2009 Payments Fraud Survey Summary of Results

Responses from Members of Minnesota Treasury Management Association and Upper Midwest Automated Clearinghouse Association

Prepared by: Federal Reserve Bank of Minneapolis

November 2009

1. Introduction

In June 2009, the Federal Reserve Bank (FRB) of Minneapolis conducted research on payments-related fraud experienced by area organizations.[1] Members of the Minnesota Treasury Management Association (MTMA) and the Upper Midwest Automated Clearinghouse (UMACHA) responded to an online survey about payments fraud their organizations incurred and methods used to reduce fraud risk. Payments covered by the survey included business-to-business (B2B) and consumer-to-business (C2B) transactions involving cash, check, debit and credit cards, automatic clearing house (ACH), and wire transfers (here, "business" includes government and nonprofit organizations).

2. Respondent Information

The survey was sent to 1495 organizations of which 185 completed it for a response rate of 12%.[2] Seventy-four percent of respondents are financial service organizations, most of which are financial institutions. Manufacturing is the next largest industry category at 8%. The remaining 18% are split among retail, insurance, government, nonprofits, energy, health services, real estate, technology, hospitality, and consulting, as shown in Table 1. Respondents are also categorized by the organization's annual revenues, listed in Table 2. Over half the organizations have annual revenues less than $100 million, and among financial services, almost half report annual revenues less than $50 million.

Table 1: Respondents by Industry	
Business Services & Consulting	1%
Energy	1%
Financial Services	74%
Government	3%
Health Services	1%
Hospitality	1%
Insurance	3%
Manufacturing	8%
Nonprofit	2%
Real Estate	1%
Retail	3%
Software & Technology	1%
Other	2%

Table 2: Respondents by Annual Revenue	
Under $50 million	40%
$50 – 99.9 million	14%
$100 - 249.9 million	10%
$250 - 499.9 million	5%
$500 - 999.9 million	4%
$1 - 4.9 billion	11%
$5 - 9.9 billion	1%
$10 - 19.9 billion	2%
Over $20 billion	4%
Not Applicable or Don't Know	10%

3. Summary of Survey Results by Question

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

[1] Questions regarding the survey summary may be directed to Claudia Swendseid or Amanda Dorphy at the Federal Reserve Bank of Minneapolis.

[2] The survey sample is not representative of MTMA or UMACHA members, and neither are the results.

a. Payment Types Used by Respondent Organizations

ACH, check and wire transfers are the most common payment types used by respondents with over 85% accepting them from businesses and/or consumers and 75% using them to disburse payments. Less than half of respondents accept or make payments using one of the four card types. These differences in payment usage, along with differences in transaction counterparties provide a useful context for assessing later responses (Charts A-D).

