2012 Payments Fraud Survey Summary of Results First District

Federal Reserve Bank of Boston

Payment Strategies

November 2, 2012

http://www.bostonfed.org/bankinfo/payment-strategies

Contents

1. Introduction

In April 2012, the Federal Reserve Bank of Boston's Payment Strategies group conducted research on payments-related fraud experienced by financial institutions (FIs) in the Federal Reserve First District.[1] We asked our FI constituents to share their experiences with payments fraud and the methods they used to reduce fraud risk through an online survey. The survey covered transactions made using cash, check, debit and credit cards, the automated clearinghouse (ACH), and wire transfers.

This survey was part of a broader initiative conducted in conjunction with the Federal Reserve Banks of Dallas, Minneapolis, and Richmond, as well as the Independent Community Bankers of America (ICBA). While focused primarily on results from FIs in the First District, this report contains some comparisons of First District data to consolidated results that include survey data from all the participating Federal Reserve Banks and the ICBA. We plan to repeat this survey biannually, which will allow us to continue to analyze trend data on payments fraud in the district over multiple years.

2. Respondent Profile

Seventy financial institutions (FIs) in New England responded to the survey. The FIs self-identified as banks, credit unions, or thrifts (Chart A). FIs represented all six New England states (Connecticut – 20%, Maine – 6%, Massachusetts – 47%, New Hampshire – 20%, Rhode Island – 1%, and Vermont – 6%). Chart B shows the percentage of respondents in each asset-size range. The majority of FIs (83%) have assets under $1 billion. Of the 70 FIs surveyed, only 12 have assets that exceed $1 billion.

Chart A: Type of Financial Institutions (*n=70*)

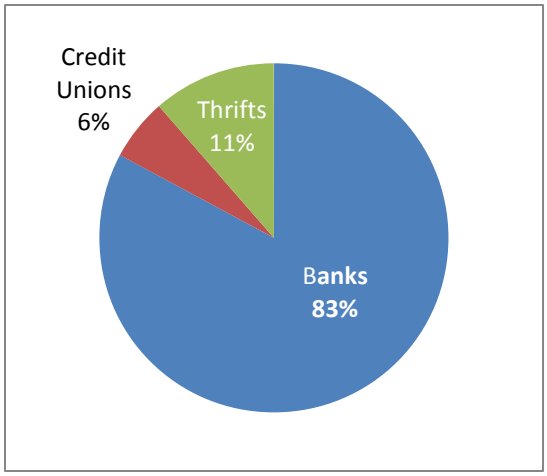
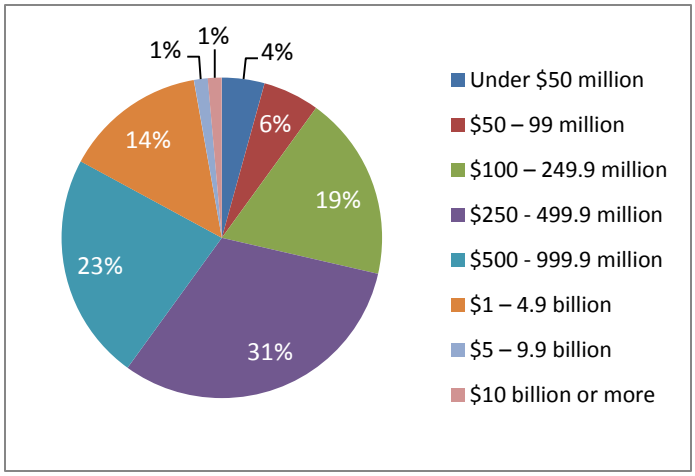


Chart B: Percentage of FIs by Asset Size (*n=70*)



[1] Questions regarding the survey summary may be directed to Marianne Crowe (marianne.crowe@bos.frb.org) at the Federal Reserve Bank of Boston.

Table 1 shows the actual number of financial institutions in New England by state, compared to the number and percentage of FIs that completed the survey for each state. Table 2 categorizes respondents by annual revenue, with over half (60%) of the respondents reporting annual revenues under $50 million.

Table 1: FIs by State

State	Total Number of FIs in New England[2]				FI Respondents (*n=70*)	
	Banks	Credit Unions	Thrifts	Total	Survey Respondents	% of total FIs
Connecticut	43	128	10	181	14	8%
Maine	22	63	7	92	4	4%
Massachusetts	139	209	19	367	33	9%
New Hampshire	17	21	6	44	14	32%
Rhode Island	10	23	4	37	1	3%
Vermont	13	27	1	41	4	10%
Total	244	471	47	762	70	9%

Table 2: FI Annual Revenue *(% of FI Respondents, n=70)*

Annual Revenue	Bank *n=58*	Credit Union *n=4*	Thrift *n=8*	All FIs *n=70*
Under $50 million	60%	25%	75%	60%
$50 – 99 million	6%	0%	13%	6%
$100 – 449.9 million	12%	25%	0%	11%
$500 – 999.9 million	12%	25%	12%	13%
$1 – 4.9 billion	3%	0%	0%	3%
$5 – 9.9 billion	0%	0%	0%	0%
$10 billion or more	1%	0%	0%	1%
Don't know	5%	25%	0%	5%
Not applicable	1%	0%	0%	1%
Total	100%	100%	100%	100%

[2] http://www.ibanknet.com, Data as of March 31, 2012

3. Summary of Survey Results

Payment Products Offered by FIs in New England

FI respondents were asked to indicate whether their customer base comprised primarily of consumers, commercial/business clients, or both. As indicated in Table 3, 93% of FIs offer services to both consumer and commercial customers.

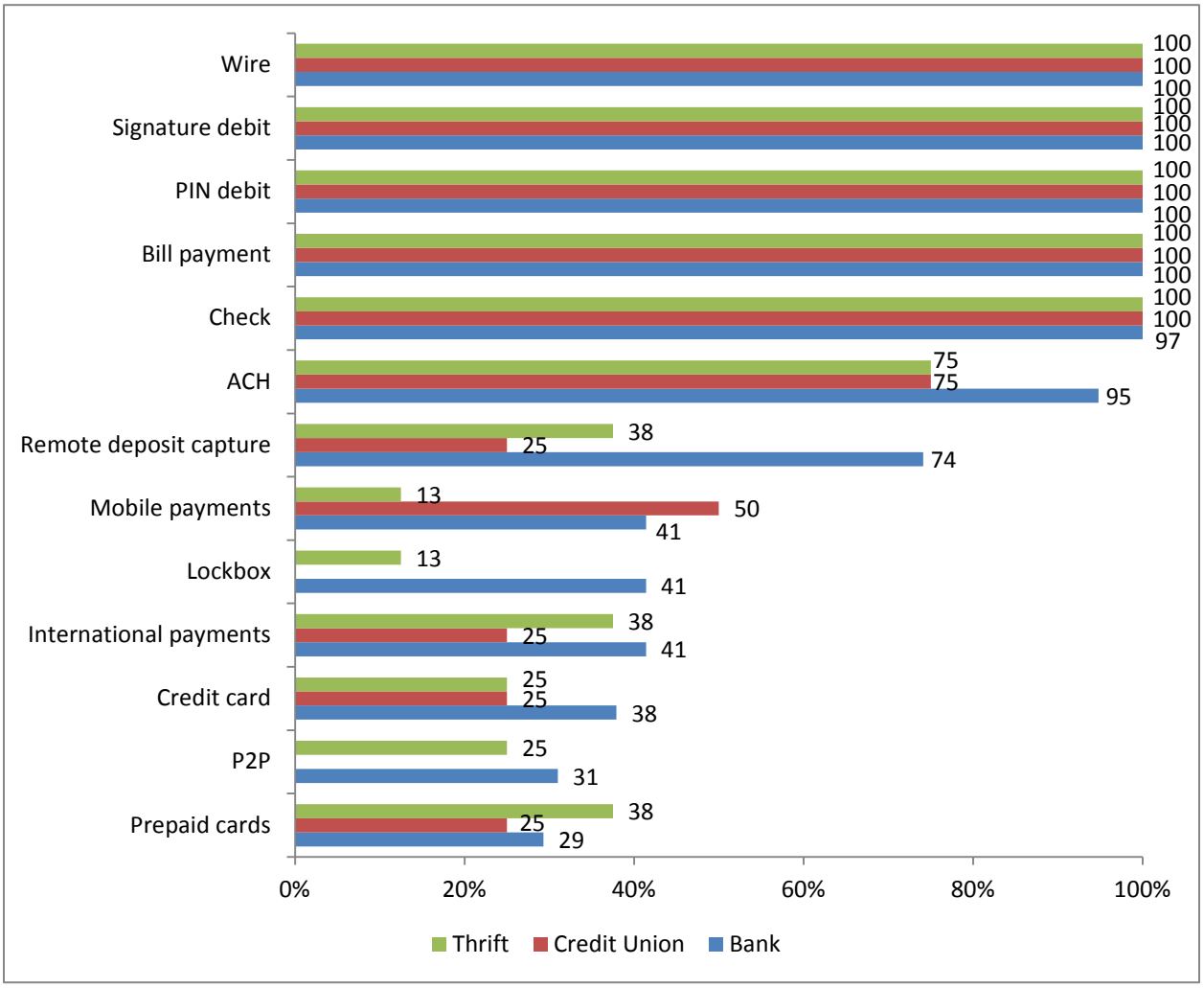
Table 3: Types of Customers to Which FIs Offer Payment Services

Target Customers	Bank *n=58*	Credit Union *n=4*	Thrift *n=8*	All FIs *n=70*
Primarily consumers	2%	50%	25%	7%
Primarily business/commercial customers	0%	0%	0%	0%
Both consumers and business/commercial customers	98%	50%	75%	93%

Chart C illustrates the types of payment products and services FIs offer. All FIs offer wire transfers, signature and PIN debit cards, and online bill payment services. All credit unions and thrifts, and almost all banks (97%) also offer check instruments.[3]

[2] Check instruments are defined as products that are payable on demand, such as checkable demand deposit accounts and share draft accounts or NOW accounts, which are offered by credit unions.

Chart C: Payment Products and Services FIs Offer (*% of FI Respondents, n=70*)



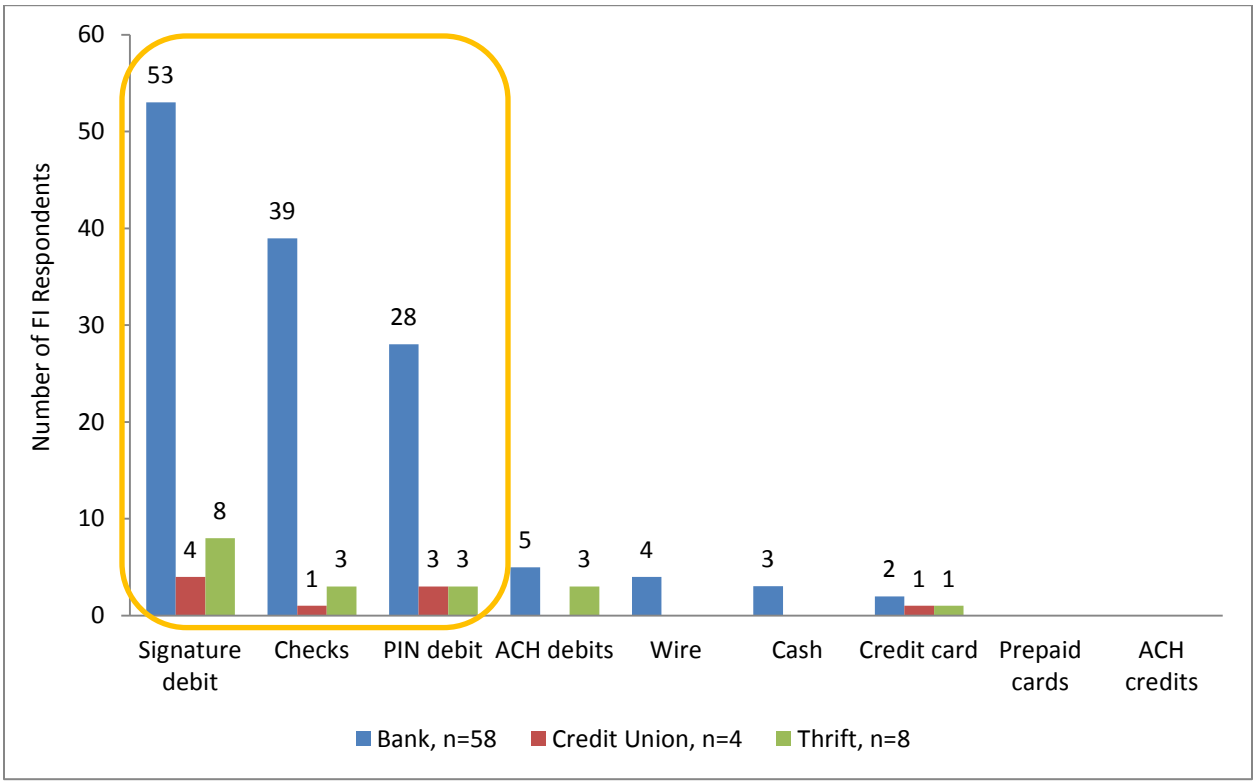
Payment Fraud Attempts and Financial Losses

All FIs reported fraud attempts on some payment methods. Respondents reported which payment types resulted in the highest number of fraud attempts in Chart D. Among the different payment types, signature debit cards had the most exposure to fraud, with 53 (92%) banks, and 4 (100%) credit unions and 8 (100%) thrifts reporting this type of fraud occurring in 2011. PIN debit card and check fraud attempts were the next highest categories: 28 (48%) banks, 3 (38%) thrifts, and 3 (75%) credit unions experienced PIN debit fraud. Among each FI category, a significantly higher percentage of banks (39 institutions or 67%) reported check fraud attempts compared to 3 thrifts (38%) and 1 credit union (25%).

