2014 Payments Fraud Survey

First District Summary of Results

Federal Reserve Bank of Boston

Payment Strategies

11/18/2014

Contents

1. Introduction

In 2014, the Federal Reserve Bank of Boston's Payment Strategies group conducted research on payments-related fraud experienced by financial institutions (FIs) as well as non-financial institutions (non-FIs) in the First District.[1] We asked our 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, prepaid cards, the automated clearinghouse (ACH), and wire transfers.

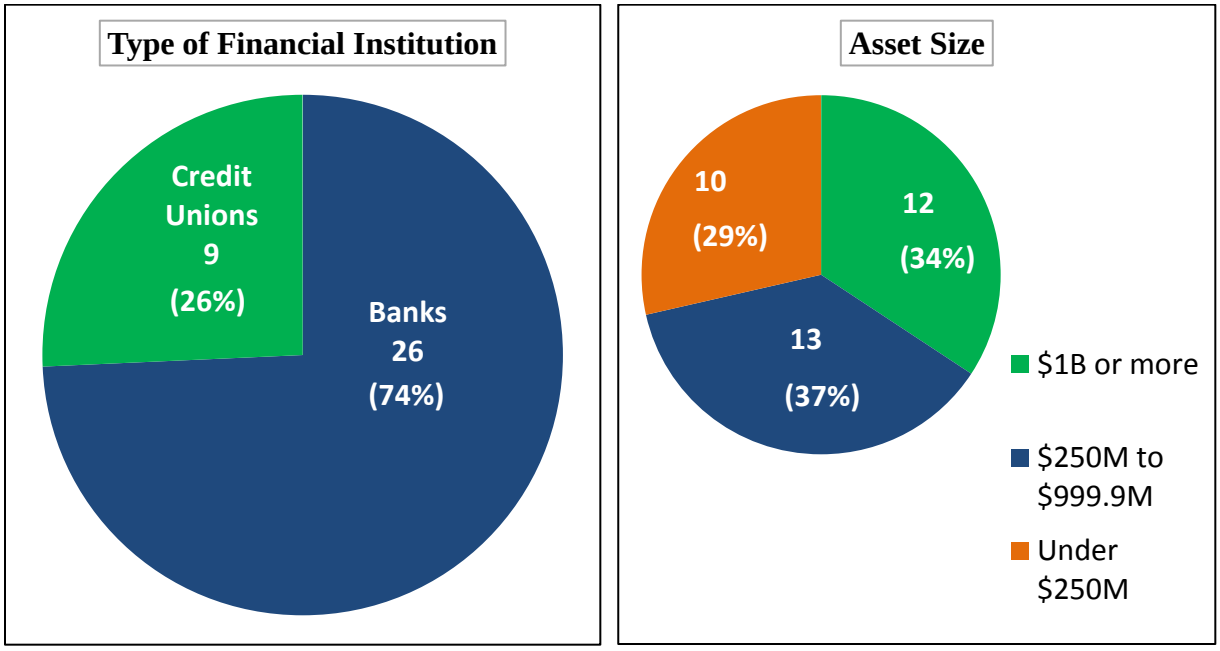
This survey was part of a broader initiative conducted in conjunction with the Federal Reserve Banks of Chicago, Dallas, Minneapolis, and Richmond. While focused primarily on results from FIs in the First District, this report contains some comparisons of First District data to consolidated results of survey data from all the participating Federal Reserve Banks and the ICBA.

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

2. FI Respondent Profile

Thirty-five financial institutions (FIs) responded to the survey, which represents just five percent of the total FIs in New England. FIs self-identified as banks, credit unions or thrifts[2]. (See Chart A.) FIs represented all New England states except Rhode Island, with Massachusetts having the highest number (22). (See Table 1.) FI respondents are evenly dispersed by Asset Size range (Chart B). Twelve of the 35 FIs have assets over $1 billion.

Chart A: Financial Institutions by Type and Asset Size (n=35)



Q1b. Select type of financial services organization (Bank, Credit Union, Thrift, Service Provider)
Q7. What is the size of your financial institution based on year-end 2013 total assets?