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

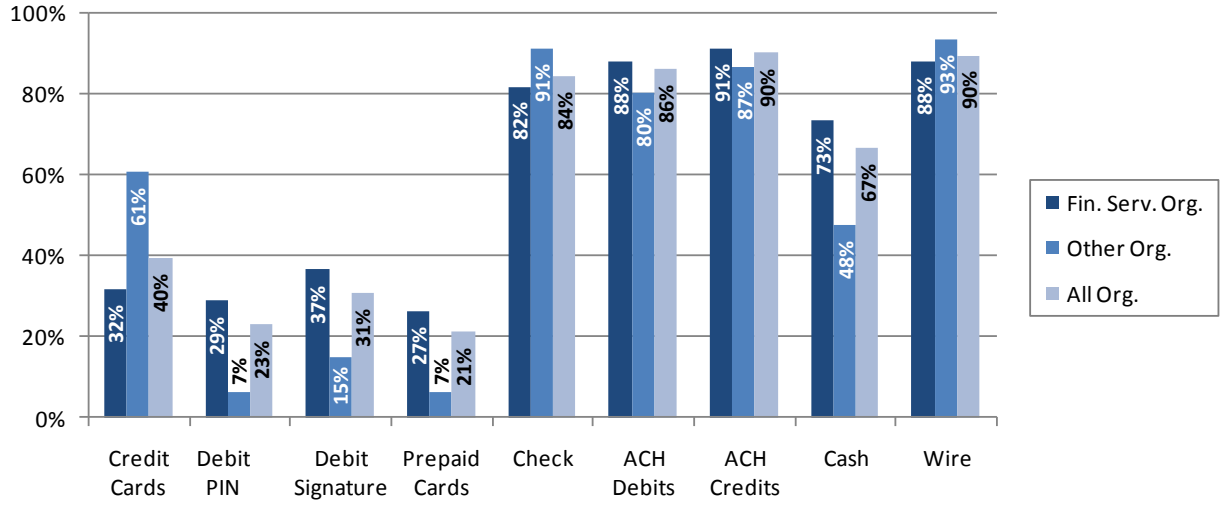


Chart B: Payment Types Accepted for C2B Payments by % of Respondents

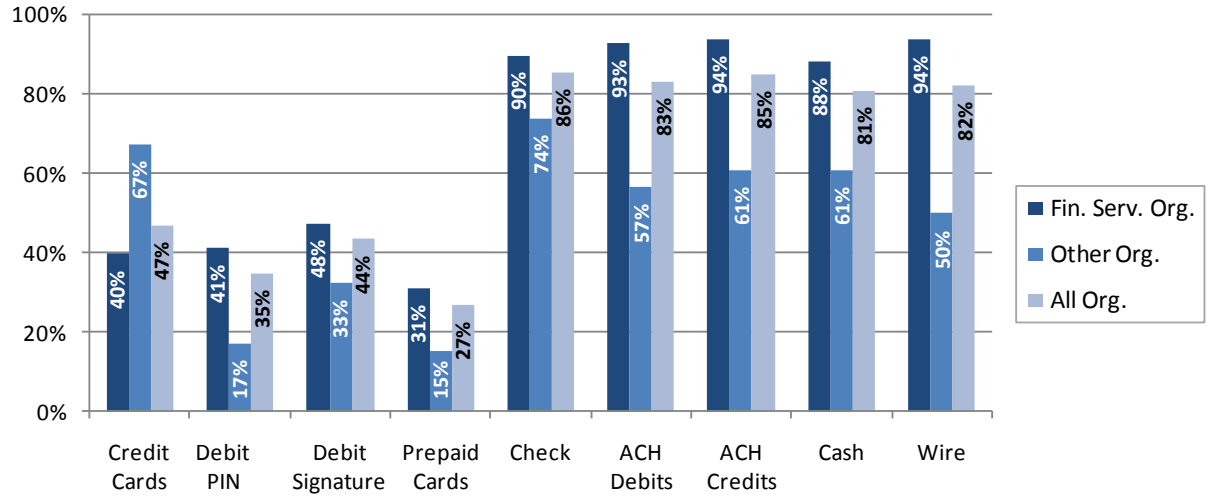


Chart C: Payment Types Used for B2B Disbursements by % of Respondents

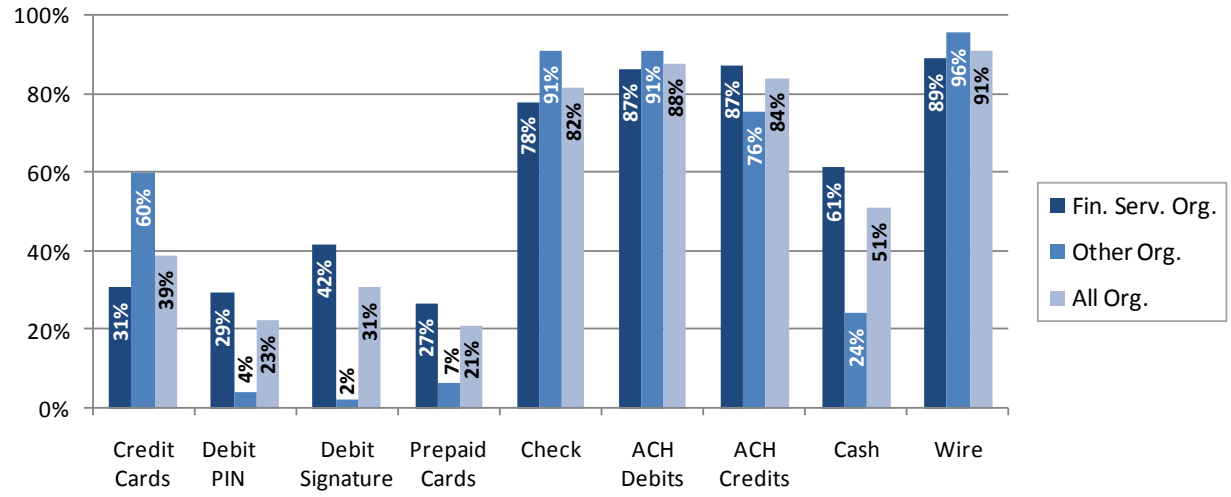
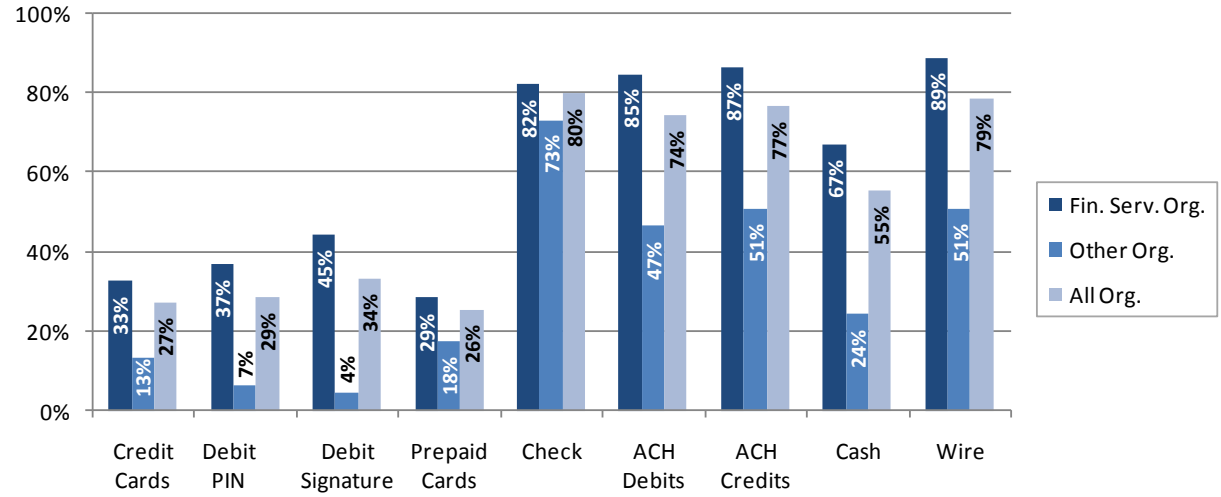


Chart D: Payment Types Used for B2C Disbursements by % of Respondents



b. Financial Losses Due to Payments Fraud

Respondents estimated the organization's financial loss due to payments fraud as a percent of total annual revenues. Table 3 shows over 87% selected the lowest range of loss available, or less than 0.3%.

Table 3: Payments Fraud Financial Losses by % of Respondents

	Loss Range as a Percent of Annual Revenue				
	Less than .3%	.3% - .5%	.6% - 1.0%	1.0% - 5.0%	Over 5%
% of All Respondents (N=181)	87.3%	6.6%	2.8%	2.8%	0.6%

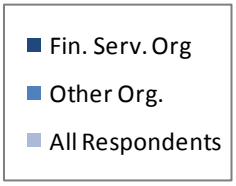
Also, most respondents said the percentage of financial loss either increased (44%) or stayed the same (43%) during the last 12 months. Fewer noted a decrease in losses, including 9% of financial service organizations and 23% of all others, as reflected in Table 4.