Consistently, payment types with highest dollar losses due to fraud match those with the highest fraud attempts. (Charts D and E.) The percentage of FIs that reported the highest dollar losses due to PIN debit card and check fraud were 50% and 55% respectively. After examining the pattern of fraud attempts for FIs and their dollar amount losses, it appears that signature and PIN debit cards, and checks are currently the most vulnerable and costly services in terms of fraud for these respondents. However,

because only 36% of the respondents offer credit cards (vs. 100% that offer checks and debit cards), we do not know if credit card fraud attempts and losses would be higher with a bigger sample size.[4]

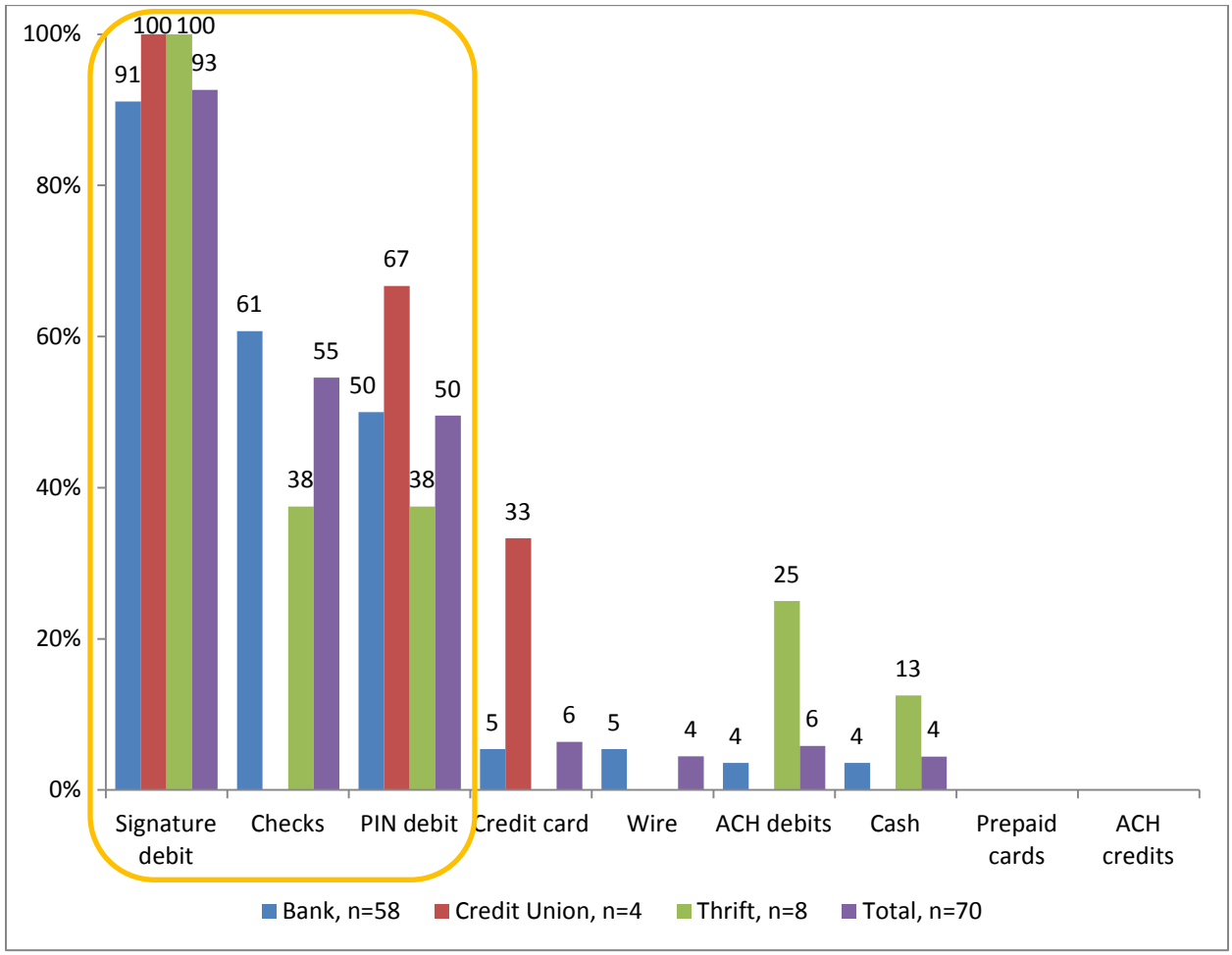
Chart D: Top 3 Payment Types with Highest Number of Fraud Attempts (*Number of FI Respondents*)



Note: Respondent rate was zero for prepaid card, ACH credit, and no fraud attempts experienced.

[4] Only two banks, two credit unions, and two thrifts reported fraud attempts for credit cards.

Chart E: Top 3 Payment Types with Highest Fraud Dollar Losses (*% of FI Respondents*)



Note: Respondent rate was zero for prepaid card, ACH credits and no fraud attempts experienced.

Mobile Payment Services

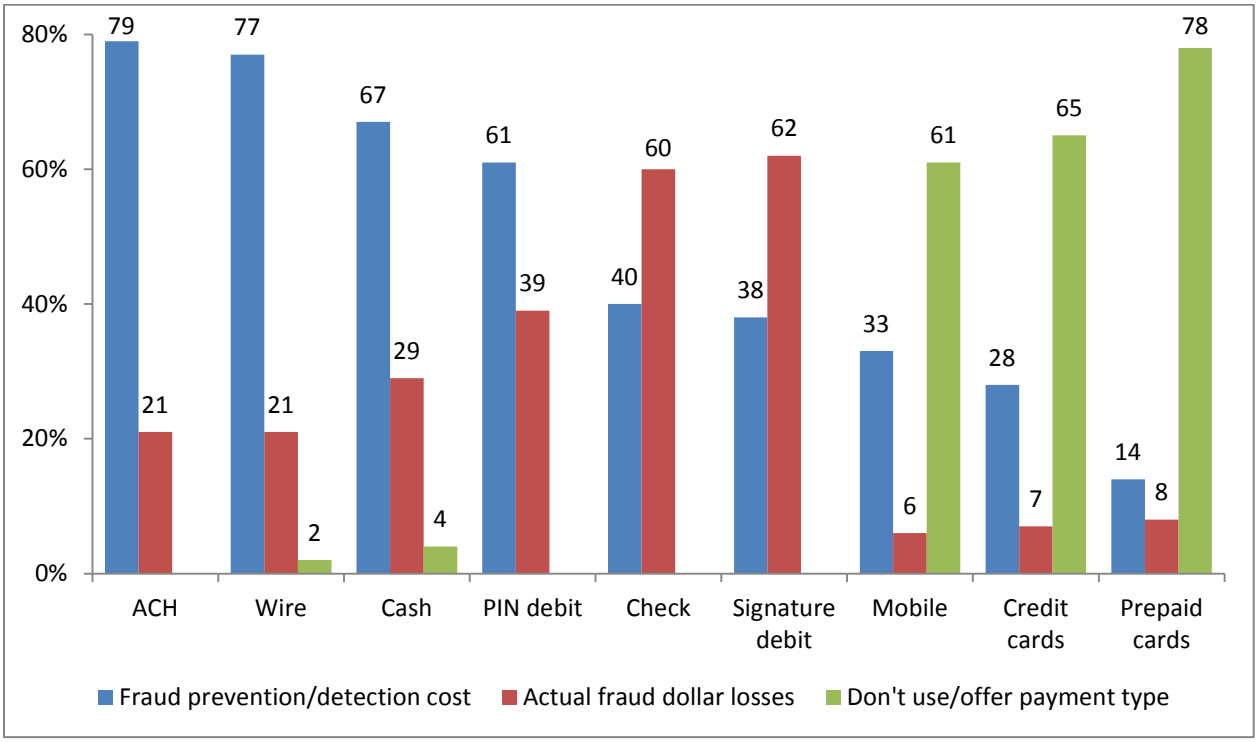
In addition to traditional payment products, FIs offer several mobile payment services, including mobile bill payment, P2P, and remote deposit.[5] The adoption rate for this new technology among First District FIs was relatively higher than the consolidated results. Thirty-nine percent of First District FIs offer mobile payments, 17% higher than the consolidated results. A noteworthy observation is that 74% of banks, 38% of thrifts, and 25% of credit unions offer remote deposit capture (RDC), which is a relatively new technology, although the survey question did not differentiate between taking a picture of a check using a mobile phone camera and using a scanner to capture the check image.

[5] We assume that remote deposit capture (RDC) includes using both mobile phone and PC scanner, since the question did not specify one method or the other.

Cost of Fraud Prevention vs. Actual Fraud Loss

For each type of payment service, FI respondents indicated whether the cost of fraud prevention or the actual fraud dollar losses was the greater expense for their organization, as shown in Chart F. For ACH, cash, wire, and PIN debit, over half of the FIs considered prevention and detection to be more costly than the actual fraud dollar losses. Conversely, signature debit and checks went the other way. Sixty-two percent of FIs suggested that actual fraud losses for signature debit exceeded the cost of prevention and detection. For checks, 60% of First District FIs suggested that actual fraud losses exceeded cost of prevention and detection, but only 51% of FIs in the consolidated results reported that the cost of actual fraud losses was higher. Even though fewer than 40% of the respondents offer the remaining services (credit card, prepaid card, and mobile payment), for all three the cost of fraud prevention and detection was reported as higher than the actual fraud dollar losses.

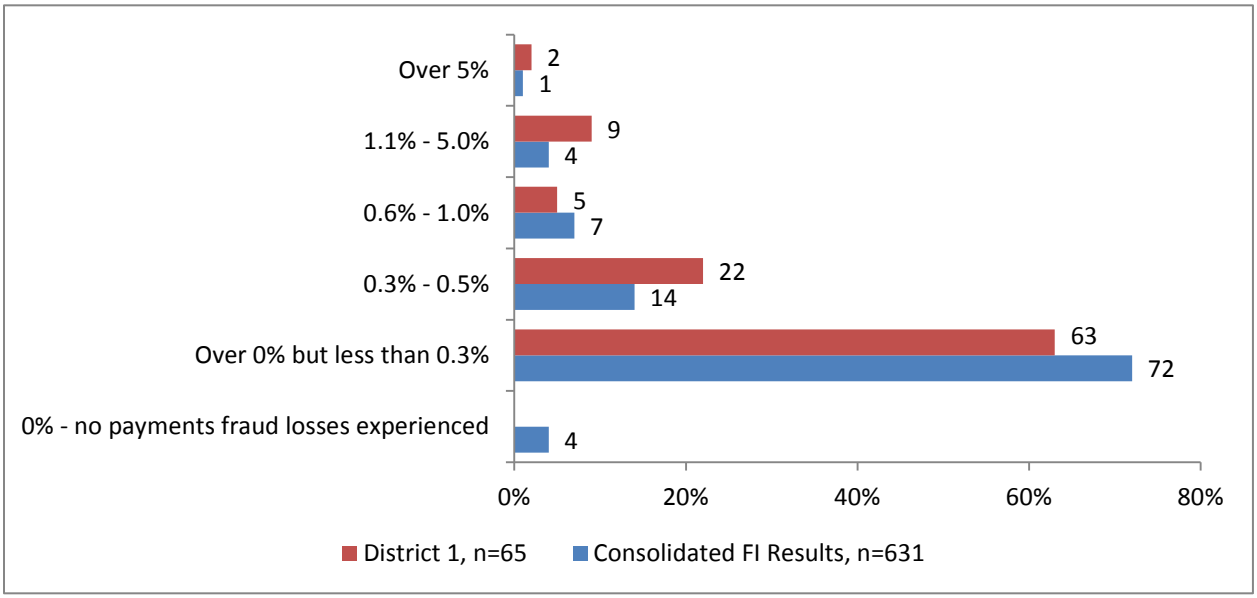
Chart F: Fraud Prevention Costs Compared to Actual Dollar Fraud Losses *(% of FI Respondents, n=70)*



Financial Losses due to Fraud

The magnitude of the total financial loss is measured by *loss as a percentage of total revenue* (Chart G). Based on the survey data, the magnitude of the First District's losses is greater than what is reported in the consolidated results. Four percent of FIs in the combined results reported no payment fraud dollar losses, compared to zero percent in the First District. Sixty-three percent of First District respondents reported very low losses (less than 0.3%); but still below the 72% combined average for that range.