Table 1 compares the actual number of financial institutions in New England to the number and percentage of FI survey respondents by state. Table 2 categorizes respondents by annual revenue, with over half of the respondents (20 out of 35) reporting annual revenues under $10 million and only two respondents reporting annual revenue of over $500 million.

[2] As only one respondent identified as a thrift, it has been included with bank results.

Table 1: Total Number of FIs by New England State

State	Total Number[3]			FI Respondents (n=35)	
	Banks	Credit Unions	Total	Survey Respondents	% of total FIs
Connecticut	45	115	160	2	1%
Maine	28	61	89	5	6%
Massachusetts	149	189	338	22	7%
New Hampshire	20	19	39	5	13%
Rhode Island	10	21	31	0	0%
Vermont	13	24	37	1	3%
Total	265	429	694	35	5%

Table 2: Annual FI Revenue

Annual Revenue	Bank *n=26*	Credit Union *n=9*	All FIs *n=35*
$500 million or more	0	1	1
$10 million to $499.9 million	9	2	11
Under $10 million	13	4	17
Non Applicable / Don't Know	4	2	6
Total	**26**	**9**	**35**

Q6. What do you estimate are your organization's 2013 annual revenues?

[3] FDIC data as of August 2014; NCUA data as of June 2014

3. Summary of Survey Results

Payment Products Offered by FIs in New England

FI respondents were asked whether their customer base comprised primarily of consumers, commercial/business clients, or both. As indicated in Table 3, 25 FIs offer services to both consumer and commercial customers, while only one FI primarily services business or commercial clients.

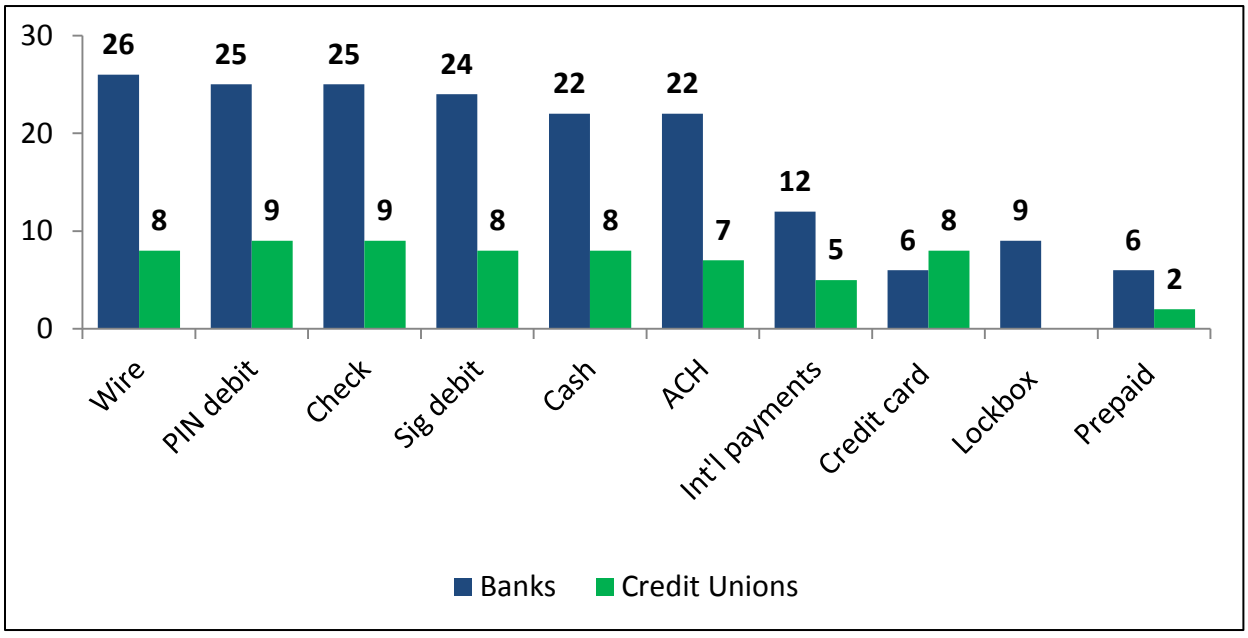
Table 3: Types of Customers to which FIs Offer Payment Services

Target Customers	Bank *n=26*	Credit Union *n=9*	All FIs *n=35*
Both consumer and business/commercial clients	20	5	25
Primarily business or commercial clients	1	0	1
Primarily consumer	5	4	9

Q12. To what type of customers does your financial institution typically offer payment products and services?

