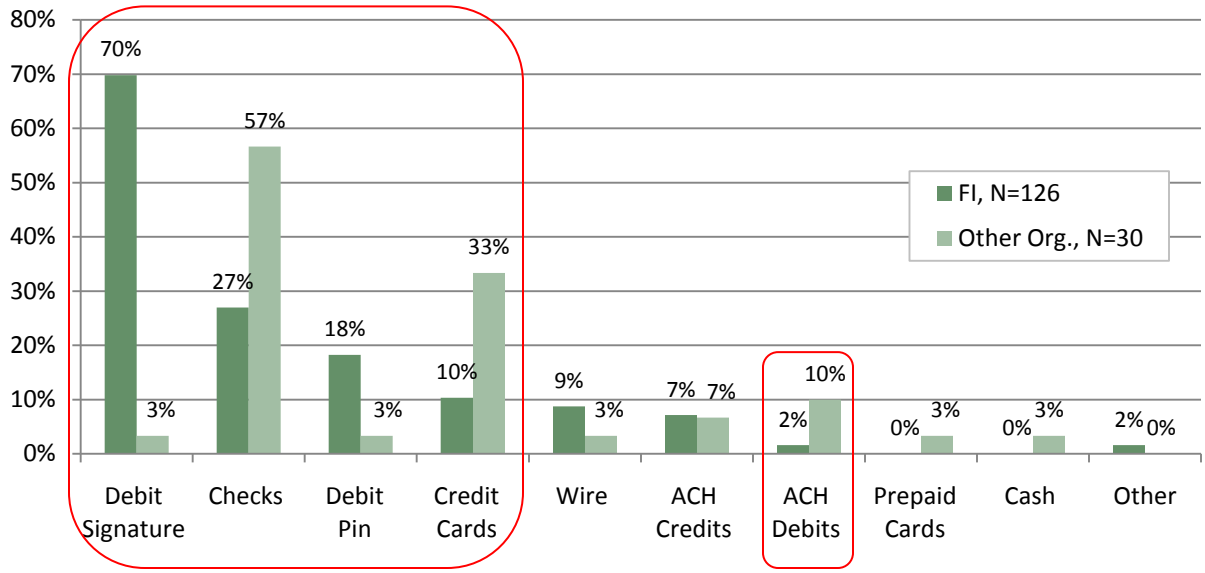
Chart F: Payment Types with Highest Number of Fraud Attempts by % of Respondents



Seventeen percent of all respondents reported no dollar losses due to payments fraud (6% of the FI respondents and 45% of all other respondents). Of those that experienced fraud losses, respondents were asked which payment types have the highest dollar losses as reported in Chart G. Seventy percent of the FI respondents identified signature debit cards as having the highest dollar losses, followed by check and PIN debit cards. In contrast, non-FI respondents identified check as having the highest dollar losses at 57%, followed by credit cards and ACH debits.

© 2011 Federal Reserve Bank of Minneapolis

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



For the organizations that experienced fraud losses, over 90% estimated losses as 0.5% or less of their annual revenue (Table 4). Of these, about 80% 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. This was also the case in 2009 when 85% of the organizations that incurred losses, estimated losses of less than 0.3% of annual revenues.

Table 4: Payments Fraud Financial Losses by % of Respondents that Incurred Losses

Loss Range as a Percent of Annual Revenue*					
	>0% - .3%	**.3% - .5%**	**.6% - 1 %**	**1% - 5%**	**Over 5%**
% of FI Respondents (N=120)	82%	11%	3%	3%	2%
% of Other Organization Respondents (N=28)	75%	11%	4%	7%	4%
% of All Respondents (N=148)	80%	11%	3%	4%	2%

*Percents by row may exceed 100% due to rounding.

The percent of respondents that experienced an increase in fraud loss declined from 44% in 2009 to 35% in 2010 (Table 5). In both years, many more FI respondents experienced an increase in financial loss due to payments fraud than did non-FI organizations. In both 2009 and 2010, the majority of non-FI organizations reported that their financial loss stayed about the same over the past year, with the numbers improving from 50% to 79% respectively. Finally, one out of ten respondents reported a decrease in financial loss due to payments fraud.

© 2011 Federal Reserve Bank of Minneapolis

Table 5: Change in Payments Fraud Losses in Last 12 Months by % of Respondents

% of Respondents	FI Respondents		Other Organizations		All Respondents	
	2010 (N=131)	2009 (N=137)	2010 (N=53)	2009 (N=38)	2010 (N=184)	2009 (N=185)
Increased	45%	50%	11%	27%	35%	44%
Stayed the same	42%	41%	79%	50%	53%	43%
Decreased	13%	9%	9%	23%	12%	12%

As shown in Charts H and I below, respondents that reported an increase in loss estimated the size of the increase. Over half of these respondents cited an increase of 1% to 5% and over 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 small for the vast majority of respondents.

Chart H: Increase in Loss Rate By % of Financial Institution Respondents N=57 (2010)

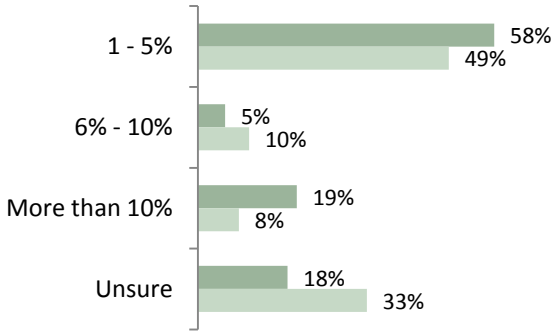
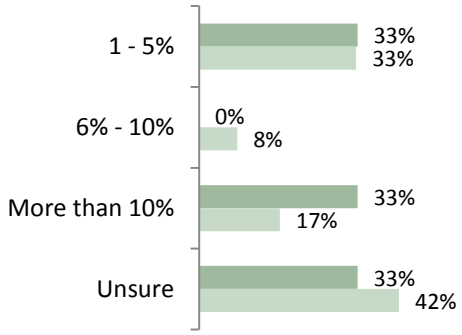


Chart I: Increase in Loss Rate By % of Other Organization Respondents N=6 (2010)



Respondents identified key factors underlying the increases in fraud losses they experienced as listed in Table 6. The top three were stolen or counterfeit cards, use of the Internet enabling fraud, and a data breach at an external organization. Responses vary between FI respondents and other organizations, but only six non-FI organizations reported increases. Top factors for FI respondents in 2009 were debit card use and liability for loss, lack of customer knowledge and care in protecting payments data, followed by stolen or counterfeit cards and a data breach at an external organization, which were cited by an equal number of FIs. Other organizations identified the state of the economy as the top factor in 2009.