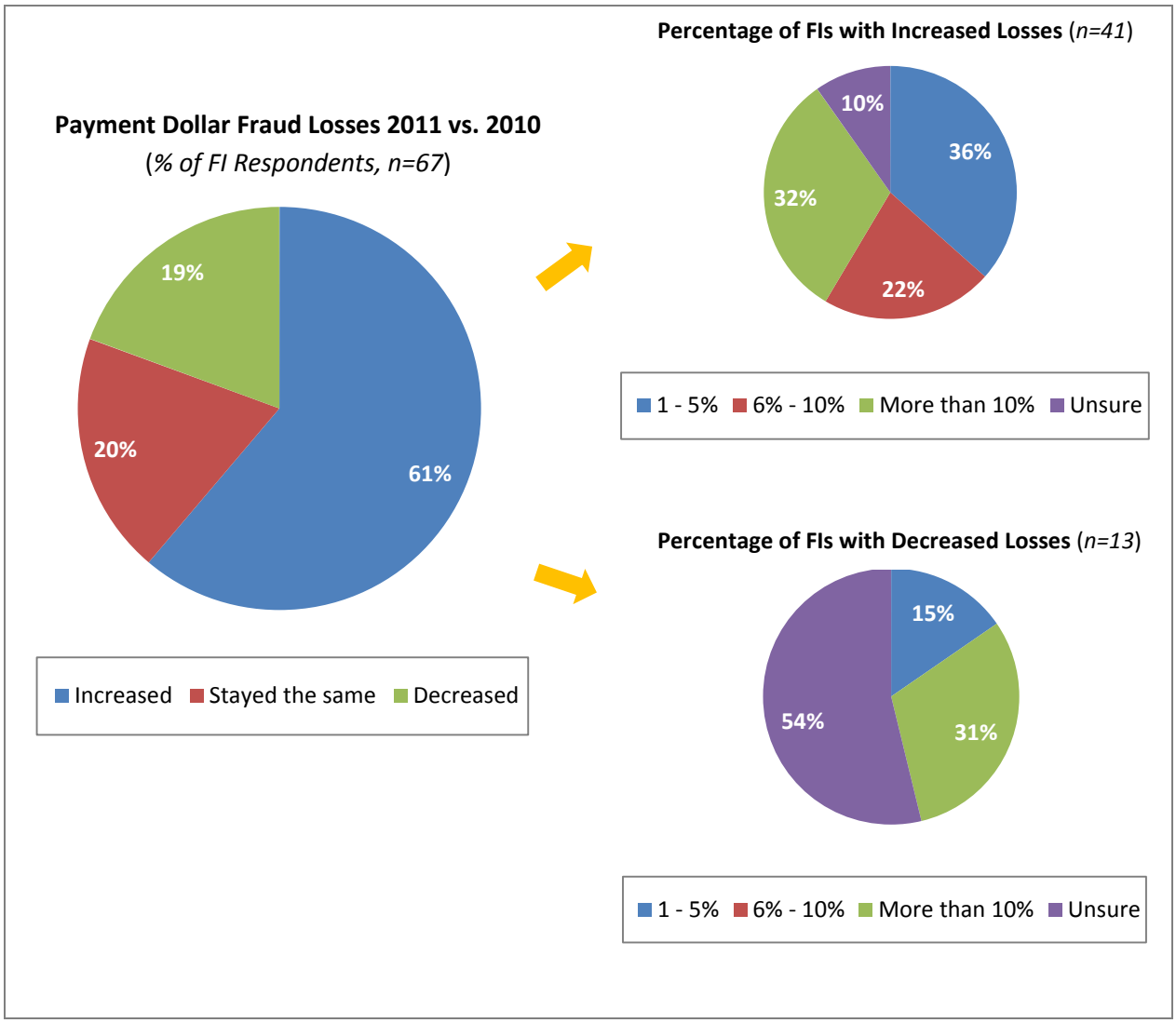
Chart G: Payments Fraud Loss Rate – First District vs. Consolidated Results (*% of FI Respondents*)



Note: Totals do not add up to 100% due to rounding.

Sixty-one percent of First District FIs reported increases in actual dollar fraud losses from the previous year, while only 19% reported decreased losses (Chart H). The increasing trend in the First District is greater than the 51% increase reported in the consolidated results. Among First District FIs reporting increased losses, 32% reported an increase over 10% higher than the previous year. Conversely, 31% of the FIs that reported lower losses claimed that losses decreased over 10%.

Chart H: Payment Fraud Losses in 2011 vs. 2010



Twenty percent of the 41 First District FIs reporting increased fraud losses in 2011 have assets over $1B. What is interesting is that these larger FIs experienced a slightly higher degree of fraud losses. It is possible that larger banks, with more customers and volume, are more attractive to fraudsters, but there is nothing in the data to explain this anomaly. Table 4 shows that 73% (8 of 11) of FIs with assets over $1B reported increases in fraud losses, while only 59% (33 of 56) of FIs with assets under $1B reported increased fraud losses in 2011.

Chart I: Trends in Losses by FI Asset Size

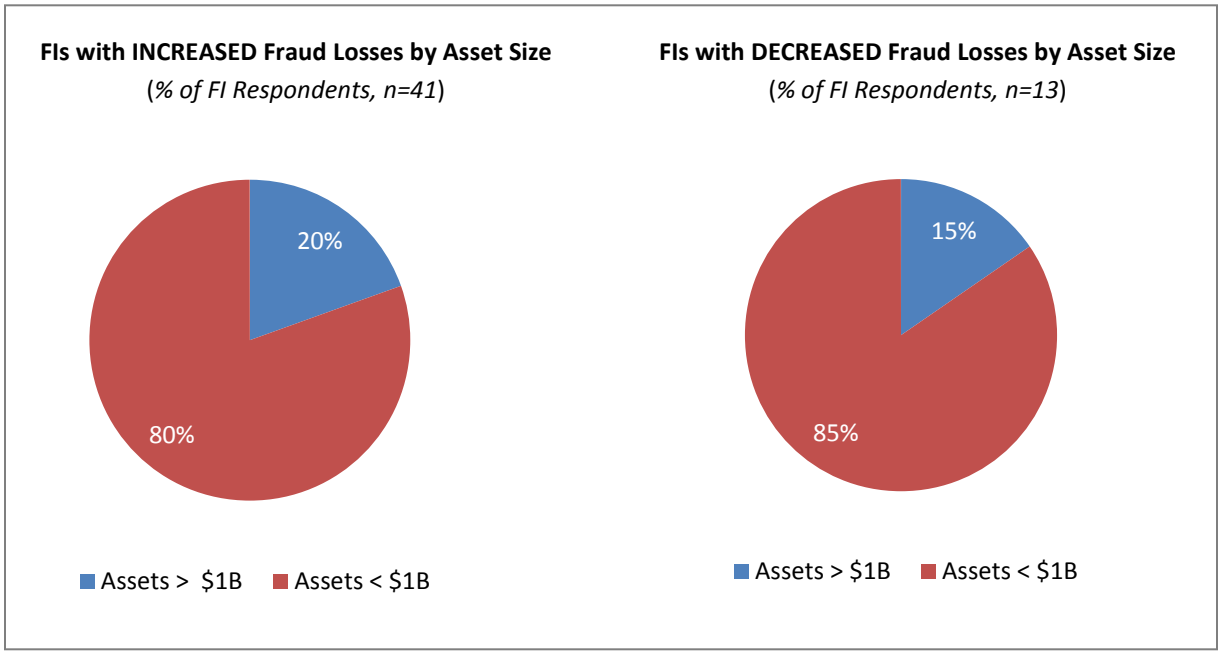
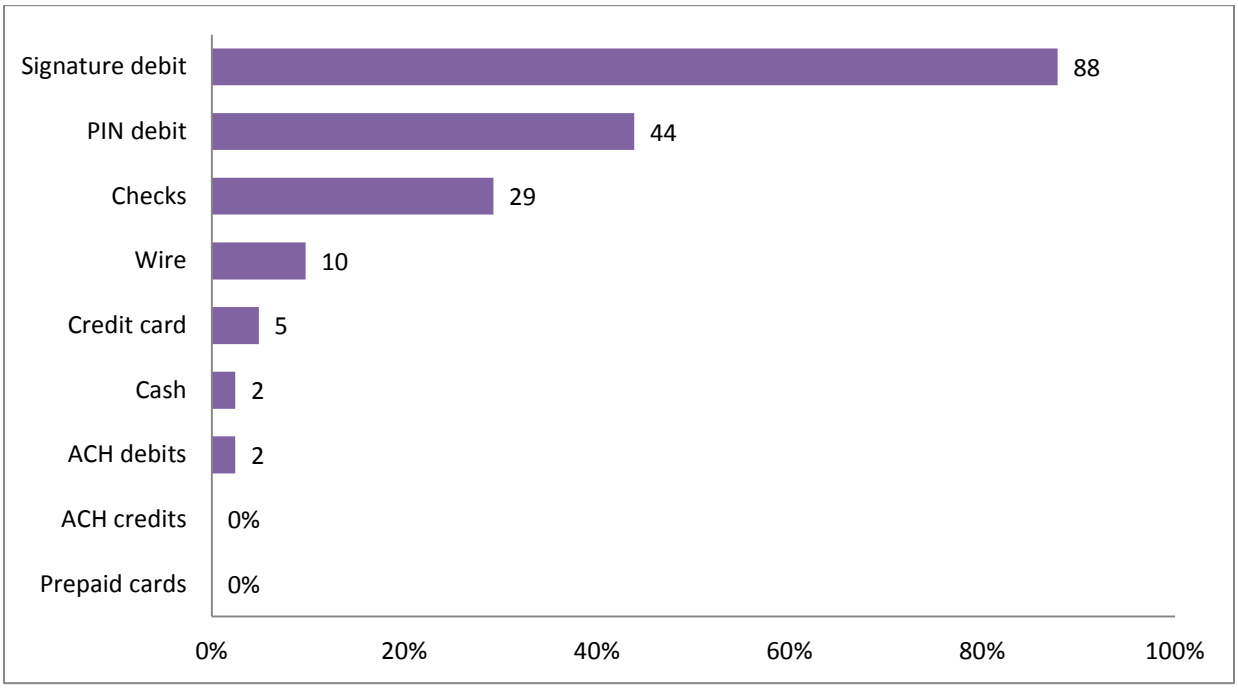


Table 4: FI Fraud Losses by Asset Size (*% and number of FI Respondents*)

Fraud Losses	FIs with Asset > $1 B (n=11)		FIs with Asset < $1 B (n=56)	
	#	Percent	#	Percent
Increased	8	73%	33	59%
Decreased	2	18%	11	20%
Stay the same	1	9%	12	21%
Losses Over 0.3% of Revenue	4	36%	24	43%
Losses Over 5% of Revenue	1	9%	0	0%

The primary payment services that contributed to increased fraud losses are signature or PIN debit cards and checks. Therefore, FIs should continue to focus their fraud prevention efforts on these three payment methods (Chart J).

Chart J: Payment Instruments Attributed to Increase in Fraud Losses *(% of FI Respondents, n=41)*

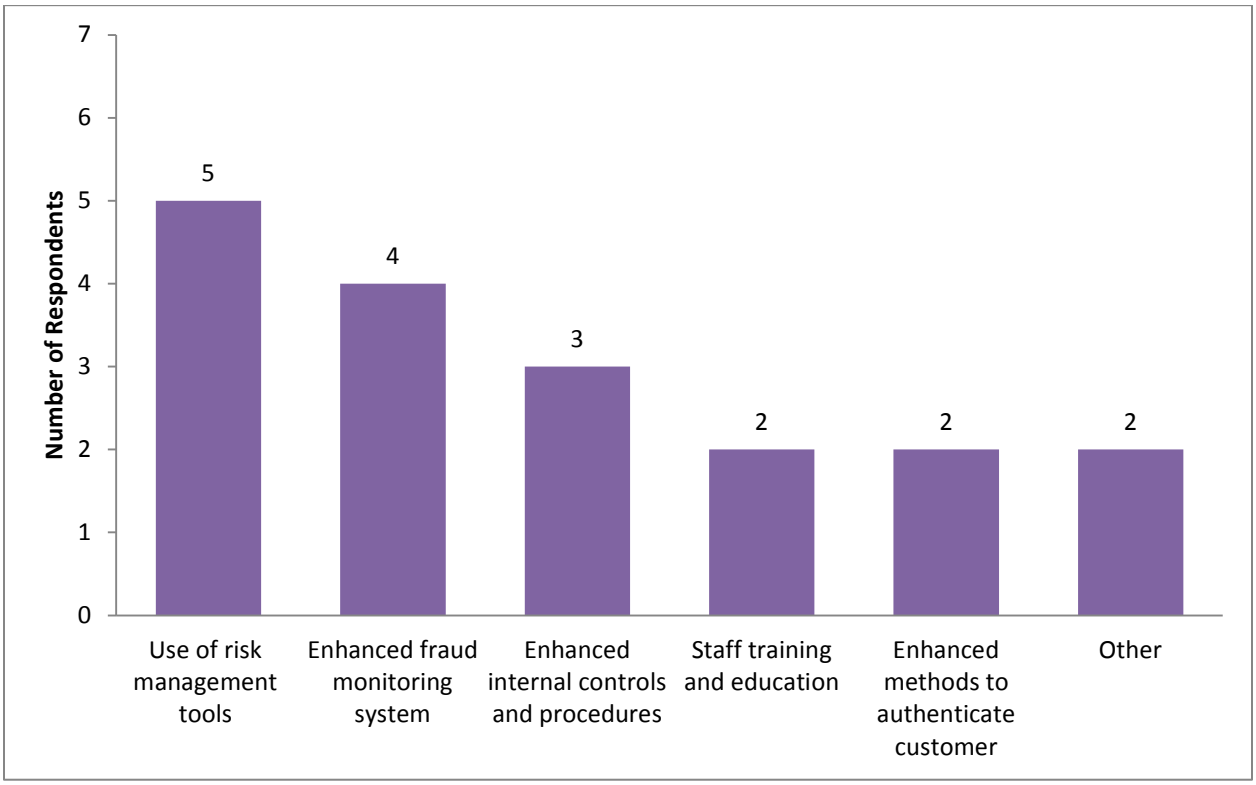


Because the check has a much longer history as a payment instrument, related fraud prevention tools and procedures are more developed and successfully applied. Better fraud prevention tools are still needed to address debit card fraud, particularly signature debit card fraud. For example, implementing EMV/dynamic data authentication (chip+PIN or chip+signature) in the United States could help to reduce fraud at the physical POS as evidenced by results in other countries. However, EMV will not mitigate online payment fraud using debit or credit cards because there is no physical connection between the card and a physical payment terminal or reader.[6]

While only 13 respondents reported decreased fraud losses, it is worth noting that seven implemented various fraud reduction methods. The top two methods adopted were risk management tools and enhanced fraud monitoring systems. The FIs also indicated that these procedures and technologies were implemented typically for card transactions for which fraud is most pervasive (Chart K).