Chart B illustrates the types of payment products and services FIs offer. Wire, check and debit cards are the services most commonly offered. All banks offer wire transfers, while 8 of 9 credit unions offer wire transfers. All credit unions, and all but one bank, offer PIN debit cards and checks.

Chart B: Payment Products and Services FIs Offer (# of FI Respondents)

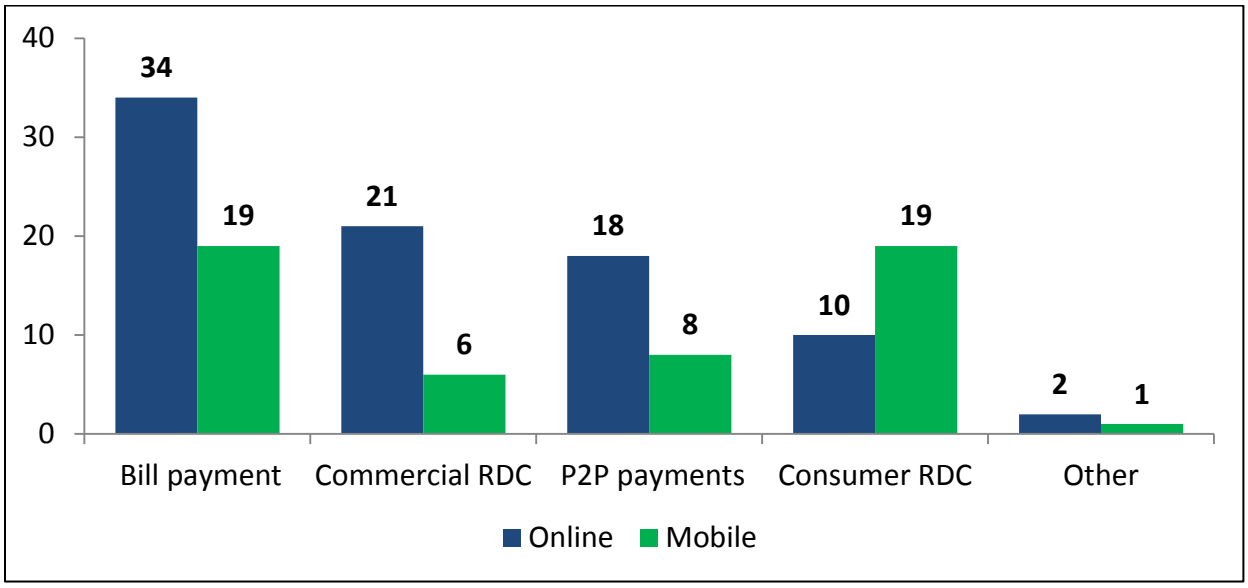


Q13. Which of the following payments products does your financial institution offer? (Select all that apply.)

Mobile Payment Services

In addition to traditional payment products, a growing number of FIs offer online banking services via the mobile channel. These mobile banking services include mobile bill payment, person-to-person (P2P) payments, and remote deposit capture (mRDC). Mobile technology adoption was relatively high among First District FI respondents, with 25 indicating that they offer some form of mobile service. More than half of FI respondents (19 of 35) offer mobile bill payment, and eight FIs offer mobile P2P payments. While mobile RDC is still a relatively new feature, many respondents provide the service to both their retail and business customers – 19 FIs reported offering consumer mRDC and six FIs reported offering commercial mRDC.

Chart C: Online & Mobile Payment Products and Services FIs Offer (# of FI Respondents)