© 2011 Federal Reserve Bank of Minneapolis

Table 6: Key Factors for Increase in Fraud Losses by % of Respondents

Key Factors for Increase in Fraud Losses	FI (N=57)	Other Org. (N=6)	All (N=63)
Stolen or counterfeit cards	70%	50%	68%
Use of internet enabling fraud	56%	0%	51%
Data breach at external organization, e.g., payments processor, merchant	46%	33%	44%
Criminal activity increased due to low likelihood of getting caught, prosecuted and light penalties	40%	50%	41%
Lack of customer knowledge or care in protecting payments data and/or processes	42%	17%	40%
Compromised payments data disclosed by consumer	37%	17%	35%
Increase in payments activity/customer base	28%	0%	25%
State of the economy	19%	33%	21%
Shift in payment types used and associated rules limiting liability of other parties to payment	18%	17%	17%
Other	9%	33%	11%

Decreases in the rate of fraud losses experienced in the last 12 months were reported by 12% of the respondents. The majority of these respondents were unsure about the size of the decrease in the fraud loss rate; another 20% estimated a 1% to 5% reduction as reflected in Charts J and K. In 2010, nearly all of the FI respondents reporting a decrease in financial loss were under $100 million in annual revenues compared to 45% in 2009. Decrease rates varied somewhat between FI and non-FI organizations. In both years, most of the organizations that reported a decrease in their loss rate also reported no financial loss or losses of less than 0.3% of annual revenues (82% in 2010, and 96% in 2009).

Chart J: Decrease in Loss Rate By % of Financial Institution Respondents N=17 (2010)

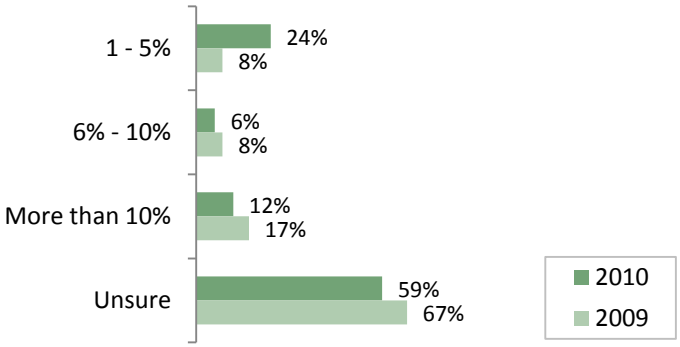
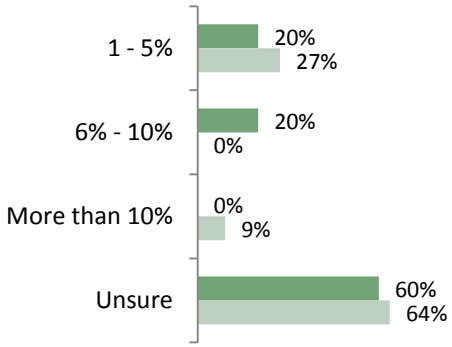


Chart K: Decrease in Loss Rate By % of Other Organization Respondents N=5 (2010)



© 2011 Federal Reserve Bank of Minneapolis

Respondents were asked to identify key factors that contributed to the decrease in fraud losses. Over half of the respondents identified staff training and education, enhanced internal controls, and enhanced fraud-monitoring systems (Table 7). In the 2009 survey, non-FI respondents identified ACH controls—payee positive pay, positive pay and filters as the top factors. These remained important in 2010, but were not the top factors. The top three factors for FI respondents did not change since 2009.

Table 7: Key Factors for Decrease in Fraud Losses by % of Respondents

Key Factors for Decrease in Fraud Losses	FI (N=17)	Other Org. (N=5)	All (N=22)
Staff training and education	82%	80%	82%
Enhanced internal controls	59%	80%	64%
Enhanced fraud monitoring system	65%	40%	59%
Customer education	47%	40%	45%
Use of check holds	35%	0%	27%
Use of ACH filters	12%	40%	18%
Use of ACH positive pay and payee positive pay	0%	40%	9%
Criminal activity decreased due to high likelihood of getting caught or prosecuted and stiff penalties	6%	20%	9%
Other	12%	20%	14%

c. Perpetrators Involved in Successful Payments Fraud

Respondents reported that external parties were most often responsible for successful fraud attempts; with 64% (65% of FIs and 56% of all others) attributing all successful fraud attempts to external parties—an increase of 3% compared to 2009 survey results. Consistent with the 2009 results, another 13% of respondents (14% of FIs and 8% of all others) could not determine the type of perpetrators involved in any of the successful fraud attempts. Finally, about 21% of respondents blamed a mix of perpetrators.

Table 8: Successful Fraud by Perpetrators Involved by % of Respondents (N=137)

Portion of Successful Payments Fraud by Perpetrators Involved					
Perpetrators	**1-25%**	**26 - 50%**	**51-75%**	**76-99%**	**100%**
Internal Only	4%	1%	1%	1%	2%
Internal w/External	4%	1%	1%	1%	0%
External Only	4%	4%	3%	7%	64%
Could Not Determine	8%	3%	1%	2%	13%

21% of respondents attributed a portion of successful fraud to more than one perpetrator category.

79% of respondents attributed all successful fraud to a single perpetrator category.

© 2011 Federal Reserve Bank of Minneapolis

d. Most Common Fraud Schemes

For payments accepted, the top three schemes most often used in both 2010 and 2009 were counterfeit and stolen cards used at the point-of-sale or on-line and counterfeit checks in general. However, the total percentage of organizations that reported counterfeit checks as a most common scheme declined slightly in 2010.

For FI respondents, the top schemes involving payments accepted also remained the same in 2010 as in 2009 (Chart L). That said, a somewhat smaller percent identified counterfeit check and counterfeit or stolen cards used at POS in the top three schemes.