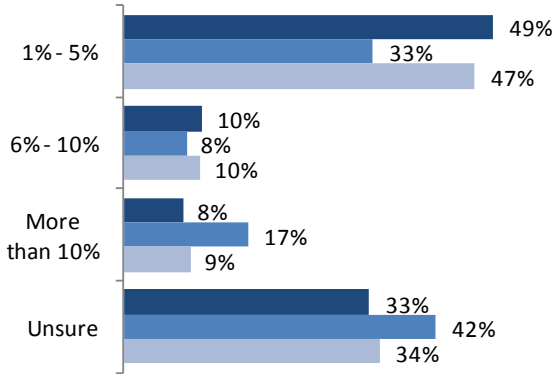
Table 4: Change in Payments Fraud Losses in Last 12 Months by % of Respondents

% of Respondents (N=184)	Financial Services Organizations	Other Organizations	All Respondents
Increased	50%	26%	44%
Stayed Same	41%	51%	43%
Decreased	9%	23%	13%

Respondents that reported an increase in fraud loss estimated the size of the increase, with about half citing an increase of 1% to 5%. The next largest group of responses was "unsure" of the increase level.

Chart E: Increase in Loss Rate by % of Respondents (N = 79)





Respondents also identified the key factors underlying the increases in fraud losses they experienced. The top four reported by financial service organizations are listed in Table 5, including compromised data, debit card rules/loss liability, lack of customer knowledge and care in protecting payments data, and stolen or counterfeit cards. The top factor identified by all other organizations was the state of the economy, cited by 25% as compared to only 9% of financial service organizations.

Table 5: Key Factors for Increased Losses by % of Financial Service Organizations

Key Factor Themes*	% of Respondents (N=65)
Compromised data (All)**	26%
Consumer disclosed data	8%
Data breach at payment processor and/or merchant	12%
Debit card rules/liability for loss	15%
Economic state	9%
Increase in payment activity/customer base	8%
Lack of customer knowledge & care in protecting payments data	14%
Online fraud or Internet used	9%
Stolen or counterfeit cards	12%

* Key factors are grouped by themes. The table lists those identified by five or more respondents.

** This theme includes any response citing compromised data or breach in the key-factor description. Many of the responses attributed the source of compromised data. The two most common were: 1) Customer disclosure of data, and 2) Data breach at external organizations, e.g., processor/merchant database compromised, processor/merchant data stolen or data breach.

When asked which payment type contributed to the increase in fraud losses, debit cards led all other categories by a wide margin. Table 6 shows 60% of financial service respondents identifying debit cards, followed by checks, which were cited by 9%.

Table 6: Payment Types Underlying Increased Losses by % of Financial Service Organizations

Payment Type	% of Respondents* (N=65)
ACH	2%
Cash	0%
Check	9%
Credit Card	5%
Debit Card	62%
Prepaid Card	0%
Wire Transfers	2%
Payment type not specified	32%

* Total exceeds 100% as some respondents indicated more than one payment type.

Decreases in the rate of fraud losses experienced in the last 12 months were reported by 13% of respondents (see Table 4 above). However, about two-thirds of these were unsure about the size of the decrease in the fraud loss rate; 17% estimated a 1% to 5% reduction, and 13% a decrease of more than 10%, reported in Table 7.

Table 7: Decreases in Financial Loss Rate by % of Respondents

	Percent Decrease in Financial Loss Rate			
	1% - 5%	**6% - 10%**	**> 10%**	**Unsure**
% of All Respondents (N=23)	17%	4%	13%	65%

As to the key factors behind the fraud loss decreases, over half of respondents noted improvements made to automated fraud detection, fraud prevention systems and/or other tools. Table 8 highlights actions by half of financial services organizations to enhance fraud-monitoring systems and by 60% of others to implement ACH related services. Enhanced internal controls were another top factor, cited by more than 20% of all respondents.

Table 8: Key Factors Underlying Decreases in Financial Losses by % of Respondents

Key Factors	Financial Service Organizations N=12	Other Organizations N=10	All Respondents N=22
Staff Training & Education	25%	0%	14%
Customer Education	8%	0%	5%
Use of Check Holds	8%	0%	5%
Enhanced Internal Controls	25%	20%	23%
ACH Positive Pay & Payee Positive Pay	0%	60%	27%
ACH Filters	0%	20%	9%
Enhanced Fraud-Monitoring System	50%	10%	32%
Other	0%	10%	5%

c. Perpetrators Involved in Successful Payments Fraud

Respondents reported that external parties were most often responsible for successful fraud attempts, with 61% attributing all successful fraud attempts to external parties. Just 2% of respondents attributed all successful fraud to internal parties only. About 24% of respondents blamed a mix of perpetrators.

Table 9: Successful Fraud by Perpetrators Involved by % Respondents (N=127)

	Portion of Successful Payments Fraud by Perpetrators Involved				
	1-25%	26-50%	51-75%	76-99%	100%
Internal Only	5%	4%	2%	1%	2%
Internal w/External	4%	5%	1%	0%	1%
External Only	8%	6%	1%	6%	61%
Could Not Determine	6%	6%	1%	6%	13%

24% of respondents attributed a portion of successful fraud to more than one perpetrator category.

76% of respondents attributed all successful fraud to a single perpetrator category.

d. Most Common Fraud Schemes

Respondents were asked to identify the main fraud schemes they experience involving payments the organization accepts and against the organization's own accounts. Chart F lists the top fraud schemes for payments accepted, which differed between financial services and all other organizations. Most prevalent schemes reported by financial services were counterfeit or stolen cards used at the point-of-sale (POS) or with online sales, and counterfeit checks at the POS or over-the-counter (OTC). The most prevalent schemes reported by all other organizations were altered, forged and counterfeit checks they accepted.