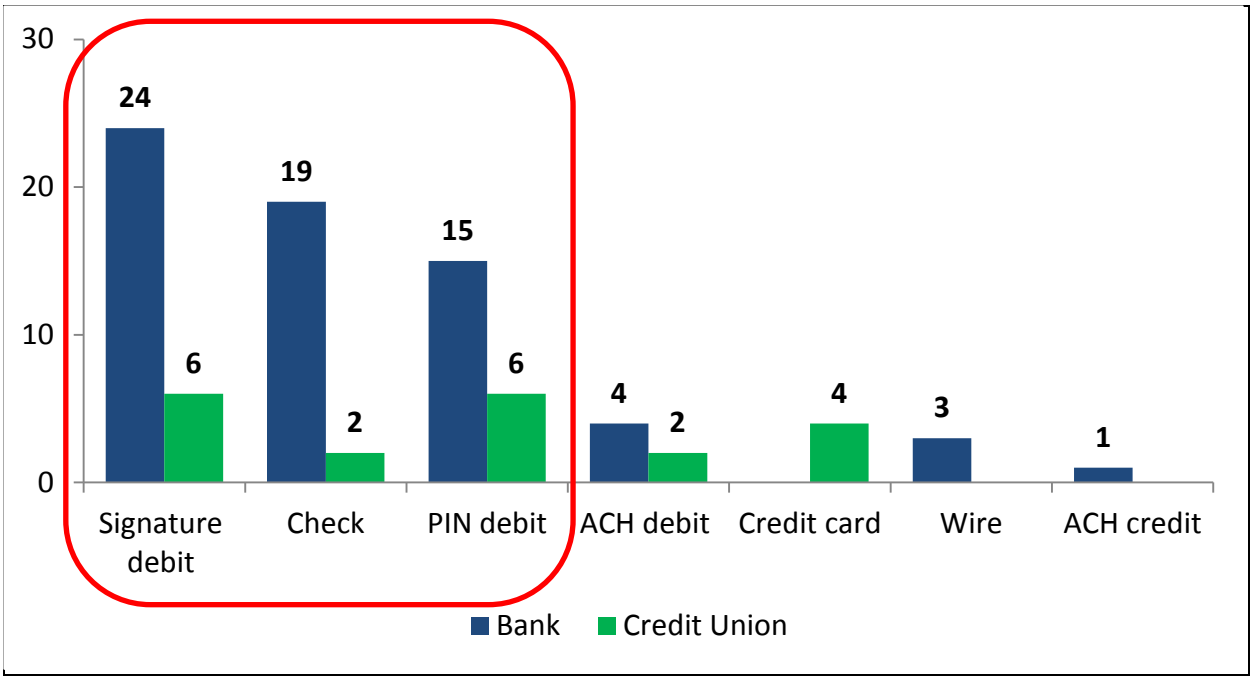


Q13. Which of the following payments products does your financial institution offer (as an online service and/or mobile service)? (Select all that apply.)

Payment Fraud Attempts and Financial Losses

Most FIs reported experiencing some fraud attempts. Respondents reported payment types which 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 24 banks and six credit unions reporting attempts of this type of fraud in 2014. PIN debit cards and checks experienced the next highest number of fraud attempts.[4] Similar to results of the 2012 survey, the same three products experienced the most fraud attempts.

Chart D: Top Three Payment Types with Highest Number of Fraud Attempts (# of FI respondents)