Thirty-four percent of non-FI respondents reported check fraud in the top three schemes most often used, which is 15% to 25% below 2009 levels (Chart M). Fraudsters appear to have diversified in 2010. Also, top schemes were typically industry neutral. In 2010, however, most respondents reporting cash register frauds were from the retail industry, whereas in 2009, none of the respondents that reported cash register frauds were retail organizations.

Chart L: Top 3 Current Fraud Schemes Involving Payments Accepted by % of Financial Institution Respondents (N= 119 for 2010)

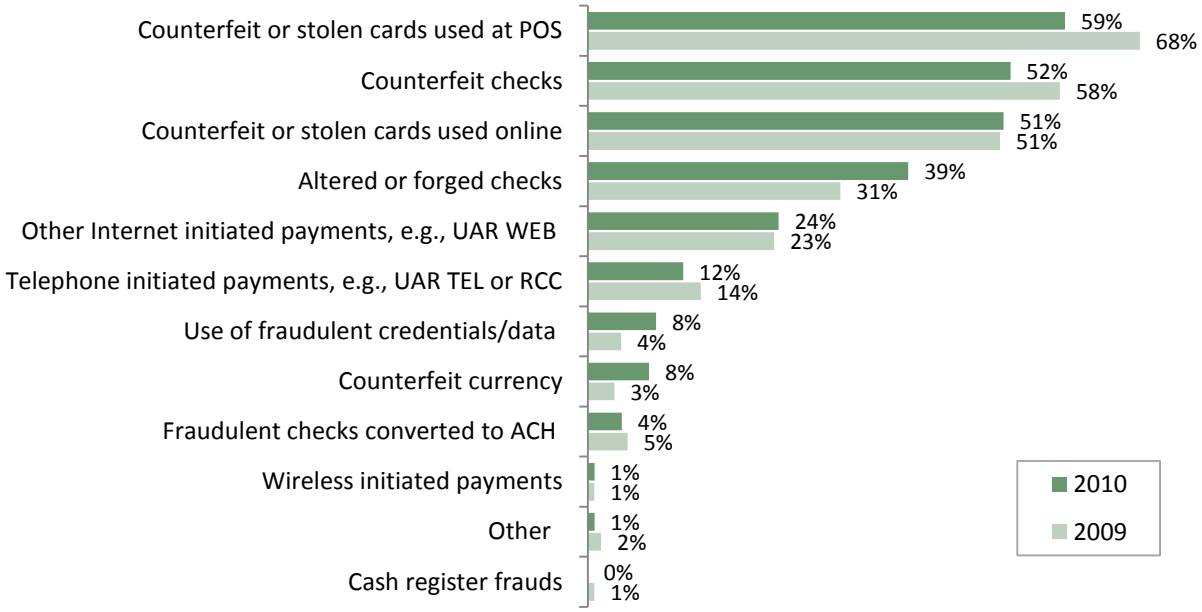
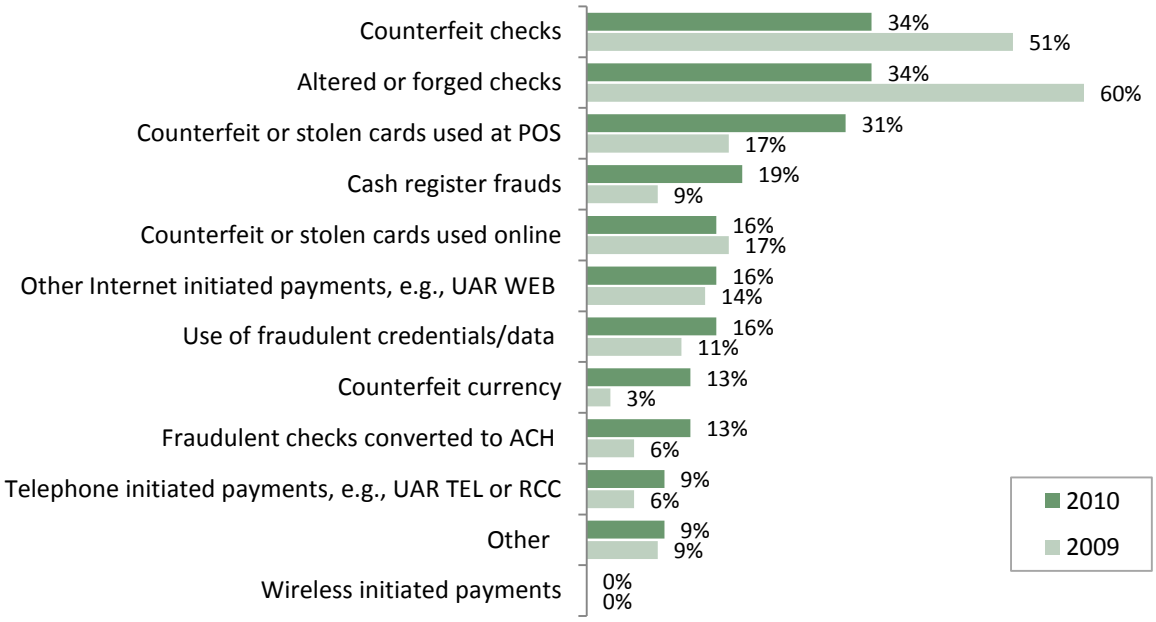


Chart M: Top 3 Current Fraud Schemes Involving Payments Accepted by % of Other Organization Respondents (N=32 for 2010)



Regarding common schemes used by fraudsters against the organization's own accounts, over 26% of FI respondents and 12% of non-FI respondents reported no fraud. 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.

About half of the respondents that experienced fraud against their organization's own account identified counterfeit checks and altered or forged checks in the top three schemes most often used (Charts N and O).[3] About 90% of respondents with annual revenues of $1 billion or more and 51% of those respondents with revenue under $1 billion reported counterfeit checks in the top three schemes.

For FIs that experienced fraud against their own accounts (Chart N), the percent of respondents reporting counterfeit checks and fraudulent or unauthorized ACH debits in the top three schemes declined between 2009 and 2010 from 55% to 51% and from 57% to 45%, respectively.