Chart G lists the fraud schemes reported by respondents that targeted the organization's own accounts. The most prevalent involved counterfeit, altered or forged checks, and fraudulent ACH debits. The volume and value of ACH debits returned based on a consumer's claim that the transaction was not authorized frequently serves as a proxy for fraud in the ACH Network—i.e., the unauthorized debit is assumed to be a deliberate attempt to take funds from the consumer's account fraudulently[3].

Chart F: Fraud Schemes Involving Payments Accepted by % of Respondents

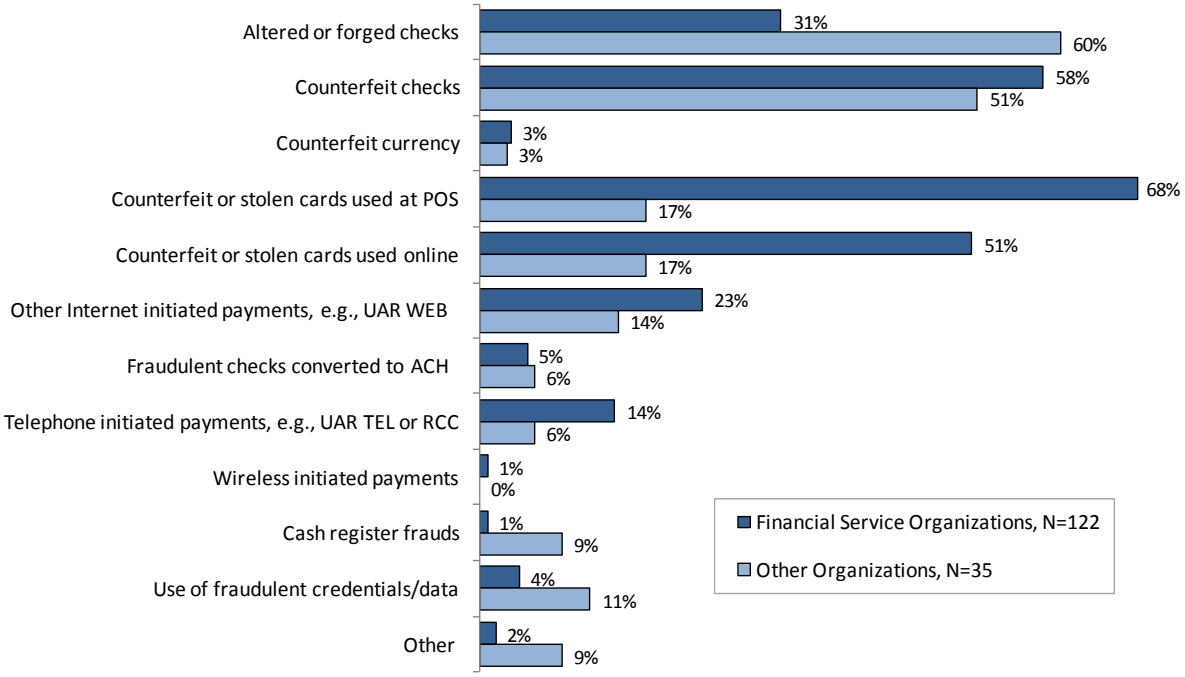
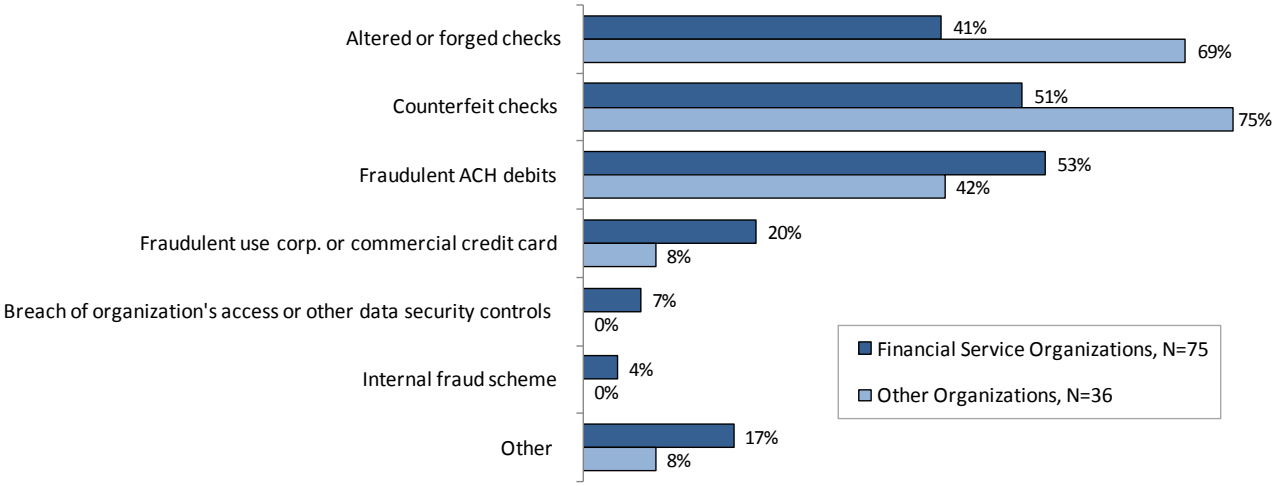


Chart G: Fraud Schemes Involving Organization's Own Accounts by % of Respondents



[3] ACH debit transactions that are in fact unauthorized are not necessarily fraudulent. For example, an ACH debit authorized for $60, but due to a data entry error is processed as $80, would be an unauthorized ACH transaction.