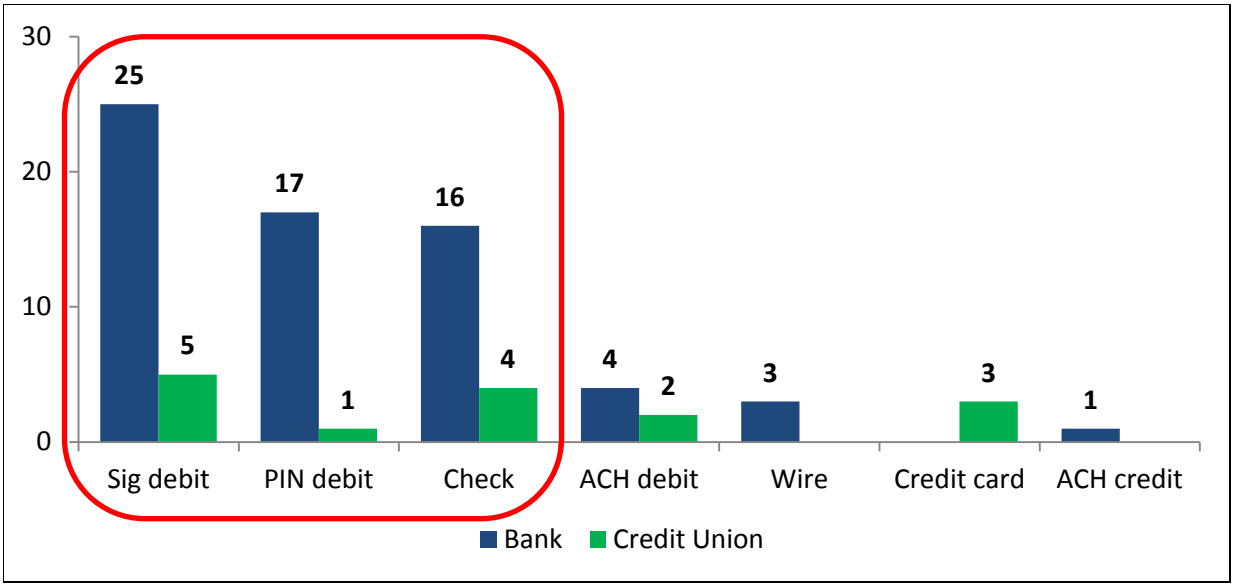


Q15. Indicate the payment types where your organization experienced the highest number of fraud attempts (regardless of actual financial losses) in 2013. (Select and rank up to three that are highest.)

[4] This is in line with the Federal Reserve's triennial report on payments released in December 2013, which found that signature debit cards were among the most susceptible to fraud, and the risk was highest for online transactions, which had about triple the fraud rate of "card-present" transactions. According to the same report, PIN Debit had the lowest fraud rates.
http://www.frbservices.org/files/communications/pdf/research/2013_payments_study_summary.pdf

Consistently, payment types with highest dollar losses due to fraud correspond to those with the highest fraud attempts (Charts D and E). The number of FIs that reported the highest dollar losses due to PIN debit card and check fraud were 20 and 18 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 14 respondents offer credit cards (vs. 34 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.[5]

Chart E: Top Three Payment Types with Highest Fraud Dollar Losses (# of FI Respondents)



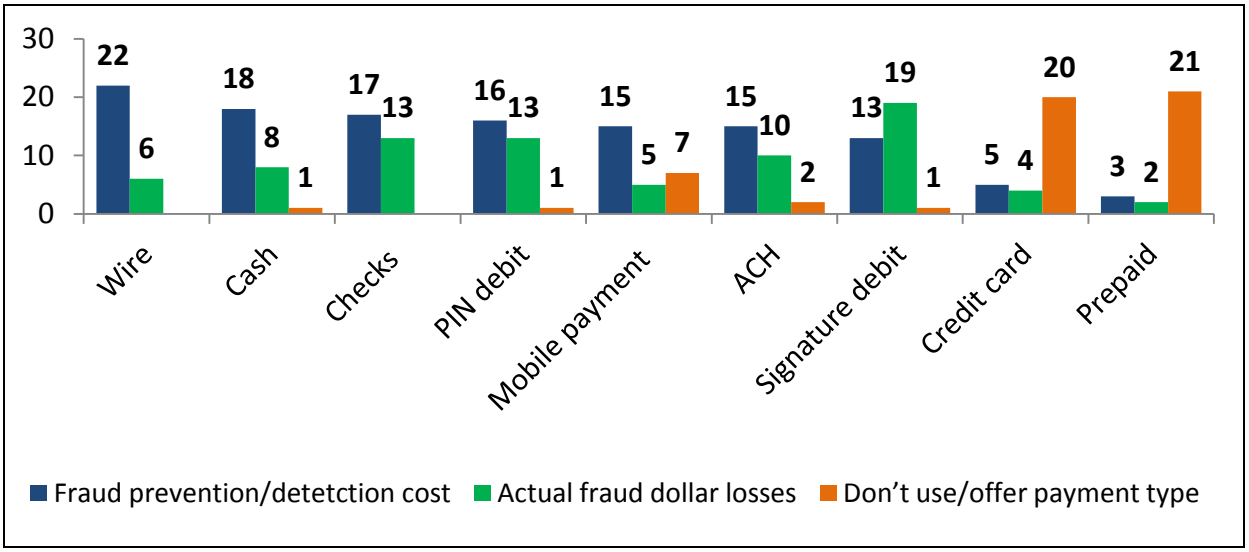
Q19. Indicate the payment types where your organization has experienced the highest dollar losses due to fraud in 2013. (Select and rank up to three that are highest.)