As shown in Chart O, changes between years for non-FIs appear material. Although non-FI respondents continued to report check schemes in the top three most often used schemes against the organization's own accounts, the percentage declined by over 20% compared to 2009. The percent of non-FIs reporting fraudulent or unauthorized debits also declined from 46% in 2009 to 31% in 2010. On the other hand, the percent of non-FIs that reported fraudulent or unauthorized corporate or commercial card transactions among the top three schemes jumped from 8% in 2009 to 38% in 2010. Respondents reporting corporate and commercial card fraud in the top schemes spanned a variety of industries and

[3] The 2009 data has been revised to exclude respondents that indicated no fraud against their organization's own accounts. In the 2009 Payments Fraud Survey Results Summary, those respondents were captured in the "Other" percentage.

© 2011 Federal Reserve Bank of Minneapolis

size of company. Finally, only 3% of respondents identified most often-used schemes as involving a breach of access or other data security controls, including account takeovers, to their payment processes.

Chart N: Fraud Schemes Involving Organization's Own Accounts by % of Financial Institution Respondents (N = 67 for 2010)

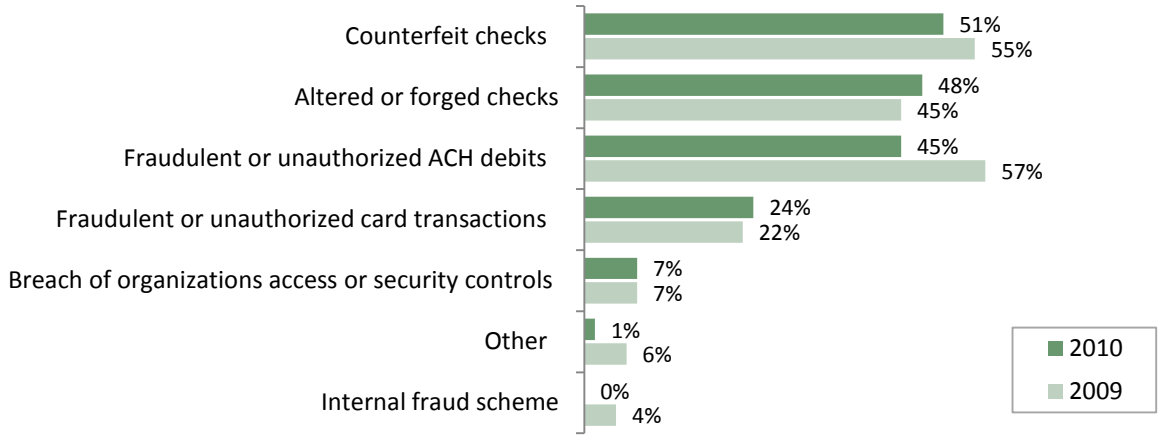


Chart O: Fraud Schemes Involving Organization's Own Accounts by % of Other Organization Respondents (N=29 for 2010)

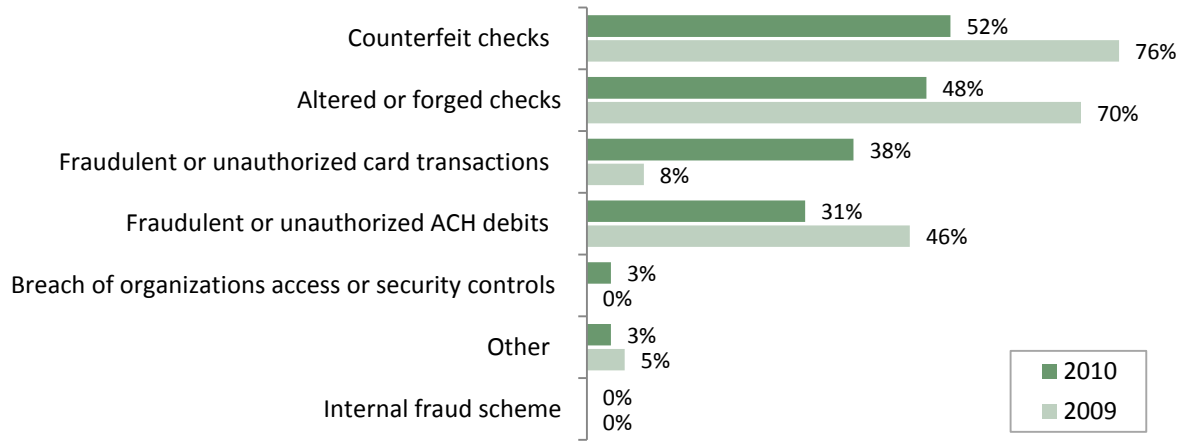


Table 9 lists the top three sources of information used in the top fraud schemes. Nearly half of the respondents identified "sensitive" information obtained from a lost or stolen card, check or other physical document or device while in the consumer's control. Information sources identified by FI respondents versus other organizations differed. For example, over half of non-FI respondents reported that their organization's information was obtained from a legitimate check issued by the organization.

© 2011 Federal Reserve Bank of Minneapolis

Table 9: Top 3 Information Sources Used in Fraud Schemes

Information Sources Used in Fraud Schemes	FI (N=107)	Other Org. (N=30)	All (N=137)
"Sensitive" information obtained from lost or stolen card, check, or other physical document or device while in consumer's control	54%	30%	49%
Phishing, spoofing, pharming or other "cyber attacks" used to obtain "sensitive" customer information	49%	17%	42%
Skimming of card magnetic stripe information	41%	3%	33%
Organization's information obtained from a legitimate check issued by your organization	22%	53%	29%
Information about customer obtained by family or friend	19%	20%	19%
Data breaches due to lost or stolen physical documentation or electronic PC/device while in control of the organization	8%	0%	7%
Employee with legitimate access to organization or customer information	1%	23%	6%
Data breaches due to cyber attacks against organization's information e.g., computer hacking	6%	3%	5%
Other	3%	7%	4%

FI respondents were asked about any experience with fraud involving a consumer's claim that an ACH debit made to their bank account was unauthorized. The NACHA rules require a consumer to submit a "written statement of unauthorized debit" (WSUD) to make such a claim within 60 days from the settlement date of the original transaction. When a claim is made, the consumer's FI (or Receiving Depository Financial Institution) returns the ACH debit. While most consumer claims of unauthorized ACH debits are legitimate, a majority of FIs report some number of claims as fraudulent (Table 10).[4] Surprisingly, 9% of the FI respondents estimated over 50% of the WUSDs they received are false or fraudulent.