Financial institution respondents were also 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 consumers to submit a "written statement under penalty of perjury" (or WSUPP) to make such a claim within 60 days from the settlement date of the original transaction. Subsequently, the consumer's financial institution (or RDFI) returns the ACH debit. While most consumer claims of unauthorized ACH debits are legitimate, survey respondents indicate that a small number are fraudulent as reported in Table 10. Half of respondents estimate that 1% to 5% of consumer WSUPPs they receive involve a false or fraudulent claim, another 22% estimate no fraud, and the rest split across several categories, including 5% of institutions that report a surprisingly high percentage of fraudulent WSUPPs at over 50%.[4]

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

Estimated Percent of False or Fraudulent Consumer Claims Made by WSUPP								
	0%	1-5 %	6 -10%	11-15%	15-20%	21-30%	31-50%	Over 50%
% of Financial Institutions (N=109)	22%	51%	5%	3%	5%	3%	5%	5%

e. Payments Fraud Mitigation Methods Used

Respondents were asked about use and 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.

i. ***Internal Controls and Procedures.*** Among the fraud mitigation areas reviewed, internal controls and procedures are most used by respondents. In fact, a number of internal controls are used by 90% or more of respondents including authentication/authorization controls with payment processes, dual controls and separation of duties within payments initiation and receipt processes, and audit or management review to verify that controls are applied. Other controls have equally high adoption rates, but these differ by financial services and all other organizations. Nearly all controls were rated as effective by 90% of the organizations that use the control. Interestingly, an employee hotline to report potential fraud was ranked lowest in terms of use and effectiveness by both financial services and low by all other organizations. Charts H and I follow with more details.[5]

[4] A consumer might falsely claim that an ACH debit to their bank account was unauthorized due to "buyer's remorse" or for other reasons.

[5] The charts show only respondents that are currently using or plan to use an internal control or procedure. Those indicating "no opinion" or "do not use or does not apply" make up the remaining percentage.

Chart H: Use and Effectiveness of Internal Controls and Procedures by % of Financial Service Organizations (N=88 to 101)