[5] No banks and only four credit unions reported fraud attempts for credit cards in their top 3.

Cost of Fraud Prevention vs. Actual Fraud Loss

For each type of payment service, FI respondents indicated whether fraud prevention or the actual fraud dollar losses cost more to their organization, as shown in Chart F. More than half of the FIs considered *prevention and detection* to be costlier than actual fraud dollar losses for PIN debit, ACH, mobile payment, checks, cash, and wire. Nineteen FIs reported that actual fraud losses exceeded the cost of prevention and detection for signature debit. While fewer than ten respondents reported offering credit and prepaid cards, (credit card: 9, prepaid: 5), responses were slightly higher for fraud prevention and detection costs exceeding actual fraud dollar losses for both payment methods.

Chart F: Fraud Prevention Costs vs Actual Dollar Fraud Losses (# of FI respondents)



Q16. For these payment types, which is a greater expense for your organization– fraud prevention costs or actual dollar losses?

Financial Losses Due to Fraud

FIs were asked to select the fraud loss dollar range as a percentage of total annual revenue. Most (24) selected the lowest option (less than 0.3%) and only one reported fraud losses of 1.1%-5% of annual revenue. None reported 2013 losses in over 5%. (See Table 4.)

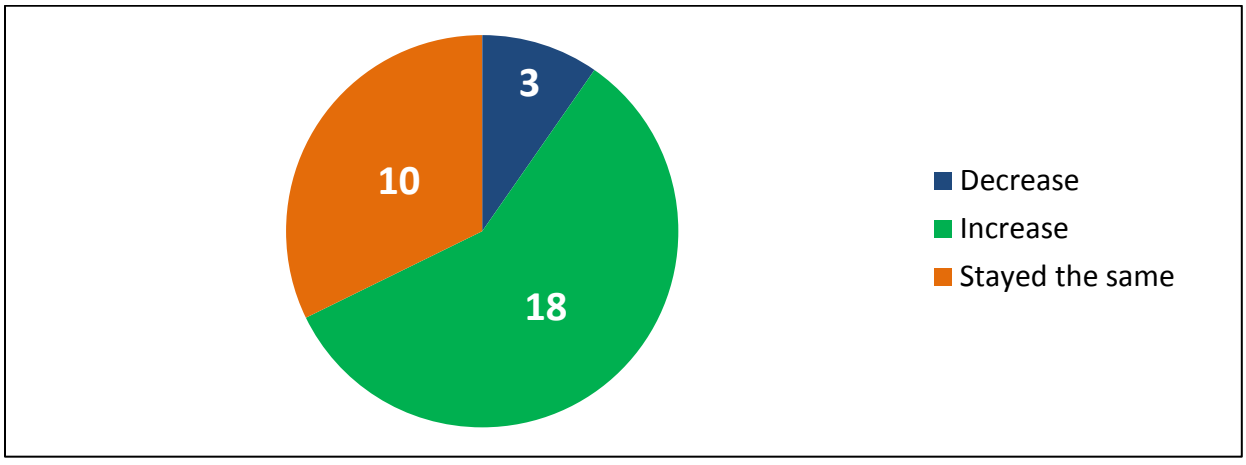
Table 4: FI Payments Fraud Loss Rates: 1st District 2013 vs. 2011 (# of FI Respondents)

Loss Range as a Percent of Annual Revenue	2013	2011
Less than 0.3%	24	41
0.3% - 0.5%	2	14
0.6% - 1%	5	3
1.1% - 5%	1	6
Over 5%	0	1

Q21. Please estimate the financial losses experienced due to payments fraud during 2013 as a percent of your company's total revenue.

Eighteen (58%) First District FIs reported increases in actual dollar fraud losses in 2013 from fiscal year 2012, while only three (10%) reported decreased losses (Chart G). The increasing trend in the First District is greater than the 40% increase reported in the consolidated results. Among First District FIs reporting increased losses, four reported an increase over 10% higher than the previous year. Conversely, one FI reported lower losses claimed that losses decreased over 10%.

Chart G: Payment Fraud Losses in 2013 vs. 2012 (# of FI respondents)



Q22. For your organization, how has the percentage of financial losses due to payments fraud changed in 2013 compared to 2012?