[4] A NACHA rule change modified the form of the written statement required from the consumer. Prior to 2010, a "written statement under penalty of perjury" was required.

© 2011 Federal Reserve Bank of Minneapolis

Table 10: False or Fraudulent Consumer WUSD Claims by % of Respondents

Estimated Percent of False or Fraudulent Consumer Claims Made by WSUD								
	0%	**1-5%**	**6-10%**	**11-15%**	**15-20%**	**21-30%**	**31-50%**	**Over 50%**
% of Financial Institutions in 2010 (N=104)	25%	46%	6%	4%	3%	3%	5%	9%
% of Financial Institutions in 2009 (N=109)	22%	51%	5%	3%	5%	3%	5%	5%

e. Payments Fraud Mitigation Methods Used

Respondents were asked about their use and the effectiveness of various types of fraud mitigation methods and tools. Questions were asked in three areas including: i) internal controls and procedures, ii) customer authentication, transaction screening and risk management approach, and iii) risk mitigation services offered by financial institutions. Between 2009 and 2010, the percent of respondents using mitigation methods changed. This may be due in part to the differences in the mix of non-FI organizations, based on annual revenues, that responded to these questions in 2009 and 2010. In 2009, 20% of the non-FIs had annual revenues under $50 million compared to 2010 when 50% of the non-FI respondents had revenue under $50 million. Further, among all respondents 5% had annual revenues over $1 billion in 2009 compared to 9% in 2010.

i. ***Internal Controls and Procedures.*** Internal controls and procedures are the fraud mitigation methods most used by respondents. Over 80% of FIs and 60% of other organizations use a majority of the 15 internal controls and procedures listed on Charts P and Q below. Further, internal controls are used broadly—i.e., 10 controls are used by 75% of the FI respondents and three controls are used by the same percentage of other respondents.

   Between 2009 and 2010, some changes occurred in the non-FI use of internal controls and procedures, but the three methods with the highest use rate stayed the same—"authentication and authorization controls to payment processes," "physical access controls to payment processing functions," and "dual controls and separation of duties within payment processes." Increased use was reported for "separate banking accounts by payment type" and "use of an employee hotline to report potential fraud" by 15% and 18%, respectively. Finally, for most of the controls that showed a decline in use, respondents not using the controls were small organizations—i.e., with annual revenues under $50 million.

© 2011 Federal Reserve Bank of Minneapolis

Chart P: Use and Effectiveness of Internal Controls and Procedures by % of Financial Institution Respondents (N=103)

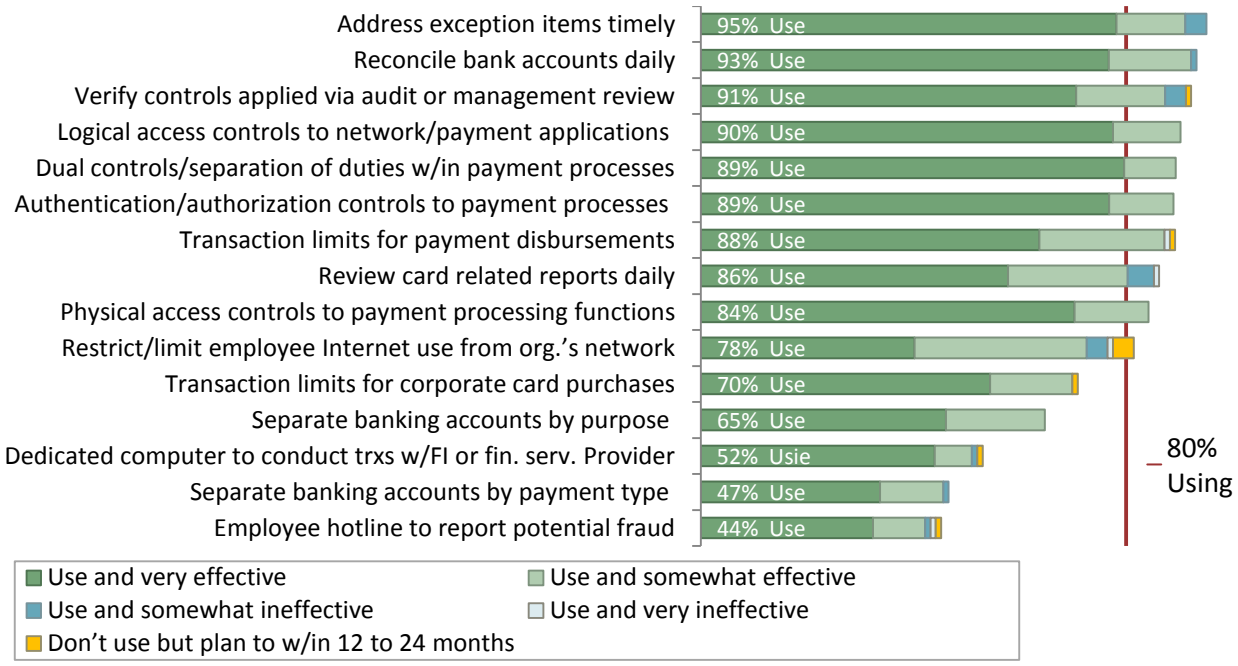
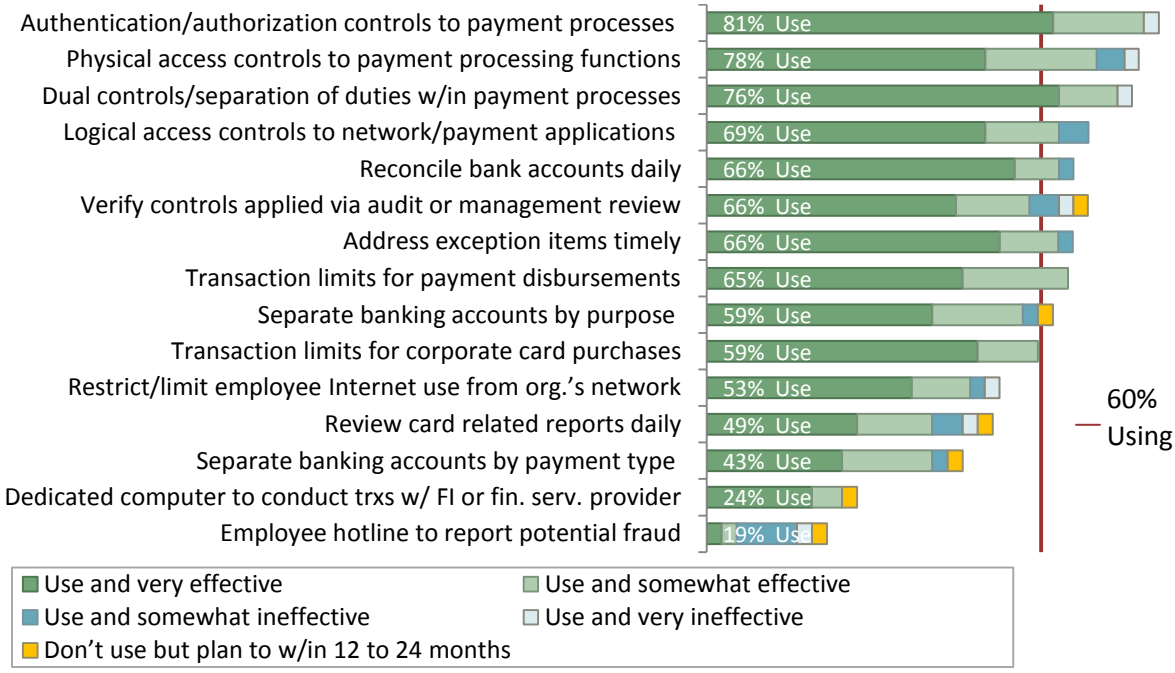