[6] In the second half of 2011, Visa, MasterCard, Discover, and AMEX announced plans to accelerate the EMV smart chip acceptance in the U.S. According to Visa, they will institute a U.S. liability shift for domestic and cross-border counterfeit card-present point-of-sale (POS) transactions, effective October 1, 2015. Fuel-selling merchants will have an additional two years, until October 1, 2017 before a liability shift takes effect for transactions generated from automated fuel dispensers. Currently, POS counterfeit fraud is largely absorbed by card issuers. With the liability shift, if a contact chip card is presented to a merchant that has not adopted, at minimum, contact chip terminals, liability for counterfeit fraud may shift to the merchant's acquirer.

Chart K: Key Changes that Contributed to Decrease in Fraud Losses (*Number of respondents, n=7*)



Most Common Fraud Schemes

Both First District and consolidated survey results indicated that most fraud is initiated externally rather than internally. In the First District, 75% of respondents reported that all of their fraud was conducted by external parties via various schemes (Table 5). Overall, 84% of the FIs attributed their fraud to a single source, e.g. external only, while 16%of the FIs reported mixed sources of successful fraud.

Table 5: Successful Payment by Perpetrators Involved *(% of Respondents, n=64)*

Perpetrators	Mixed Types of Perpetrators	
Internal Only	**16%** of respondents attributed a portion of successful fraud to more than one perpetrator category.	3.1%
Internal w/External		1.6%
External Only		75.0%
Could Not Determine		4.7%

84% of respondents attributed 100% of successful fraud to a single perpetrator category.

The top two fraud schemes against customers' accounts were related to card transactions, as reported in Chart L. Eighty-six percent of FIs' customers experienced fraud from counterfeit or stolen cards used at point-of sale (POS), and 85% experienced fraud due to online use of counterfeit or stolen cards. For bank- or thrift-owned accounts (Chart M), the most common fraud schemes were check-related. Counterfeit, altered or forged checks were the top fraudulent activities experienced by 58% and 42% of respondents, respectively.

Chart L: Top 3 Current Fraud Schemes Involving Payments by or on Behalf of FI Customers
(*% of FI Respondents, n=65*)

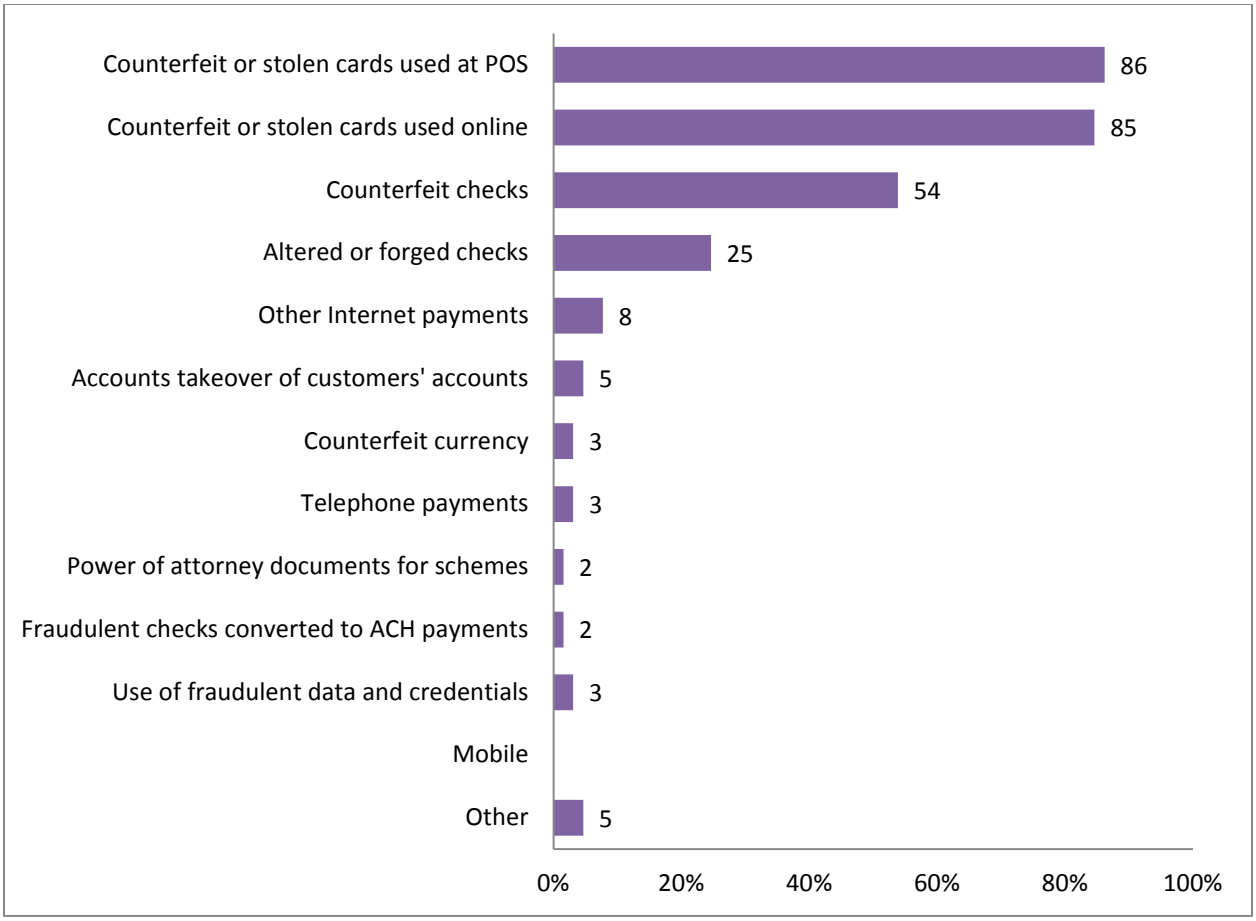
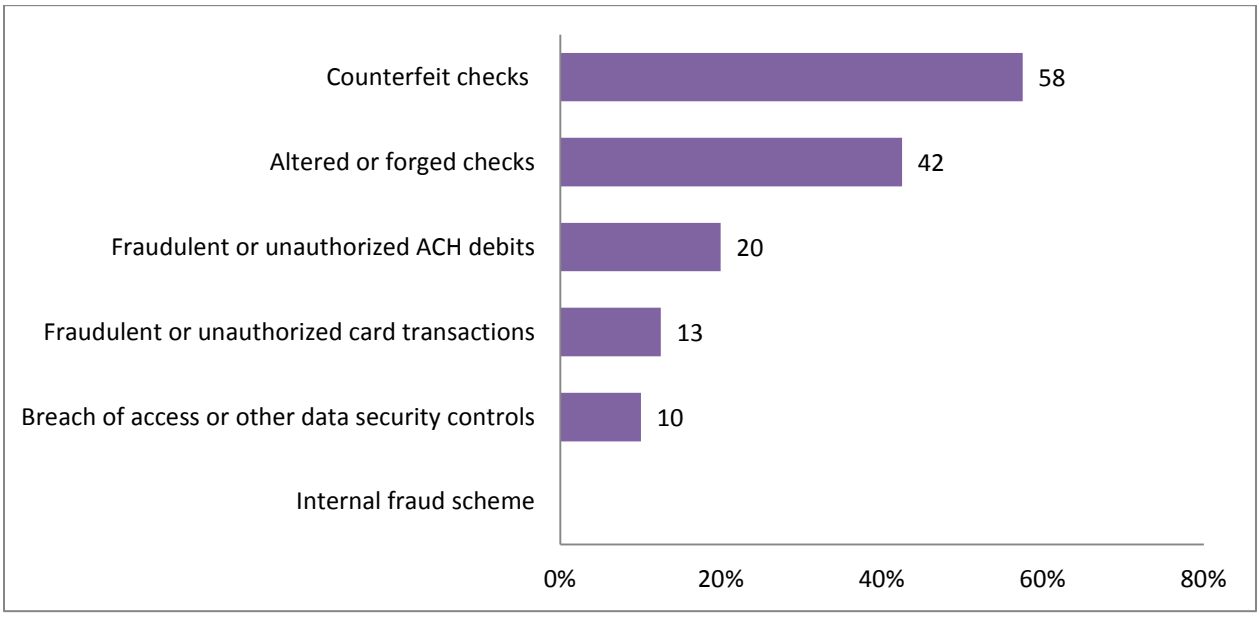


Chart M: Top 3 Fraud Schemes Involving FI's Own Accounts (*% of FI Respondents, n=40*)



Note: Thirteen FIs reported "Not applicable" and are not included in Chart M.

Fraudsters obtained most of the information used to initiate fraud schemes directly from consumers, which makes controlling the fraud more difficult (Table 6). Consumer awareness of how to avoid payment fraud needs to be addressed through education. Sixty-four percent of FIs indicated that "sensitive information obtained from a lost or stolen card, check, or other physical document or device while in the consumer's control," was the top source used in fraud attempts. However, other sources of information fraudsters used to initiate fraud included "physical device tampering," "email and webpage cyber-attacks," and "data breach due to computer hacking," all of which can be mitigated by implementing stronger controls and increasing investment in fraud prevention and detection tools, such as fraud monitoring systems.

Table 6: Information Sources Used in Fraud Schemes (*% of FI Respondents, n=63*)

Information Sources	All FIs *n=63*
"Sensitive" information obtained from lost or stolen card, check, or other physical document or device while in consumer's control	64%
Data breach due to computer hacking, e.g., use of default or guessable credentials, brute force attacks, access through open ports or services, etc.	43%
Physical device tampering, e.g., use of skimmer on POS terminal or ATM to obtain card magnetic stripe information	43%
Email and webpage cyber-attacks, e.g., phishing, spoofing, and pharming used to obtain "sensitive" customer information	37%
Information about customer obtained by family or friend	24%
Organization's information obtained from a legitimate check issued by your organization	16%
Other [7]	10%
Employee with legitimate access to organization or customer information	0%

Payment Fraud Mitigation Strategies

Respondents were asked about their use and the effectiveness of various types of fraud mitigation methods and tools in four areas: internal controls and procedures; customer authentication methods; transaction screening and risk management methods; and risk mitigation services offered by FIs. Fraud can be prevented at different stages of a transaction. Prior to or while a transaction is conducted, effective authentication methods can be implemented to verify the identity of the user to prevent fraud. When an FI is processing a payment transaction, it can apply transaction screening and risk management tools to detect suspicious transactions or patterns. Furthermore, as a long-term fraud prevention strategy, organizations should always enhance internal controls and procedures to avoid damage from internal fraud and material weakness. This survey not only provides means to examine the degrees of implementation for three fraud mitigation strategies, but also measures the efficiency level of each strategy.

Authentication Methods

The implementation of appropriate authentication methodologies should start with an assessment of the risk posed by the FI's online banking systems. The risk should be evaluated in light of the type of customer (e.g., retail or commercial); the customer transactional capabilities (e.g., bill payment, wire transfer, loan origination); the sensitivity of customer information being communicated to both the

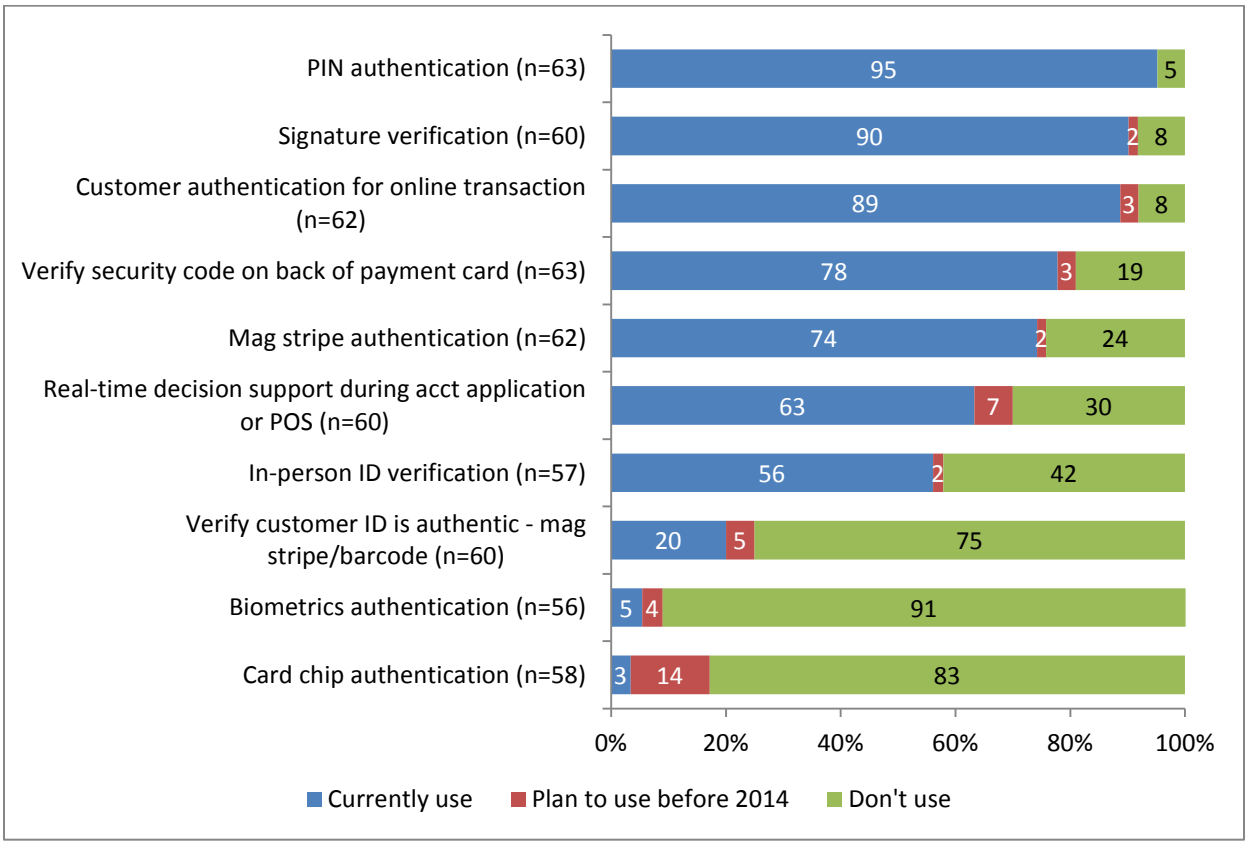
[7] Other fraud information sources include counterfeit debit cards manufactured using card numbers obtained from hacking of a merchant that is not a bank customer or hacking a payment processor; card compromised at payment processor or debit card third-party processor; scraping of public records; counterfeit checks.

institution and the customer; the ease of using the communication method; and the volume of transactions. This guidance as described by the FFIEC is considered a risk-based and "layered" approach to information security.[8]

The top authentication methods used by survey respondents are PIN authentication, signature verification, and customer authentication for online transactions. However, not all of the methods are considered to be equally effective by the FIs. Ninety-eight percent of First District respondents reported that PIN authentication is very or somewhat effective and 96% reported authentication for online transactions is very or somewhat effective. In contrast, more FIs (11%) indicated that signature verification was somewhat ineffective (Charts N and O).