Table 5: Percentage Change in Payment Fraud Losses (# of FI Respondents)

Percent Change	FIs (n=34)
Increased very substantially (more than 10%)	4
Increased substantially (up 5-10%)	8
Increased somewhat (up 1-5%)	6
Stayed the same	10
Decreased somewhat (down 1-5%)	2
Decreased substantially (down 5-10%)	0
Decreased very substantially (down 10% or more)	1
Don't know	3
Total	34

Q22. For your organization, how has the percentage of financial losses due to payments fraud changed in 2013 compared to 2012?

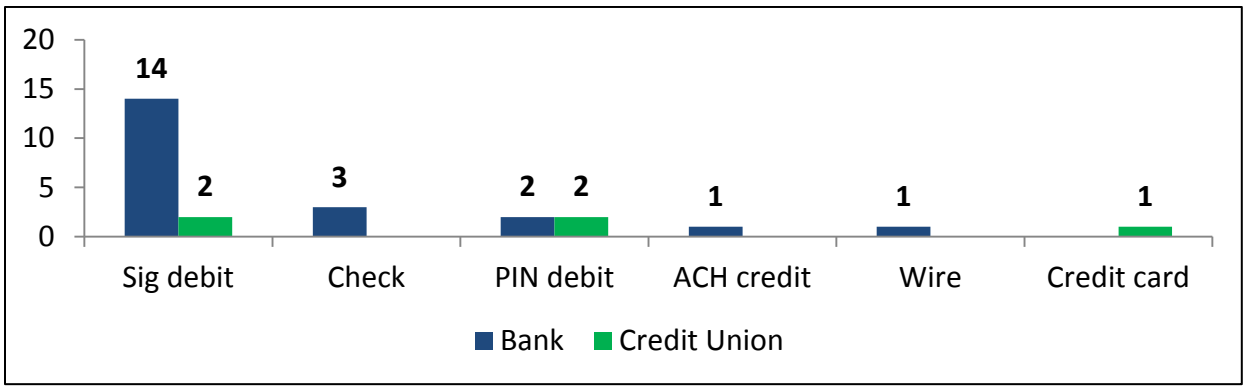
Six of the ten FIs with assets over $1 billion reported increased fraud losses in 2013. With more customers and transaction volume larger banks may be more attractive to fraudsters, although there is no data to explain this anomaly (Table 6). However, only 12 of 21 FIs with assets under $1 billion reported increased fraud losses in 2013.

Table 6: FI Fraud Losses by Asset Size (# of FI Respondents)

Fraud Losses	FIs with Asset > $1 B *(n=10)*		FIs with Asset < $1 B *(n=21)*	
	#	Percent	#	Percent
Increased	6	60%	12	32%
Decreased	1	10%	2	10%
Stay the same	3	30%	7	58%
FIs with losses less than or equal to 0.5% of revenue	8	80%	17	81%
FIs with losses over 0.5% of revenue	2	20%	4	19%

The primary payment methods that contributed to increased fraud losses were signature and PIN debit cards and checks, the same three categories recorded in 2012. Therefore, FIs should continue to focus their fraud prevention efforts on these three payment methods (Chart H). Nearly all FI respondents (16 of 18) attributed their increase in fraud losses to signature debit cards.

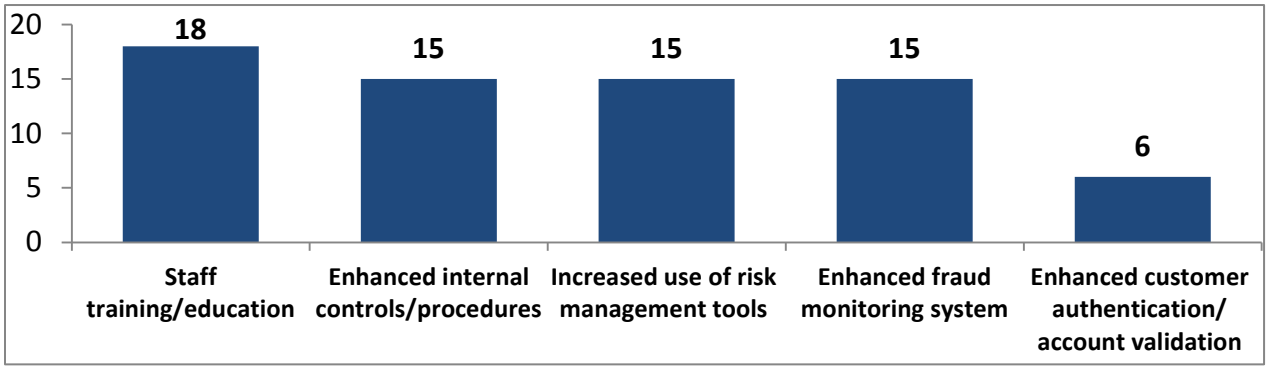
Chart H: Payment Instruments Attributed to Increase in Fraud Losses (# of FI respondents)