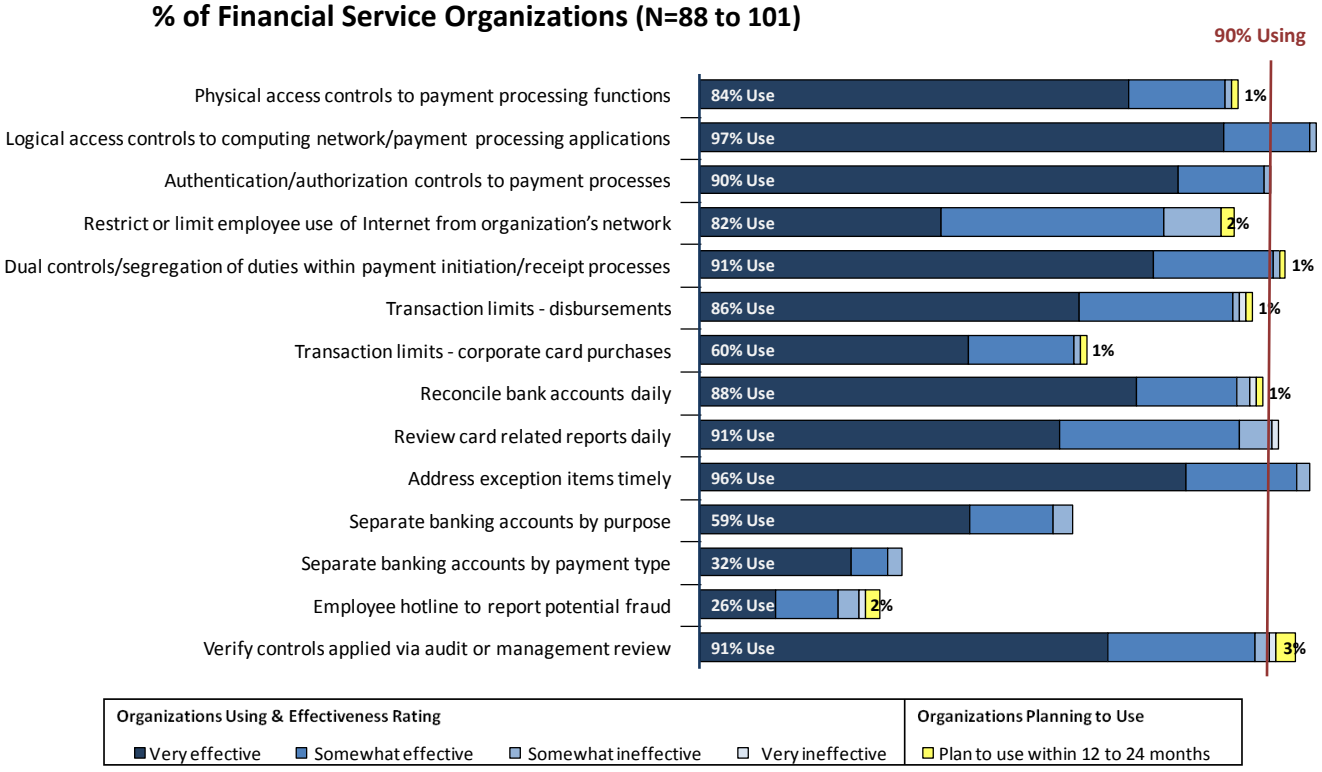
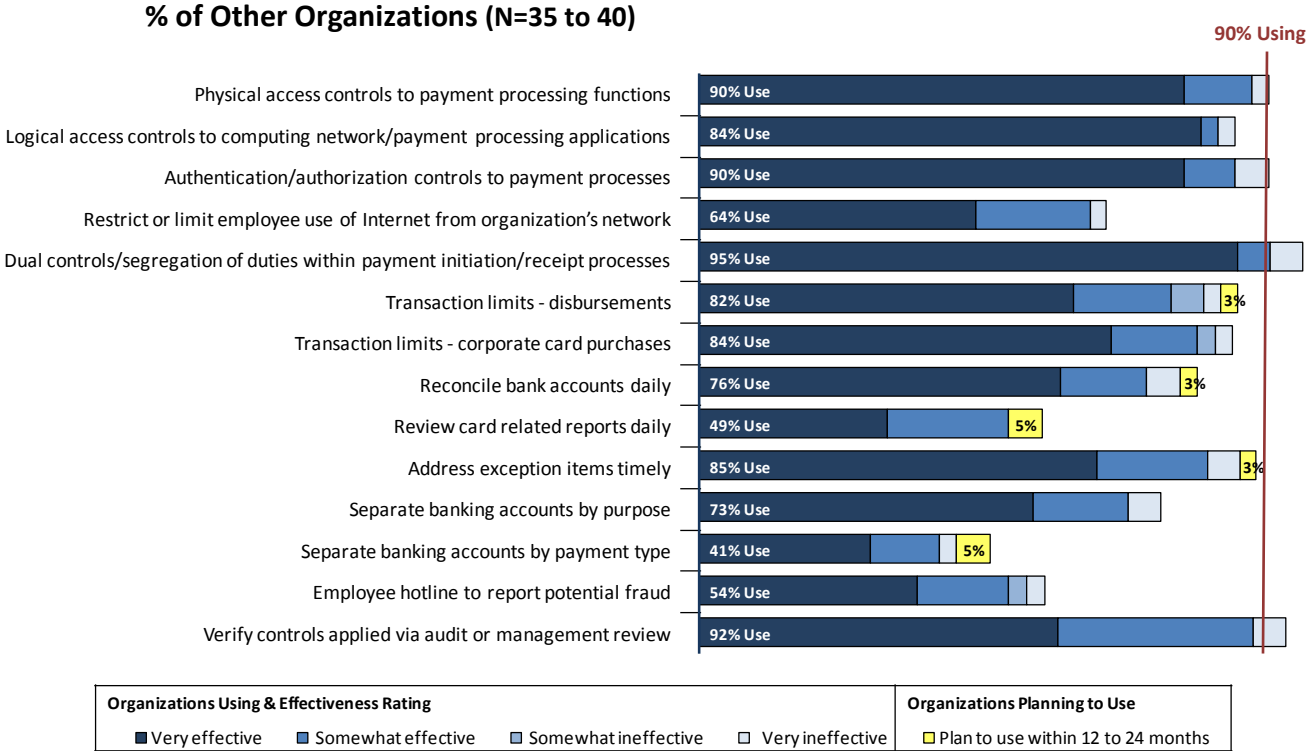
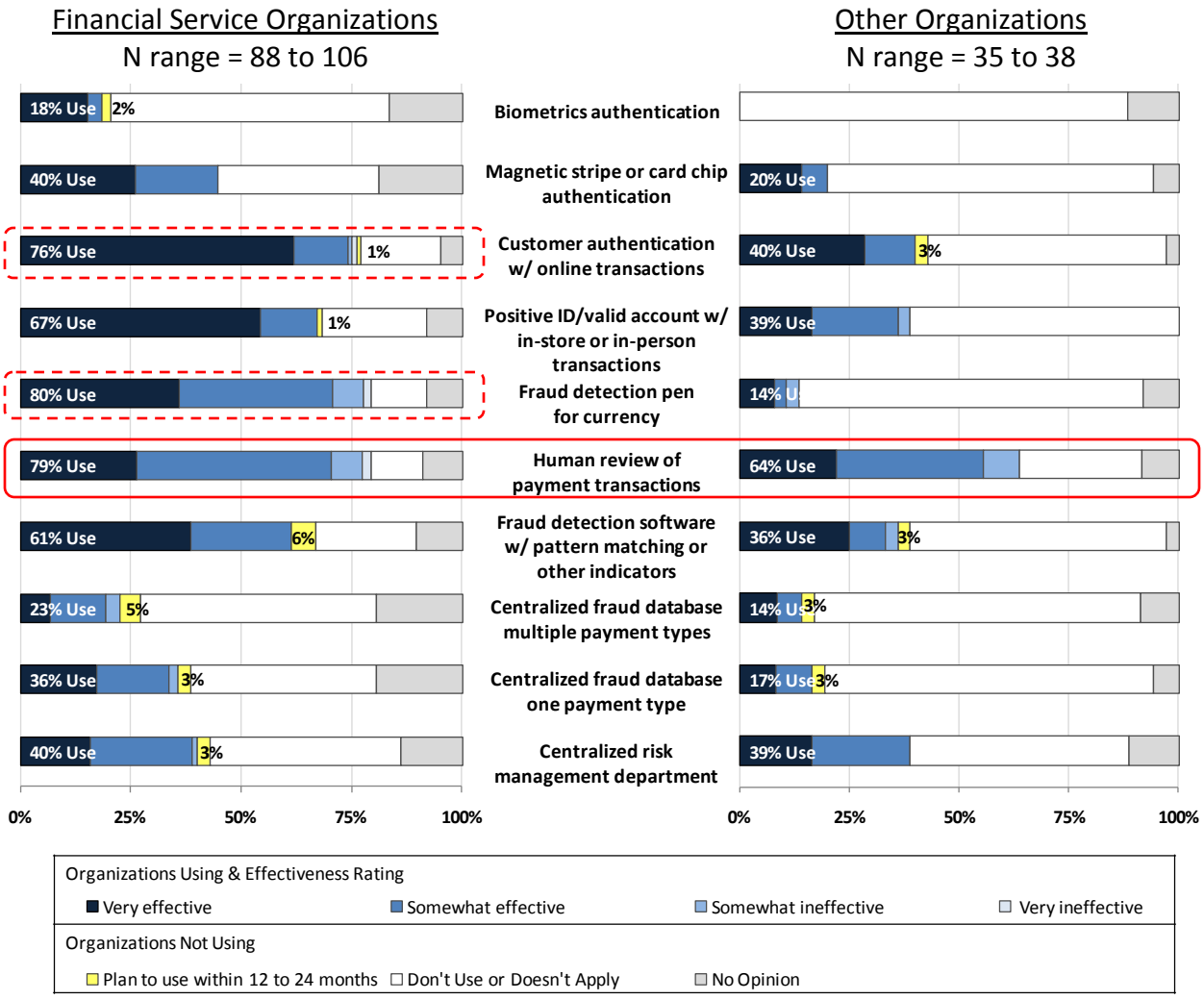