Chart Q: Use and Effectiveness of Internal Controls and Procedures by % of Other Organization Respondents (N=40)



© 2011 Federal Reserve Bank of Minneapolis

ii. ***Customer Authentication, Transaction Screening and Risk Management Approach.*** Use of different methods to authenticate customers, screen transactions and apply centralized risk management varied significantly in overall adoption between FIs and other organizations (Charts R and S). With two exceptions—"use of a centralized risk management department" and "verify customer's state ID card is authentic"—a larger percent of non-FI respondents have adopted these methods compared to FI respondents. The most material difference is in FI's participation in fraudster databases and receipt of alerts, which 73% of the FI respondents indicate using compared to only 8% of other organizations.

Although overall use rates of customer authentication, et. al. are lower than those for internal controls and procedures, these rates are still high with 60% of the FI respondents using half of these methods. Further, the use rates for several methods increased by 10% between 2009 and 2010, including "fraud detection pen for currency," "centralized fraud information database of one payment type" and "multiple payment types." Interestingly, usage fell the most for human review of payment transactions, which dropped from 79% in 2009 to 68% in 2010. This may be due to the substitution of more automated methods—e.g., the use of fraud detection software for pattern matching or other indicators increased 4%, and in both 2009 and 2010 had the highest percent (6% - 7%) of FIs planning to use it in the next 12 to 24 months.

Chart R: Authentication, Transaction Screening and Risk Management by % of Financial Institution Respondents (N=106)

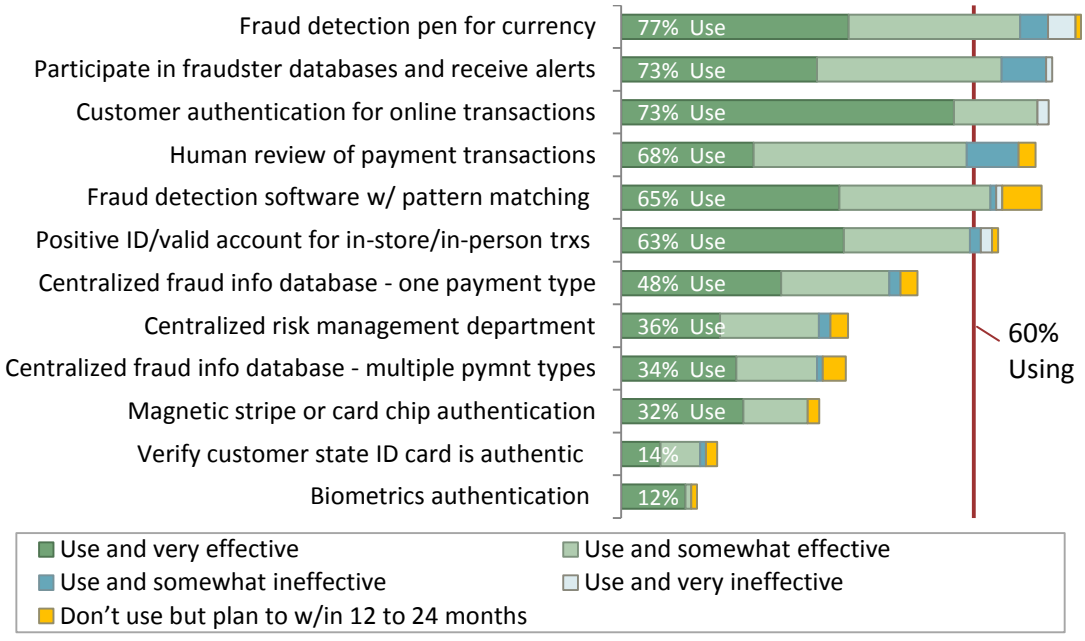
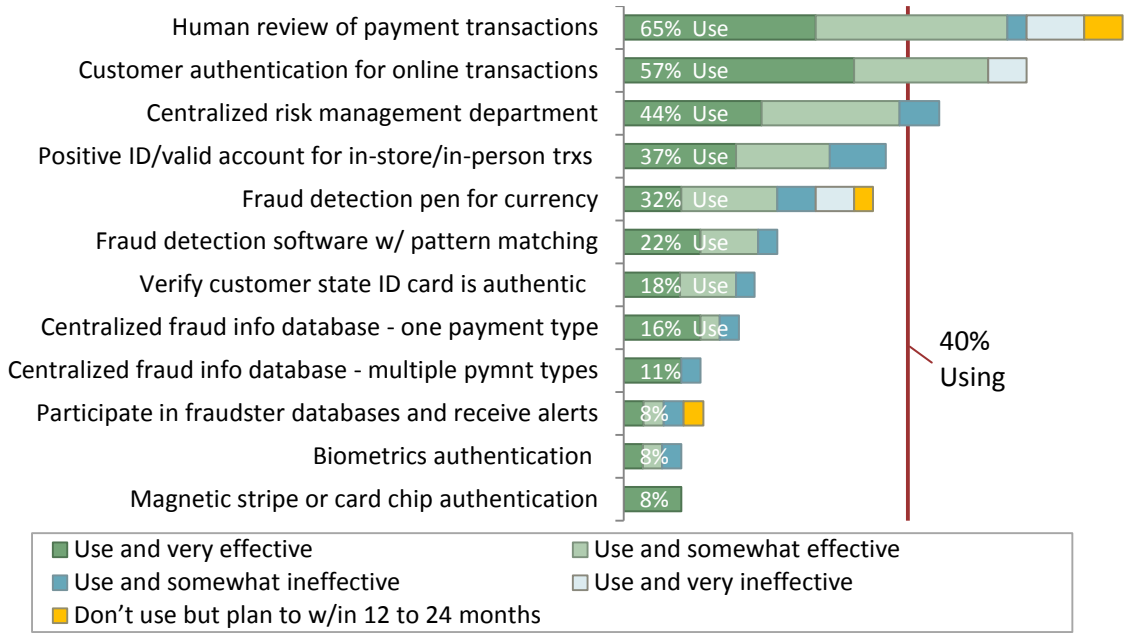