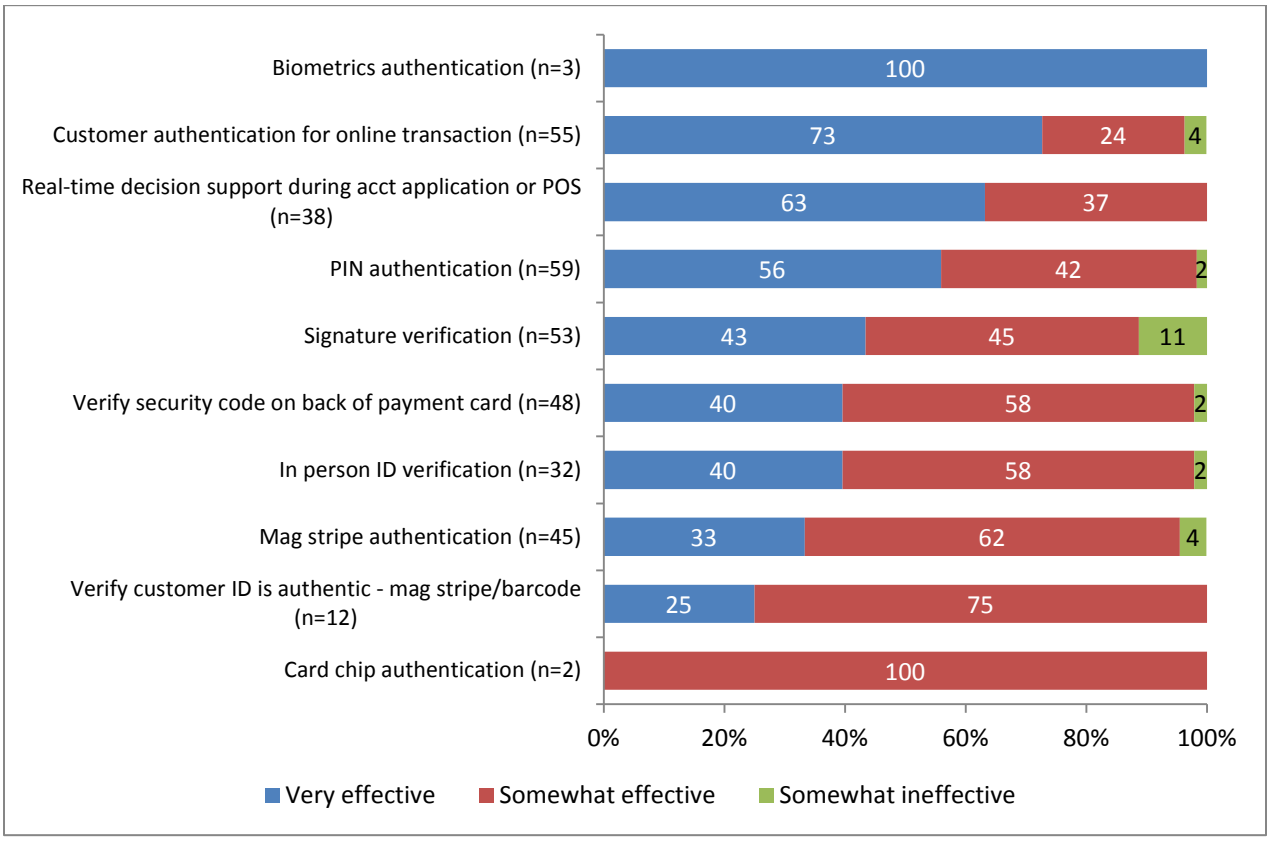
The three least implemented authentication methods reported were mag stripe/2D barcode for state ID (12 users), biometrics (3 users) and card chip authentication (2 users). However, 14% of the respondents plan to implement card chip authentication by 2014, which may be related to the EMV migration. Looking at both the First District and consolidated data results, the newer authentication technologies may be more effective, but are being used by a very small number of institutions.

Chart N: Use of Authentication Methods (*% of FI Respondents*)



[8] http://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formated).pdf

Chart O: Effectiveness of Authentication Methods (*% of FI Respondents*)



Transaction Screening and Risk Management Methods

Charts P and Q summarize the main transaction screening and risk management methods that FIs have implemented or plan to implement for various payment methods. Staff education is the most implemented method (97%), followed by use of a fraud detection pen for currency (87%). Customer education, accessing fraudster databases, receiving alerts, fraud detection/analysis software, and human review of transactions have similar adoption rates, range from 76% to 79%. Compared to the authentication methods, transaction screening methods show higher use; while risk management methods show lower use. Almost all of the methods are considered either very effective or somewhat effective. Only 26% of FIs rated customer education on payment fraud risk very effective, which may indicate that fraud tools are better suited to this fraud mitigation strategy.

Chart P: Use of Transaction Screening and Risk Management (*% of FI Respondents*)

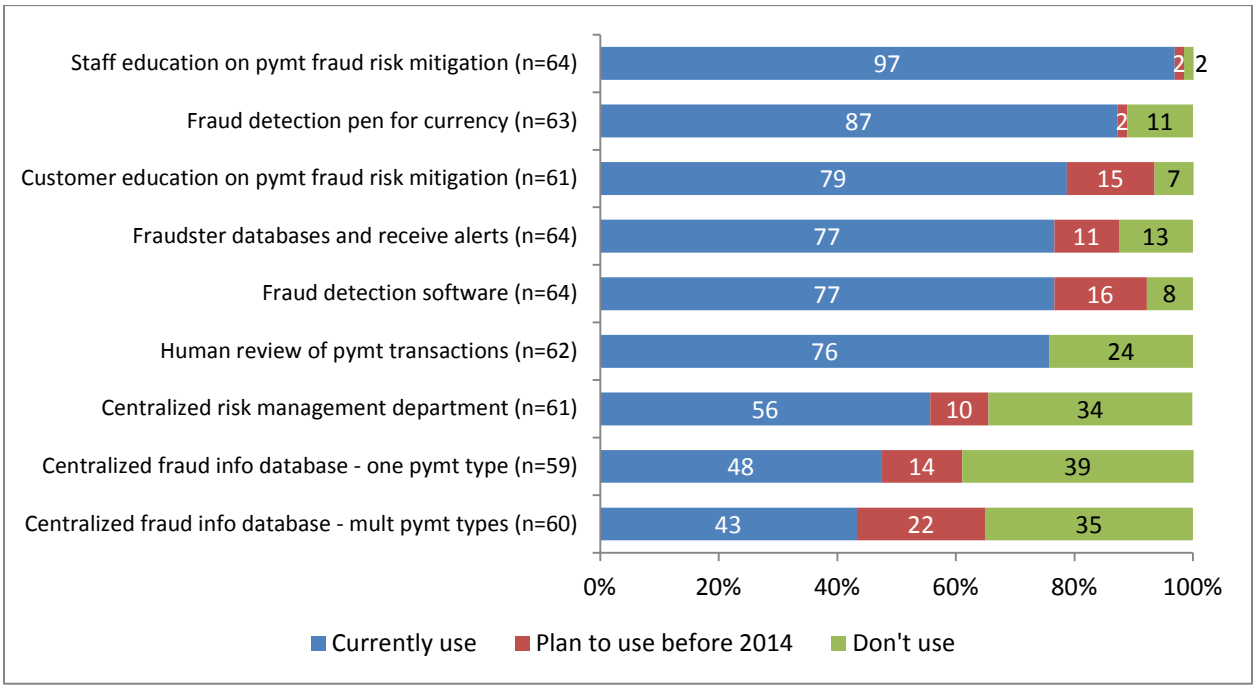
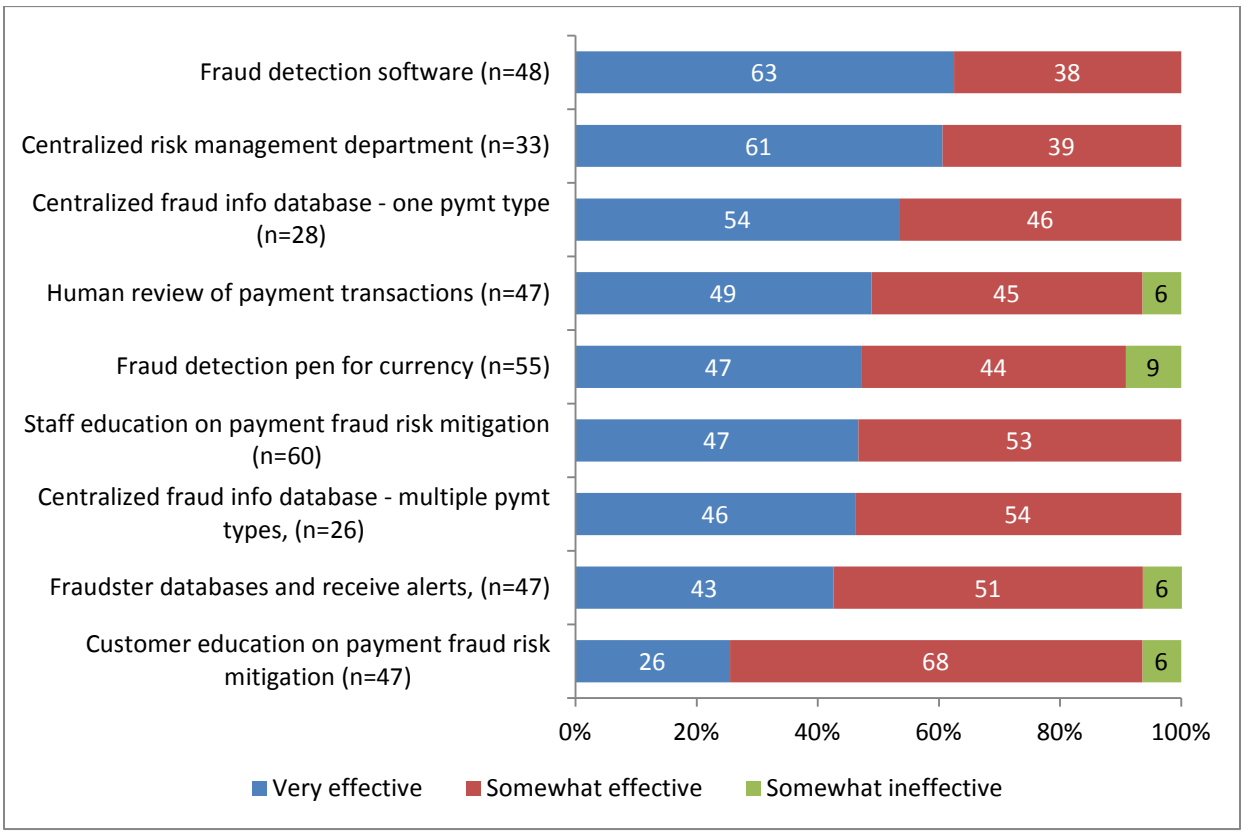


Chart Q: Effectiveness of Transaction Screening and Risk Management (*% of FI Respondents*)



Internal Control and Procedures

The "fraud triangle" comprises three factors: incentive, rationalization, and opportunity. Among them, opportunity for fraud is usually caused by lack of control. Therefore, strong and effective internal controls and procedures are essential for effective fraud prevention, especially to mitigate internal fraud. Compared to authentication and transaction screening and risk management methods, internal control procedures have a much higher overall adoption rate (Charts R and S). Some of the procedures are required by regulation or corporate policies. Of the possible internal control methods, employee hotlines for fraud reporting and dedicated computers to conduct transactions had the lowest adoption rates (approximately 40% of the FIs do not implement these methods). Because hotlines require additional staff and dedicated computers require investment in new hardware and software, budget constraints or resource issues could be a barrier.