Chart I: Use and Effectiveness of Internal Controls and Procedures by % of Other Organizations (N=35 to 40)



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. Financial services used more of these methods than other organizations. Across the board, human review of payment transactions is most common, but is rated somewhat ineffective to very ineffective by 11% of financial services and 17% of all other organizations. This contrasts with the ratings of most other methods as effective by more than 90% of those that use it, as shown in Chart J.

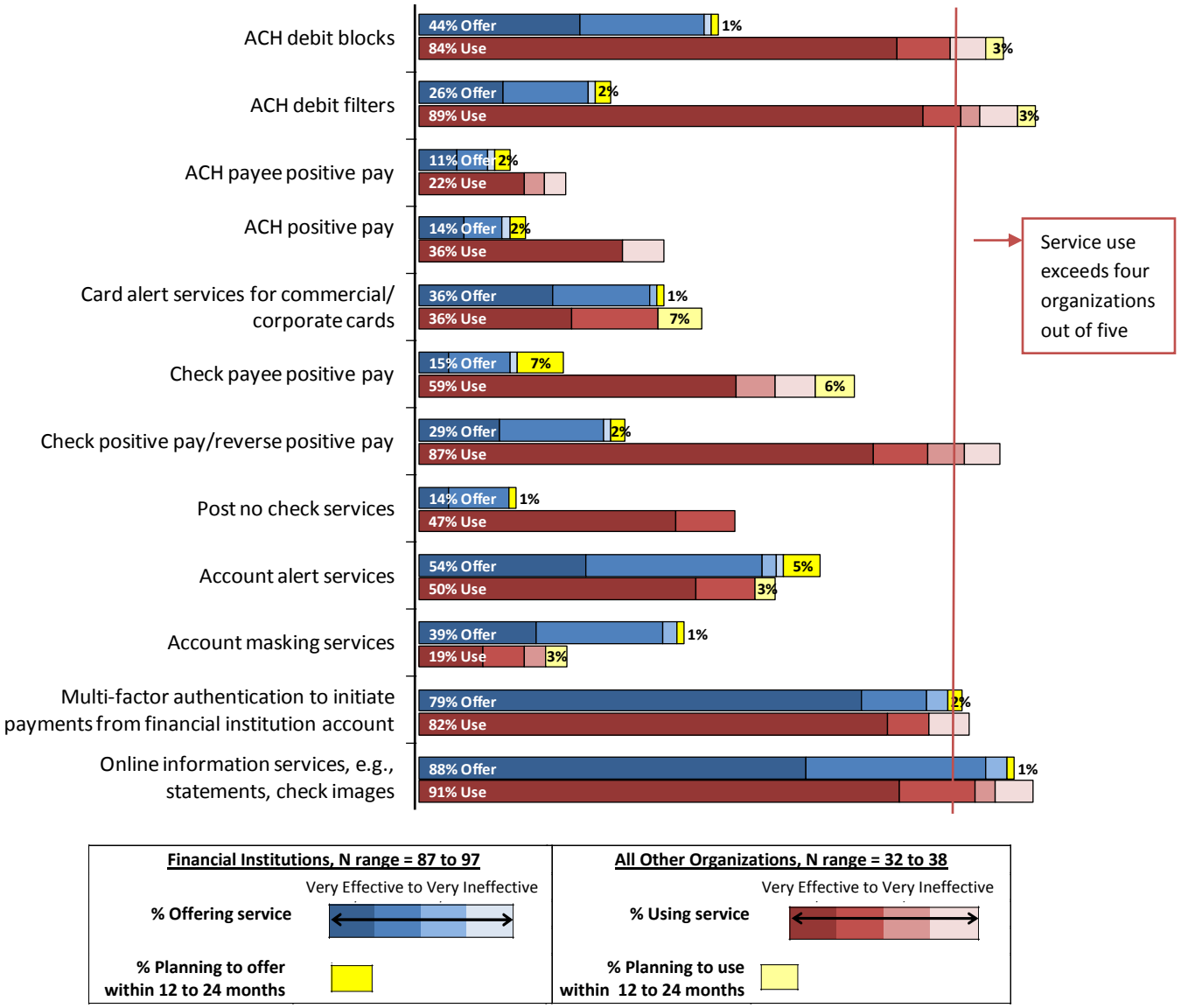
Chart J: Authentication, Transaction Screening and Risk Management by % of Respondents



iii. ***Risk Mitigation Services Offered by Financial Institutions.***[6] 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 75% of financial institution respondents, whereas the other three services are offered by many fewer FIs (e.g., ACH debit filters and blocks, and ACH positive pay and reverse positive pay). This level of availability may be insufficient to future demand, given the success that non-financial service respondents attribute to these services in reducing fraud losses from fraudulent ACH debits, reported in Chart K.

Chart K: Financial Institution Risk Mitigation Services Offered and Used by % of Respondents[7]



[6] FI respondents were asked what services their institution offers; all others were asked about services used.