Chart S: Authentication, Transaction Screening and Risk Management by % of Other Organization Respondents (N=38)

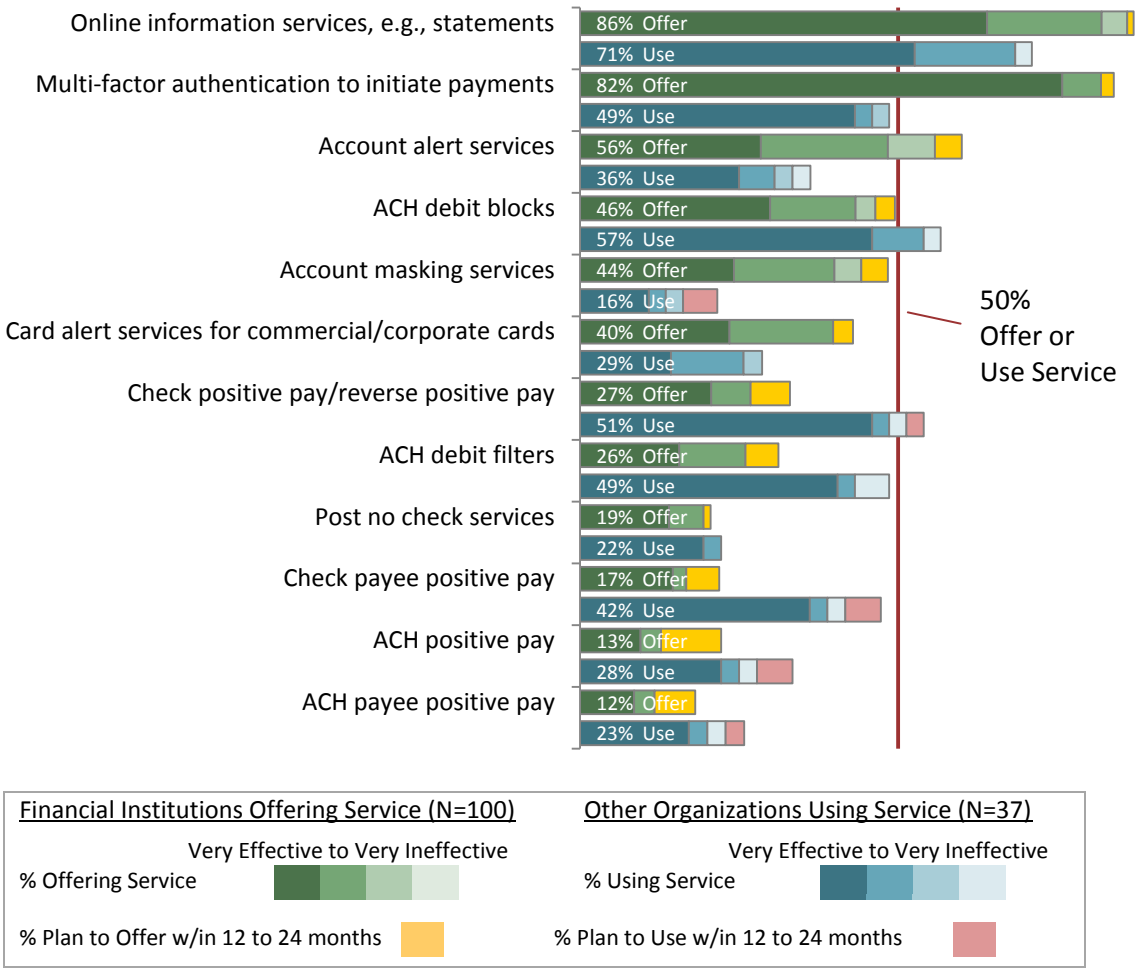


iii. ***Risk Mitigation Services Offered by Financial Institutions.*** The top five methods used by respondents as reported in Chart T are online information services, ACH debit blocks, check positive pay/reverse positive pay, ACH debit filters, and multi-factor authentication to initiate payments. These are the same services identified as the most used services in the 2009 survey. Usage rates in 2010 are materially lower ranging from 20% to 40% lower in 2010 than in 2009, which might be explained by the change in respondent mix relative to size of annual revenue—i.e., an increase in small organizations responding. In the 2009 survey, all five services reflected use rates of 90% or more. All of the top five risk mitigation services are used to help lower the risk of payments fraud against an organization's own accounts. Four of these focus on preventing successful fraud and one on addressing possible fraudulent exception items.

Two of the top five risk-mitigation services used are offered by over 80% of the FI respondents. The other three (ACH debit blocks, check positive pay/reverse positive pay, ACH debit filters) are offered by a much lower rate of FI respondents. These results raise two questions. First, is the level of availability sufficient to meet demand, suggesting that demand for these services is relatively low? Second, are smaller organizations underserved relative to both availability and cost? In the next section, barriers to fraud mitigation are discussed and cost is a key factor for non-FI respondents, (Table 11).