Chart R: Use of Internal Control Methods (*% of FI Respondents*)

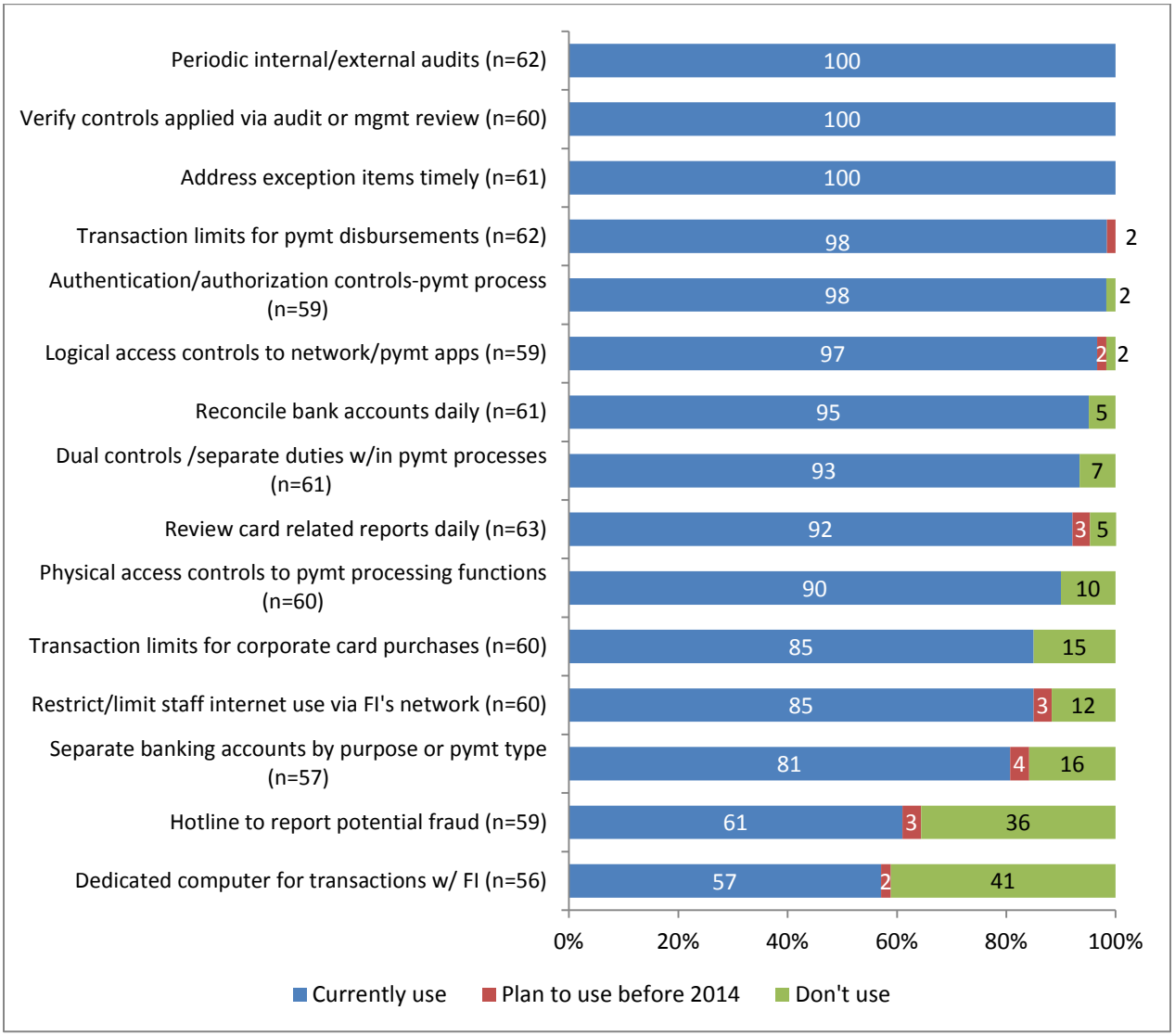


Chart S: Effectiveness of Internal Control Methods (*% of FI Respondents*)

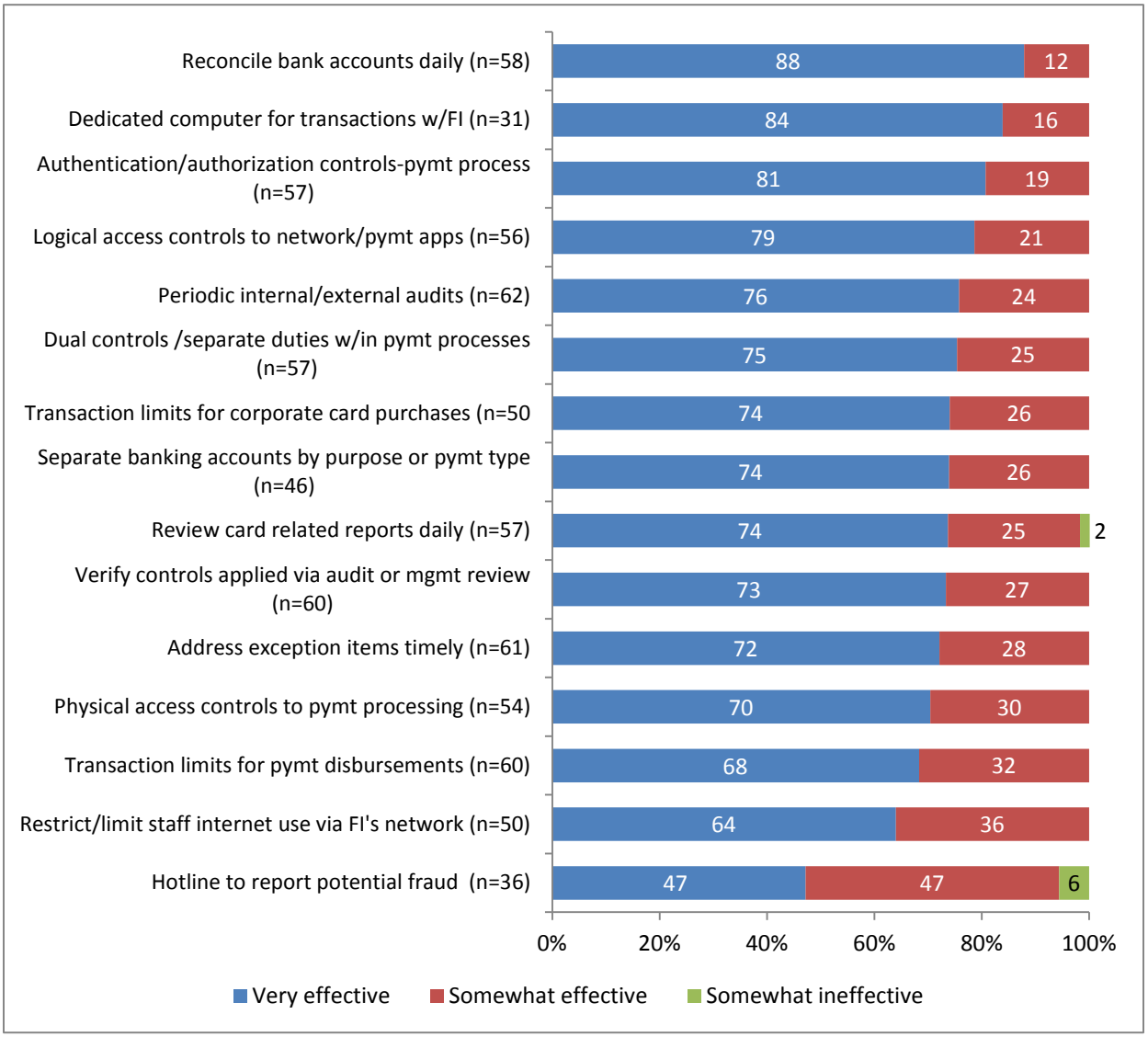


Chart T lists the risk mitigation services that FIs provide to their business customers. The most commonly provided tools are online information services and multi-factor authentication (MFA). Online information services help customers detect fraud by providing them with timely tools to check account information and balances, and view check images. MFA can be achieved through different channels, for example, a smartphone can be used as another layer of authentication. However, survey results indicated a relatively low level of willingness among FIs to adopt mobile devices for authentication, compared to other methods (Chart U). This may be an area where further education could incent FIs to consider using mobile phones to assist with security.

Chart T: Risk Mitigation Services Offered by FIs (*% of FI Respondents*)

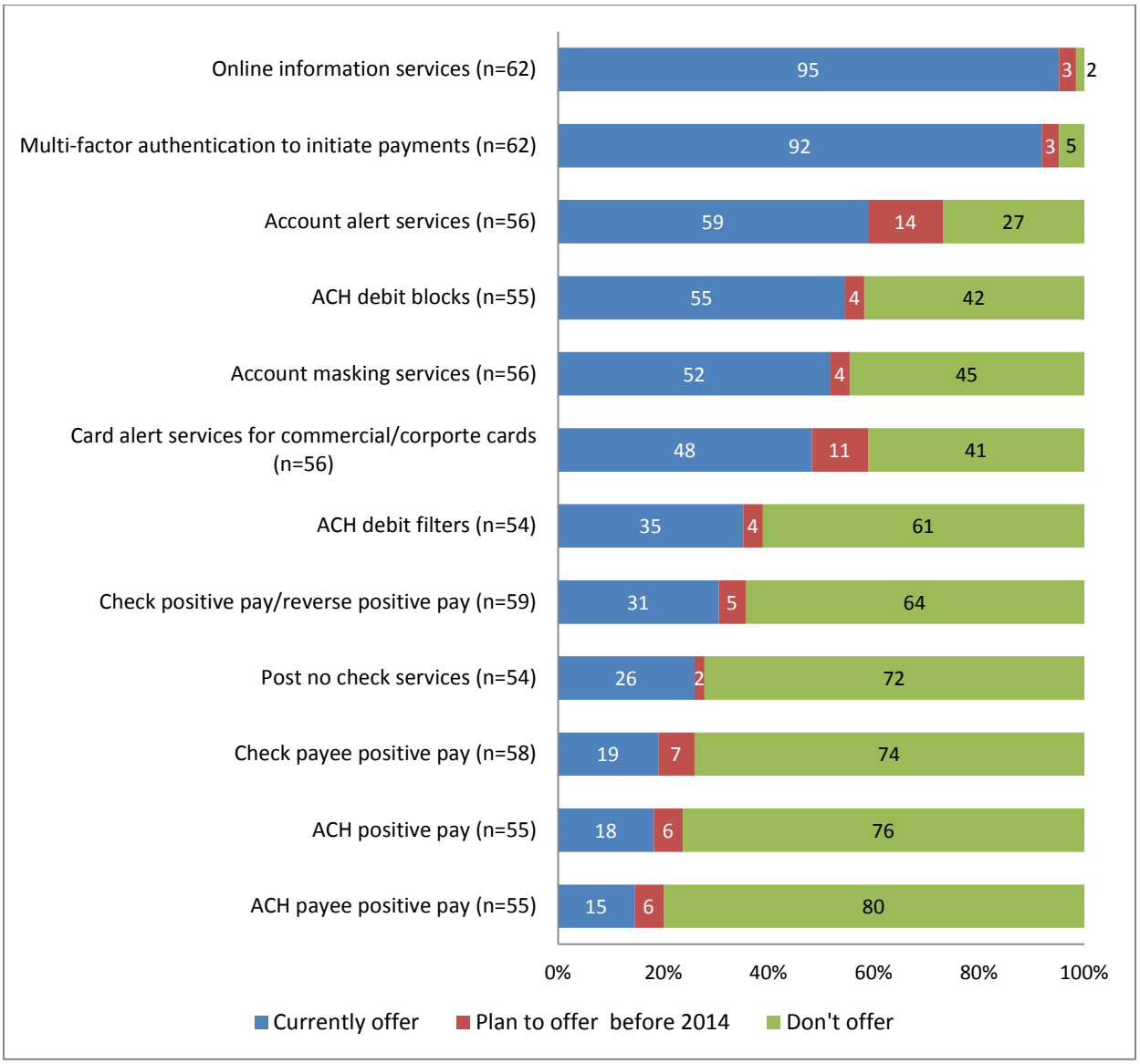
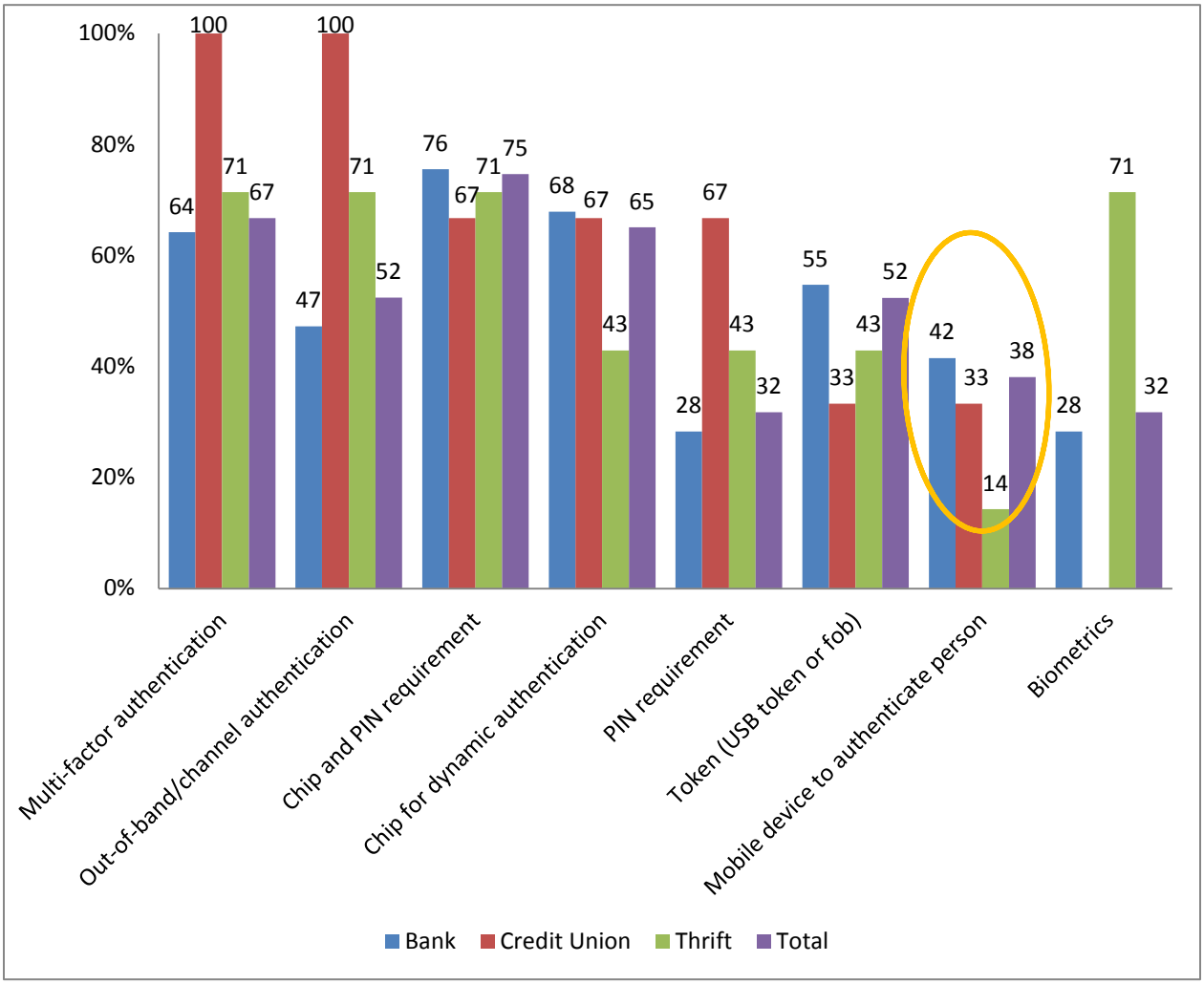