[7] The number of financial institutions (FI) that offered some or all of the 12 mitigation services varies. Only one FI offered all 12 services, 11 FIs offered between eight and 11 services. Most FIs offering eight or more services offered all ACH and check positive pay and payee services. Some mitigation services were offered more by FIs with annual revenues over $50 million; others were offered more by smaller FIs.

f. Barriers to Reduce Payments Fraud

Respondents report the existence of various barriers to add and strengthen fraud mitigation controls at their organizations. Most identified implementation costs and/or the lack of resources as the main barriers. Non-financial service organizations also cited the lack of a compelling business case as an impediment to adopting new or changing existing fraud mitigation methods. A complete summary of responses is listed in Table 11.

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

	Financial Service Organizations N=91	Other Organizations N=29	All Respondents N=120
Consumer data privacy issues/concerns	37%	34%	37%
Cost of implementing in-house fraud detection tool/method	62%	48%	58%
Cost of implementing commercially available fraud detection tool/service	57%	52%	56%
Unable to combine payment information for review due to operating in multiple states	3%	10%	5%
Unable to combine payment information for review due to using multiple banks	2%	14%	5%
Corporate reluctance to share information due to competitive issues	5%	10%	7%
Lack of compelling business case (cost vs. benefit) to adopt new or change existing methods	36%	55%	41%
Lack of staff resources	56%	52%	55%
Other	2%	10%	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.*** Two-thirds of respondents said their organizations should share information about the prevalence of emerging fraud schemes to reduce payments fraud. The same percentage said applying new controls, like authentication, to Internet payments was needed. "Other" ideas mentioned were putting more responsibility on the organization accepting fraudulent debit cards, improving methods used to authenticate debit card users, stiffening penalties for fraud and increasing the number of available fraud prevention services used—e.g., positive pay services. Table 12 summarizes this information.

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

	Financial Service Organizations N=99	Other Organizations N=34	All Respondents N=133
Restrict access to customer DDA accounts	16%	29%	20%
Controls over Internet payments	68%	53%	64%
Information sharing on emerging fraud tactics being conducted by criminal rings	62%	85%	68%
Other	12%	12%	12%

ii. ***Industry Actions.*** In general, respondents supported industry-sponsored actions to reduce payments fraud, as evidenced by over 60% of them that supported all three ideas for industry action presented in the survey. These are listed in Table 13, along with the specific response rates.

Table 13: Industry Considerations by % of Respondents

	Financial Service Organizations N=94	Other Organizations N=33	All Respondents N=127
Industry-sponsored fraudster databases	63%	58%	61%
Industry alert services	65%	70%	66%
Industry-specific education on fraud prevention best practices	75%	76%	75%
Other	2%	6%	3%

iii. ***Legal or Regulatory Changes.*** Finally, respondents offered views on legal or regulatory changes that would help reduce payments fraud. All of these suggestions are listed in Table 14, but among them four main principles arise:

- Strengthen disincentives to committing fraud through stiffer penalties and more likely prosecution.
- Assign responsibility for mitigating fraud risk to the party best positioned to take action against fraud.
- Assign liability for fraud losses to the party most responsible for not acting to reduce the risk of payment fraud.[8]
- Establish new laws/regs or change existing ones in order to strengthen the management of payments fraud risk.

[8] The most common idea illustrating this principle was to align the responsibility to validate/authenticate the person using a debit card and the liability for associated losses with the entity accepting the card payment.

Table 14: Legal and Regulatory Considerations by % of Respondents

Legal and Regulatory Changes to Reduce Payments Fraud	N =39
1. Place responsibility to mitigate fraud and shift liability for fraudulent card payments to the entity that initially accepts the card payment • Align incentives to mitigate debit card fraud by allocating losses to the entity that first accepts the payment • Eliminate credit card zero-liability rules as they reduce incentives to ensure appropriate controls on processing these payments • Require entities accepting cards at the POS to check IDs and signatures • Use more than one method to authenticate in-person and cross-border/overseas initiated transactions • Require PINs on credit cards transactions • Institute fraud prevention programs with debit cards that are now used effectively with credit cards, e.g., Verified by Visa	**46%**
Place more responsibility on consumers and customers • Make customers responsible for timely management and review of their account information through online services and statements • Place more responsibility on consumers to protect sensitive information; increase their liability for losses due to fraud they cause through changes in Regulation E	**8%**
Focus future legal or regulatory changes on data breaches to where the breaches occur • Target legal and regulatory changes to where breaches occur without creating barriers for financial institutions to effectively conduct business • Prohibit recording of driver's license number on the face of checks	**5%**
Increase penalties for fraud and attempted fraud • Increase financial and criminal penalties for fraud and attempted fraud • Enforce responsibility and assess penalties on ODFIs that continue to process for third parties with a relatively high volume of fraudulent payments	**18%**
Improve law enforcement cooperation on domestic and international payments fraud and fraud rings • U.S. agencies and local law enforcement must be willing to pursue payments fraud • Enhance international cooperation in combating fraud rings and related activities	**8%**
Align Regulation E and Regulation CC to reflect changes in check collection systems' use of check images and conversion of checks to ACH • Rework regulations or combine under one set of rules • Identify industry solutions that are beneficial to banks and consumers to address return of fraudulent checks; the two-day hold for local items is inadequate resulting in charge-backs to consumer accounts for returned deposits • Prohibit corporations and check cashing entities from adding check cashing fees to checks converted to electronic payments; these payments fail positive pay systems	**8%**
Enable information sharing by location and industry • Relax data privacy restrictions to allow financial institutions to share information more easily • Establish a standard method to report fraud to banking organizations that also expedites review and follow-up	**8%**
Miscellaneous • Regulate the establishment of online businesses by requiring a license subject to a review of the business purpose and background checks • Enhance capabilities to monitor for duplicate files	**5%**