© 2011 Federal Reserve Bank of Minneapolis

Chart T: Financial Institution Risk Mitigation Services Offered and Used by % of Respondents



© 2011 Federal Reserve Bank of Minneapolis

f. Barriers to Reduce Payments Fraud

Respondents reported on barriers to further reducing payments fraud. Most identified a version of "cost" as the main barrier citing lack of resources, implementation costs, and lack of compelling business case as the main barriers. A complete summary is listed in Table 11.

Table 11: Main Barriers to Payments Fraud Mitigation by % of Respondents

	FI (N=92)		Other Org. (N=34)		All (N=126)	
	2010	**2009**	**2010**	**2009**	**2010**	**2009**
Lack of staff resources	54%	56%	53%	52%	54%	55%
Cost of implementing in-house fraud detection tool/method	52%	62%	38%	48%	48%	58%
Cost of implementing commercially available fraud detection tool/service	48%	57%	41%	52%	46%	56%
Lack of compelling business case (cost versus benefit) to adopt new or change existing methods	47%	36%	35%	55%	44%	41%
Consumer data privacy issues/concerns	38%	37%	41%	34%	39%	37%
Corporate reluctance to share information due to competitive issues	9%	5%	3%	10%	7%	7%
Unable to combine payment information for review due to operating in multiple states	2%	3%	3%	10%	2%	5%
Unable to combine payment information for review due to operating with multiple banks	2%	2%	3%	14%	2%	5%
Other	4%	2%	15%	10%	7%	4%

g. Opportunities to Reduce Payments Fraud

Respondents reported on opportunities to reduce fraud in three areas: i) organization actions, ii) industry actions, and iii) legal and regulatory changes.

i. ***Organization Actions.*** About two-thirds of the respondents said their organizations should apply controls over Internet payments and about the same number of respondents said their organizations should share information about emerging fraud tactics being conducted by criminal rings.

© 2011 Federal Reserve Bank of Minneapolis

Table 12: New Methods Needed by Organizations by % of Respondents

	FI (N=95)	Other Org. (N=31)	All (N=126)
Controls over Internet payments	67%	65%	67%
Information sharing on emerging fraud tactics being conducted by criminal rings	62%	74%	65%
Restrict access to customer DDA accounts	23%	26%	24%
Other	12%	13%	12%

ii. ***Industry Actions.*** In general, respondents supported industry-sponsored actions to reduce payments fraud with two of three organizations supporting industry specific education on fraud prevention and best practices and industry alert services. All three ideas listed in the survey were supported as shown in Table 13.

Table 13: Industry Considerations by % of Respondents

	FI (N=95)	Other Org. (N=38)	All (N=133)
Industry specific education on fraud prevention best practices	73%	74%	73%
Industry alert services	66%	61%	65%
Industry sponsored fraudster databases	55%	66%	58%
Other	7%	0%	5%

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 more likely prosecution were identified by many. FI respondents identified placing more responsibility on customers for protecting information, and more responsibility and liability for fraudulent payments on the entity that initially accepts the card. Other organizations identified improved law enforcement cooperation as a consideration. Table 14 lists these and other considerations.

© 2011 Federal Reserve Bank of Minneapolis

Table 14: Legal and Regulatory Considerations by % of Respondents

Information Sources Used in Fraud Schemes	FI (N=104)	Other Org. (N=39)	All (N=143)
Increase penalties for fraud and attempted fraud	70%	67%	69%
Place more responsibility on consumers and customers to reconcile and protect their payments data	79%	26%	64%
Strengthen disincentives to committing fraud through stiffer penalties and more likely prosecution	59%	72%	62%
Place responsibility to mitigate fraud and shift liability for fraudulent card payments to the entity that initially accepts the card payment	79%	18%	62%
Improve law enforcement cooperation on domestic and international payments fraud and fraud rings	38%	69%	46%
Align Regulation E and Regulation CC to reflect changes in check collection systems' use of check images and conversion of checks to ACH	52%	26%	45%
Assign liability for fraud losses to the party most responsible for not acting to reduce the risk of payment fraud	47%	26%	41%
Assign responsibility for mitigating fraud risk to the party best positioned to take action against fraud	40%	26%	36%
Focus future legal or regulatory changes on data breaches to where the breaches occur	30%	15%	26%
Establish new laws/regs or change existing ones in order to strengthen the management of payments fraud risk	18%	28%	21%
Other	2%	8%	3%

h. Conclusions

Considered as a whole, the results of the 2010 payments fraud survey suggest the following:

- Payments related fraud remains a significant concern of financial institutions and other corporations in the region, including very small organizations that responded to the Minneapolis Federal Reserve's 2010 payments fraud survey.
- Most problematic is fraud that affects checks and debit cards, as these are the payment types that were most often attacked by fraud schemes and that sustained the highest losses as a result. These results are generally consistent with a similar 2009 survey conducted by the Minneapolis Fed and with fraud surveys conducted by national industry associations.[5]

[5] American Bankers Association, 2009 ABA Deposit Account Fraud Survey Report; Association for Financial Professionals 2011 AFP Payments Fraud and Control Survey Report of Survey Findings.

© 2011 Federal Reserve Bank of Minneapolis

- Within the ACH is a process for consumers to return debit payments as unauthorized, called written statement of unauthorized debit. While the vast majority of these are legitimate transactions, a small number of financial institutions report a surprisingly high number of WSUDs, up to 50%, as fraudulent. The 2009 survey identified a similar condition.
- While corporate account take-over fraud 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 0.3% of their annual revenues. This is consistent with 2009 results. While any loss due to fraud is undesirable, by this measure these levels are relatively small.
- Various types of internal controls and procedures are the main methods used by most organizations to mitigate payments fraud risk. Transaction monitoring, authentication, risk services offered by financial institutions are also used, but not as broadly. These are consistent with 2009 results.
- Cost is the main barrier to organizations of all kinds adopting more defenses against payments fraud. Similar results were reported in 2009.
- At the industry level, respondents believe that sharing fraud related information among organizations would help to mitigate fraud.

In summary, payments fraud is a continuing problem and source of concern that financial institutions and other organizations work hard to mitigate in order to limit financial losses.

© 2011 Federal Reserve Bank of Minneapolis