Chart U: Adoption Preferences of Authentication Methods (*% of FI Respondents, n=63*)



In Table 7, FIs indicated the new security controls and other activities that they felt would be needed to reduce payments fraud. Replacement of the magnetic stripe technology was number one, selected by 79% of the (63) respondents. This may be indicative of the growing interest in the U.S. by FIs and other payments stakeholders in migrating to EMV to improve card security, recognizing that current mag stripe cards are not as secure as EMV chip cards being implemented in most other developed countries, including Canada. A close second (68%) was the desire for authentication controls to protect Internet payments, which will not be addressed by replacing mag strip cards with chip cards.

Table 7: New Methods Needed by FIs *(% of FI Respondents)*

New Methods Needed	All FIs (*n=63*)
Replacement of card, magnetic stripe technology	79%
Authentication controls over Internet initiated payments	68%
Consumer education on fraud prevention	62%
Authentication controls over mobile device initiated payments	57%
Improved methods for information sharing on emerging fraud	49%
Industry specific education on payments fraud prevention best practices	48%
More aggressive law enforcement	44%
Industry alert services	40%
Image survivable check security features for business checks	21%
Other	13%

4. Barriers to Reducing Payments Fraud

FIs identified lack of staff resources and implementation costs as the top barriers to mitigating fraud (Table 8). Since most respondents are relatively small FIs, they may lack the financial capability to dedicate special resources to managing fraud prevention and detection. At the same time, fraud prevention tools that could reduce manual labor involved in fraud management efforts may be cost prohibitive, as reported by over half of the respondents in Table 8.

Table 8: Main Barriers to Payments Fraud Mitigation *(% of FI Respondents)*

Barriers	All FIs (*n=59*)
Lack of staff resources	54%
Cost of implementing commercially available fraud detection tool/service	54%
Cost of implementing in-house fraud detection tool/service	41%
Lack of compelling business case (cost vs. benefit) to adopt new or change existing methods	37%
Consumer data privacy issues/concerns	34%
Unable to combine payment information for review due to operating w/ multiple business areas, states, or banks	20%
Corporate reluctance to share information due to competitive issues	15%
Other	9%

5. Legal and Regulatory Considerations

Table 9 summarizes all responses regarding legal and regulatory changes that could help reduce payments fraud. Highlighted changes reflect the top three actions that FIs in the First District suggest would help reduce payments fraud. All three relate to placing more responsibility on the appropriate parties involved in preventing the fraud, including customers. Placing more responsibility on customers to reconcile and protect their payments data ranked third, selected by 76% of the FIs. A much higher percentage of FIs in the First District also identified increased penalties for fraud and attempted fraud as important.

Table 9: Legal and Regulatory Considerations (*% of FI Respondents*)

Legal and Regulatory Changes	**First District** *n=63*	**Consolidated Results** *n=540*
Place responsibility to mitigate fraud and shift liability for fraudulent card payments to entity that initially accepts card payments	89%	64%
Assign liability for fraud losses to party most responsible for not acting to reduce the risk of payment fraud	79%	60%
Place more responsibility on consumers and customers to reconcile and protect their payment data	76%	69%
Focus future legal or regulatory changes on data breaches to where breaches occur	76%	43%
Increase penalties for fraud and attempted fraud	66%	71%
Strengthen disincentives to committing fraud through more likely prosecution	56%	51%
Align Regulation E and Regulation CC to reflect changes in check collection systems' use of check images and conversion of checks to ACH	53%	40%
Assign responsibility for mitigating risk to party best positioned to take action against fraud	48%	39%
Improve law enforcement cooperation on domestic and international payments fraud and fraud rings	42%	49%
Establish new laws/regs or change existing ones in order to strengthen management of payments fraud risks	27%	29%

6. Conclusions

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

- Financial institutions, whether they are commercial and community banks, thrifts or credit unions, continue to be concerned about payments-related fraud in the First District. All respondents experienced some number of payment fraud attempts and incurred payment fraud losses.

- For all types of FIs in the First District, signature and PIN debit cards and checks are the payment instruments most vulnerable to fraud attempts and losses.

- Over 60% of FIs reported that signature debit card and check 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.

- Most FIs reported total fraud losses that represented less than 0.3% of their annual revenue. 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 FIs. Transaction monitoring, transaction authentication, and other risk management services are also used by a majority of FIs. However, the most frequently used methods were not necessarily the most effective.

- Nineteen percent of respondents reported reduced fraud losses and attributed this to changes made in risk management tools and enhanced fraud monitoring systems.

- The majority of FIs cited cost as a major barrier that prevents them from investing in additional staff and detection tools to mitigate payments fraud.

- Almost 80% of respondents indicated the need for alternatives to magnetic stripe authentication technology to secure card payments and reduce payments fraud, which may be indicative of the growing interest of FIs and other payments stakeholders in migrating to EMV chip technology for cards (and possibly mobile payments in the future).

Appendix: 2012 Payments Fraud Questionnaire

Survey Questions and Corresponding Charts/Tables

Question	Table/Chart
1	Chart A
2	Table 1
6	Table 2
7	Chart B
9	Table 3
13	Chart C
14	Chart D
15	Chart F
16	Chart E
17	Chart G
18	Chart H
19	Chart H
20	Chart J
21	Chart H
24	Chart K
25	Table 5
27	Chart L
28	Chart M
29	Table 6
30	Chart N
31	Chart O
32	Chart P
33	Chart Q
34	Chart R
35	Chart S
36	Chart T
39	Table 7
40	Chart U
41	Table 8
42	Table 9

2012 Payments Fraud Questionnaire

The survey was administered online. Information in red font represented logic in the survey tool and was not displayed. Bullet formatting – if bullets are circles, then respondent could choose only one answer. If bullets are squares, respondents could choose one or more answers.

Introduction

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

Payments Fraud Survey Instructions

- Please try to answer all questions the best you can. If you are unsure, please provide your best estimate.
- It is best if you do not exit the survey until all questions have been completed. The survey should take about 20 minutes to complete.
- Use the "Save" button if you wish to review or modify a response. You may need to copy and save a new link to return to your survey, depending on how you received the survey invitation. The online survey tool will provide this link during the save process. To return to the survey, paste the new link into your browser. You will be directed to the first survey question. Click the "Next" button to view or modify your previous answers.
- Do not use the "Back" button on your browser to review your completed questions. The survey does not support use of this.
- Responses will be sent to the Federal Reserve Bank after the "Submit Survey" button on the last page has been clicked.

Confidentiality of Response

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

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

Organization Profile:

1. A) Is your organization a banking or financial services organization?
   - o Yes Go to Q1B
   - o No Go to Q1C

1. B) Please select the type of financial services organization below.
   - o Bank
   - o Credit Union
   - o Thrift
   - o Service provider
   - o Insurance company and pension funds
   - o Brokers, underwriters and investment company

1. C) How do you classify your organization? (Please select one answer)

- o Agriculture
- o Brokers, underwriters and investment company
- o Business services/Consulting
- o Construction
- o Educational services
- o Energy
- o Government
- o Health services
- o Hospitality/Travel
- o Insurance company and pension funds
- o Manufacturing
- o Nonprofit
- o Real estate/Rental/Leasing
- o Retail trade
- o Software/Technology
- o Telecommunications
- o Transportation/Warehousing
- o Wholesale trade
- o Other, please specify _____

2. What is your … Ask when answer to Q1B is Bank, Credit Union, or Thrift and then go to Q4 next.

Financial institution name _____
City/Town ___ _____
State Choose response from drop down list.
ZIP/Postal Code _ _ _ _ _
Main nine digit routing and transit number. Please specify the head office number.
_ _ _ _ - _ _ _ _ - _ Response must be numeric.

3. What is your… Skip when answer to Q1B is Bank, Credit Union, or Thrift.

Company Name: _____
City/Town: _____
State Choose response from drop down list.
ZIP/Postal Code _ _ _ _ _

4. What is…

Your name _____ (optional)
Your title _____ (optional)

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

E-mail address _____ (optional)

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

- o Accounts payable or receivable
- o Audit
- o Compliance/Risk Management
- o Finance
- o Operations/Payments processing function
- o Senior management over multiple departments
- o Treasury
- o Other

6. What do you estimate are your organization's 2011 annual revenues? If you don't know, please provide your best estimate.

- o Under $50 million
- o $50 – 99 million
- o $100 – 249.9 million
- o $250 - 499.9 million
- o $500 - 999.9 million
- o $1 – 4.9 billion
- o $5 – 9.9 billion
- o $10 billion or more
- o Not applicable

7. What is the size of your financial institution based on year-end 2011 total assets? If you don't know, please provide your best estimate. Ask when answer to Q1B Bank, Credit Union, or Thrift.

- o Under $50 million
- o $50 – 99 million
- o $100 – 249.9 million
- o $250 - 499.9 million
- o $500 - 999.9 million
- o $1 – 4.9 billion
- o $5 – 9.9 billion
- o $10 billion or more

8. Are you or your bank a member of a banking association? (Select all that apply.) A when answer to Q1B is a bank.

- ☐ Independent Community Bankers of America (ICBA)
- ☐ A state banking association
- ☐ Other
- ☐ None

9. In terms of your organization's payments volume, who are the typical counterparties? Note: Businesses includes government entities. Skip Q9 when answer to Q1B is Bank, Credit Union, or Thrift.

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

10. What types of payments does your organization accept? Skip Q10 when answer to Q1B is Bank, Credit Union, or Thrift.

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

11. What types of payments does your organization use to disburse payments? Skip Q11 when answer to Q1B is Bank, Credit Union, or Thrift.

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

12. To what type of customers does your financial institution typically offer payment products and services? Ask when answer to Q1B is Bank, Credit Union, or Thrift.

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

13. Which of the following payments products does your financial institution offer? Select all that apply. Ask when answer to Q1B is Bank, Credit Union, or Thrift.

Payment Products	Offer
Credit cards	☐
Debit cards – PIN based	☐
Debit cards – signature based	☐
Prepaid cards, e.g., gift, payroll, etc.	☐
Check instruments	☐
Automated Clearinghouse (ACH) Origination	☐
Wire transfer	☐
Bill payment	☐
Lockbox services	☐
International payments	☐
Mobile payments	☐
P2P payments	☐
Remote deposit capture	☐

Fraud by Payment Type:

14. Indicate the payment types where your organization experienced the highest number of fraud attempts (regardless of actual financial losses) in 2011. Select up to three that you think are highest.

- ☐ Credit cards
- ☐ Debit cards – PIN based
- ☐ Debit cards – signature based
- ☐ Prepaid cards
- ☐ Checks
- ☐ Automated Clearinghouse credits
- ☐ Automated Clearinghouse debits
- ☐ Cash
- ☐ Wire

or

- ☐ No payment fraud attempts experienced.

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

Payment Product	Fraud prevention costs	Actual fraud dollar losses	Don't use/offer payment type
Credit cards	O	O	O
Debit cards – PIN based	O	O	O
Debit cards – signature based	O	O	O
Prepaid cards	O	O	O
Check instruments	O	O	O
Automated Clearinghouse (ACH)	O	O	O
Mobile	O	O	O

16. Indicate the payment types where your organization has experienced the highest dollar losses due to fraud in 2011. Select up to three that you think are highest.

- ☐ Credit cards
- ☐ Debit cards – PIN based
- ☐ Debit cards – signature based
- ☐ Prepaid cards
- ☐ Checks
- ☐ Automated Clearinghouse credits
- ☐ Automated Clearinghouse debits
- ☐ Cash
- ☐ Wire

  or
- ☐ No payment fraud attempts experienced.

17. For your organization, please estimate the financial losses experienced due to payments fraud during 2011 as a percent of the company's total revenue.

- o 0% - no payments fraud losses experienced
- o Over 0% but less than .3%
- o .3% - .5%
- o .6% - 1.0%
- o 1.1% - 5.0%
- o over 5%

18. For your organization, how has the percentage of financial losses due to payments fraud changed in 2011 compared to 2010? If the answer to Q17 is 0%, only show Q18 response options of "stayed the same" or "decreased".

- o Increased (go to Q 19)
- o Stayed the same (go to Q 25)
- o Decreased (go to Q 21)

19. The percentage of dollar losses at my organization due to fraud has increased by __% in 2011 compared to 2010. (go to 20)

- o 1 - 5%
- o 6% - 10%
- o More than 10%
- o Unsure

20. To which payment types do you attribute the 2011 increase in your organization's actual dollar losses? Select all that apply. (go to Q 25)

- ☐ Credit cards
- ☐ Debit cards – PIN based
- ☐ Debit cards – signature based
- ☐ Prepaid cards
- ☐ Checks
- ☐ Automated Clearinghouse credits
- ☐ Automated Clearinghouse debits
- ☐ Cash
- ☐ Wire

21. The percentage of dollar losses at my organization due to fraud has decreased by __% in 2011 compared to 2010. (go to 22)

- o 1 - 5%
- o 6% - 10%
- o More than 10%
- o Unsure

22. To which payment types do you attribute the 2011 decrease in your organization's actual dollar losses? Select all that apply. (go to Q23)

- ☐ Credit cards
- ☐ Debit cards – PIN based
- ☐ Debit cards – signature based
- ☐ Prepaid cards
- ☐ Checks
- ☐ Automated Clearinghouse credits
- ☐ Automated Clearinghouse debits
- ☐ Cash
- ☐ Wire

23. Did your organization make changes to its payments risk management practices that led to the decrease in 2011 payments fraud losses? If answer to Q23 is "no", then skip Q24 and go to Q25.

- o Yes
- o No

24. What are the key changes made by your organization that you think have contributed to the decrease in your organization's payments fraud losses? Select all that apply. (go to Q 25)

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

25. For payment fraud that was successful, please estimate the percentage that involved... Answers should total 100%. (Please enter only numbers from 0 – 100, without a decimal point, % sign or space.)

Only internal staff from your own organization_____%
Internal staff collaborating with external parties _____%
Only external parties _____%
Unknown- could not determine_____%
or
No successful attempts (fill in 100% here) _____%

Common Fraud Schemes and Mitigation Strategies:

26. For payments received by your organization, what are the three current fraud schemes that fraudsters are using most often to initiate payments fraud? Select no more than three. Skip when answer to Q1B is Bank, Credit Union, Thrift or Service Provider.

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

27. For payments by or on behalf of your customers, what are the three current fraud schemes that fraudsters are using most often to initiate payments fraud? Select no more than three. Ask when answer to Q1B is Bank, Credit Union, Thrift or Service Provider.

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

28. Against your organization's own bank accounts, what are the three current fraud schemes that fraudsters are using most often to initiate payments fraud? Select no more than three.

- ☐ Altered or forged checks
- ☐ Counterfeit checks drawn against your accounts
- ☐ Fraudulent or unauthorized ACH debits against your accounts
- ☐ Fraudulent or unauthorized card transactions against your corporate/commercial card accounts
- ☐ Payment fraud due to breach of access or other data security controls to your organization's payment processes, e.g., account takeovers
- ☐ Check or electronic payment made by organization due to internal fraud scheme
- ☐ Other (please specify) _____

29. In your response to the last two questions, you identified the most often used fraud schemes in payments fraud attempts experienced by your organization. What are the top three sources of information fraudsters used for these attempts? Select no more than three.

- ☐ Information about customer obtained by family or friend
- ☐ "Sensitive" information obtained from lost or stolen card, check, or other physical document or device while in consumer's control
- ☐ Physical device tampering e.g., use of skimmer on POS terminal or ATM to obtain card magnetic stripe information
- ☐ Email and webpage cyber attacks e.g., phishing, spoofing, and pharming used to obtain "sensitive" customer information
- ☐ Lost or stolen physical documentation or electronic PC/device while in control of the organization
- ☐ Data breach due to computer hacking e.g., use of default or guessable credentials, brute force attacks, access through open ports or services, etc.
- ☐ Organization's information obtained from a legitimate check issued by your organization
- ☐ Employee misuse, e.g., employee with legitimate access to organization or customer information
- ☐ Other (please specify) _____

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

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

30. Which of the following authentication methods does your organization currently use or plan to use to mitigate payment risk? Limit response to one per row.

	Currently use	Plan to use before 2014	Don't use
Verify customer state identification card is authentic (machine read magnetic stripe or 2-D bar code)	O	O	O
Positive identification of purchaser or valid account for in-store/in-person transactions e.g., review picture ID	O	O	O
Card security code located on back of payment card verified e.g., CVV2, CVC2, or CID codes	O	O	O
Signature verification	O	O	O
Customer (consumer or business) authentication for online transactions	O	O	O
Biometrics authentication	O	O	O
Magnetic stripe authentication	O	O	O
Card chip authentication	O	O	O
PIN authentication	O	O	O
Real-time decision support during account application or point of sale, e.g., score or alert on potential or known ID fraud or account takeover	O	O	O

Are the other authentication methods your organization currently uses to mitigate payment risk?
Other methods (please specify) _____

31. Please rate the effectiveness of authentication methods currently used by your organization. List only the methods selected as "currently use" in Q30. Limit response to one per row.

	Very effective	Somewhat effective	Somewhat ineffective
Verify customer state identification card is authentic (machine read magnetic stripe or 2-D bar code)	O	O	O
Positive identification of purchaser or valid account for in-store/in-person transactions e.g., review picture ID	O	O	O
Card security code located on back of payment card verified e.g., CVV2, CVC2, or CID codes	O	O	O
Signature verification	O	O	O
Customer (consumer or business) authentication for online transactions	O	O	O
Biometrics authentication	O	O	O
Magnetic stripe authentication	O	O	O
Card chip authentication	O	O	O
PIN authentication	O	O	O
Real-time decision support during account application or point of sale, e.g., score or alert on potential or known ID fraud or account takeover	O	O	O

32. Which of the following transaction screening and risk management methods does your organization currently use or plan to use to mitigate payment risk? Limit response to one per row.

	Currently use	Plan to use before 2014	Don't use
Human review of payment transactions	O	O	O
Fraud detection pen for currency	O	O	O
Software that detects fraud through pattern matching, predictive analytics, or other indicators	O	O	O
Centralized fraud-related information database for one payment type	O	O	O
Centralized fraud-related information database for multiple payment types	O	O	O
Participate in fraudster databases and receive alerts	O	O	O
Centralized risk management department	O	O	O
Provide customer education and training on payment fraud risk mitigation	O	O	O
Provide staff education and training on payment fraud risk mitigation	O	O	O

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

Other methods (please specify)_____

33. Please rate the effectiveness of the transaction screening and risk management methods used by your organization. List only the methods selected as "currently use" in question 32. Limit response to one per row.

	Very effective	Somewhat effective	Somewhat ineffective
Human review of payment transactions	O	O	O
Fraud detection pen for currency	O	O	O
Software that detects fraud through pattern matching, predictive analytics, or other indicators	O	O	O
Centralized fraud-related information database for one payment type	O	O	O
Centralized fraud-related information database for multiple payment types	O	O	O
Participate in fraudster databases and receive alerts	O	O	O
Centralized risk management department	O	O	O
Provide customer education and training on payment fraud risk mitigation	O	O	O
Provide staff education and training on payment fraud risk mitigation	O	O	O

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

	Currently use	Plan to use before 2014	Don't use
Physical access controls to payment processing functions	O	O	O
Logical access controls to your computing network and payment processing applications	O	O	O
Dedicated computer used to conduct transactions with financial institution or financial service	O	O	O
Authentication and authorization controls to payment processes	O	O	O
Restrict or limit employee use of Internet from organization's network	O	O	O
Dual controls and segregation of duties within payment initiation and receipt processes	O	O	O
Transaction limits for payment disbursements	O	O	O
Transaction limits for corporate card purchases	O	O	O
Reconcile bank accounts daily	O	O	O
Review card related reports daily	O	O	O
Address exception items timely	O	O	O
Separate banking accounts by purpose or by payment type	O	O	O
Employee hotline to report potential fraud	O	O	O
Verify application of controls via audit or management review	O	O	O
Periodic internal/external audits	O	O	O

Are there any other internal controls and procedures your organization currently uses?
Other internal controls or procedures (please specify)_____

35. Please rate the effectiveness of the internal controls and procedures used by your organization. List only the controls/procedures selected as "currently use" in question 34. Limit response to one per row.

	Very effective	Somewhat effective	Somewhat ineffective
Physical access controls to payment processing functions	O	O	O
Logical access controls to your computing network and payment processing applications	O	O	O
Dedicated computer used to conduct transactions with financial institution or financial service	O	O	O
Authentication and authorization controls to payment processes	O	O	O
Restrict or limit employee use of Internet from organization's network	O	O	O
Dual controls and segregation of duties within payment initiation and receipt processes	O	O	O
Transaction limits for payment disbursements	O	O	O
Transaction limits for corporate card purchases	O	O	O
Reconcile bank accounts daily	O	O	O
Review card related reports daily	O	O	O
Address exception items timely	O	O	O
Separate banking accounts by purpose or by payment type	O	O	O
Employee hotline to report potential fraud	O	O	O
Verify application of controls via audit or management review	O	O	O
Periodic internal/external audits	O	O	O

36. What risk mitigation services offered by your financial institution/service provider does your organization use? Skip Q36 – 37 if answer to Q1B is Bank, Credit Union, Thrift or Service Provider. Limit response to one per row.

	Currently use	Plan to use before 2014	Don't use
Check positive pay/reverse positive pay	O	O	O
Check payee positive pay	O	O	O
Post no check services	O	O	O
ACH debit blocks	O	O	O
ACH debit filters	O	O	O
ACH positive pay	O	O	O
ACH payee positive pay	O	O	O
Account masking services	O	O	O
Account alert services	O	O	O
Card alert services for commercial/corporate cards	O	O	O
Fraud loss prevention services e.g., insurance	O	O	O
Online information services, e.g., statements, check images	O	O	O
Multi-factor authentication controls to initiate payments from bank account	O	O	O

Are there other risk mitigation services offered by your financial institutions/service provider that your organization uses?

Other services (please specify)_____

37. Please rate the effectiveness of risk mitigation services used by your organization? Skip Q36 – 37 if answer to Q1B is Bank, Credit Union, Thrift or Service Provider. Limit response to one per row. List only the risk mitigation services where response was "currently use" in Q 36.

	Very effective	Somewhat effective	Somewhat ineffective
Check positive pay/reverse positive pay	O	O	O
Check payee positive pay	O	O	O
Post no check services	O	O	O
ACH debit blocks	O	O	O
ACH debit filters	O	O	O
ACH positive pay	O	O	O
ACH payee positive pay	O	O	O
Account masking services	O	O	O
Account alert services	O	O	O
Card alert services for commercial/corporate cards	O	O	O
Fraud loss prevention services e.g., insurance	O	O	O
Online information services, e.g., statements, check images	O	O	O
Multi-factor authentication controls to initiate payments from bank account	O	O	O

38. What risk mitigation services/products does your organization currently offer or plan to offer to your businesses customers? Ask when the answer to Q1B is Bank, Credit Union, Thrift or Service Provider. Limit response to one per row.

	Currently use	Plan to use before 2014	Don't use
Check positive pay/reverse positive pay	O	O	O
Check payee positive pay	O	O	O
Post no check services	O	O	O
ACH debit blocks	O	O	O
ACH debit filters	O	O	O
ACH positive pay	O	O	O
ACH payee positive pay	O	O	O
Account masking services	O	O	O
Account alert services	O	O	O
Card alert services for commercial/corporate cards	O	O	O
Fraud loss prevention services e.g., insurance	O	O	O
Online information services, e.g., statements, check images	O	O	O
Multi-factor authentication controls to initiate payments from bank account	O	O	O

Are there other risk mitigation services offered by your financial institutions/service provider that your organization uses?

Other services (please specify)_____

39. From your organization's perspective, what new or improved methods are most needed to reduce payments fraud? Select those you think would be most helpful.

- ☐ Authentication controls over Internet initiated payments
- ☐ Authentication controls over mobile device initiated payments
- ☐ Replacement of card, magnetic stripe technology
- ☐ Improved methods for information sharing on emerging fraud tactics e.g., those being conducted by criminal rings
- ☐ More aggressive law enforcement
- ☐ Image survivable check security features for business checks
- ☐ Industry alert services
- ☐ Industry specific education on payments fraud prevention best practices
- ☐ Consumer education of fraud prevention
- ☐ Other (please specify) _____

40. What authentication methods would your organization prefer or consider adopting to help reduce payments fraud? Select all methods your organization would most likely prefer or consider for adoption.

- ☐ Biometrics
- ☐ Chip for dynamic authentication (e.g., EMV)
- ☐ Chip and PIN requirement
- ☐ PIN requirement
- ☐ Token (USB token or fob)
- ☐ Mobile device to authenticate person
- ☐ Out-of-band/channel authentication (email, text, fax, or phone) to authorize payment
- ☐ Multi-factor authentication
- ☐ Other (please specify) _____

41. What are the main barriers to mitigate payments fraud that your organization experiences? Select all that you consider to be the main barriers.

- ☐ Consumer data privacy issues/concerns
- ☐ Corporate reluctance to share information due to competitive issues
- ☐ Cost of implementing in-house fraud detection tool/method If selected ask:
- ☐ Please describe what tool/method your organization wants to implement, but cannot afford to do so _____
- ☐ Cost of implementing commercially available fraud detection tool/service If selected ask:
- ☐ Please describe what tool/service your organization wants to implement, but cannot afford to do so _____
- ☐ Lack of compelling business case (cost vs. benefit) to adopt new or change existing methods
- ☐ Lack of staff resources
- ☐ Unable to combine payment information for review due to payments operations performed in multiple business areas, multiple states, with multiple banks, etc. Corporate reluctance to share information due to competitive issues
- ☐ Other (please specify) _____

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

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

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