Q23. To which payment types do you attribute the 2013 increase in your organization's actual dollar losses? (Select all that apply.)

Only three FI respondents reported decreased fraud losses. Two of the FIs attributed the decrease to use of risk management tools, and one also implemented an enhanced fraud monitoring system for debit card transactions. While they did not experience a decrease in fraud losses, other FIs were asked if they had taken measures to help control their organization's payment fraud losses. Twenty-four FIs of varying asset sizes (more than $1billion: 8; $250 million to $999.99 million: 12; under $250 million: 4) reported making changes. The most common measures to help control fraud losses included staff training and education, risk management tools, enhanced internal procedures, and enhanced fraud monitoring systems for debit card, check, ACH, and wire transactions (Chart I).

Chart I. Key Measures to Help Control Payment Fraud Losses (# of FI respondents)



Q27A. Which of the following changes did your organization make that helped to control your organization's payments fraud losses? (Select all that apply.)

The implementation of EMV cards in the U.S. is expected to reduce some forms of debit and credit card fraud[6].

- For example, mandated by the major card networks to avoid a liability shift for fraudulent transactions effective in October 2014, the implementation of EMV chip cards and POS terminals in the U.S is underway. EMV should reduce fraud at the physical POS as evidenced by results in other countries.[7] An EMV card includes a secure microprocessor chip that can store information securely and perform cryptographic processing during a payment transaction. The card's security credentials or keys are encoded by the card issuers and stored securely in the card's chip, rendering them useless to unauthorized individuals attempting to access the credentials.

- EMV helps to prevent card skimming and card cloning, among the most frequent ways magnetic stripe cards are compromised and used for fraudulent activity. EMV transactions carry dynamic data, meaning that data cannot be used to initiate a fraudulent transaction.[8] In countries where EMV has been implemented, there has been a significant reduction in card-present fraud. According to a report by Discover Financial Services in 2013, since the European Union (EU) has migrated fully to EMV, the region has seen credit card fraud decrease by 80%, while the U.S. has seen an increase of 47%.[9]

- However, EMV will not mitigate online or card-not-present payment fraud using debit or credit cards because there is no physical connection between the card and a payment terminal or reader. In the United Kingdom (UK), which has implemented EMV since 2001 (although the liability shift did not occur until 2005), card not present (CNP) fraud increased from 54% of total fraud in 2007 to 63% of total fraud in 2012.[10]

---

[6] EMV stands for Europay, Mastercard and Visa – a global open-standard set of specifications for smart card payments and acceptance devices. The EMV specifications were developed to define a set of requirements to ensure interoperability between chip-based payment cards and terminals. EMV chip cards contain embedded microprocessors that provide strong transaction security features and other application capabilities not possible with traditional magnetic stripe cards. A white paper released by Gemalto noted that 99.99% of EMV cards produce safe face-to-face transactions, citing data received from Banque de France and the UK Cards Association http://www.gemalto.com/brochures-site/download-site/Documents/documentgating/fin_wp_Migration_to_EMV.pdf. For more information on the migration to EMV in the US, see: http://www.smartcardalliance.org/activities-emv-migration-forum/.

[7] 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.

[8] EMV security protocols are discussed on the Smart Card Alliance webpage. http://www.smartcardalliance.org/resources/pdf/EMV-FAQ-update-053014.pdf

[9] Taken from Gemalto's EMV information site http://www.thatsemv.com/stats/

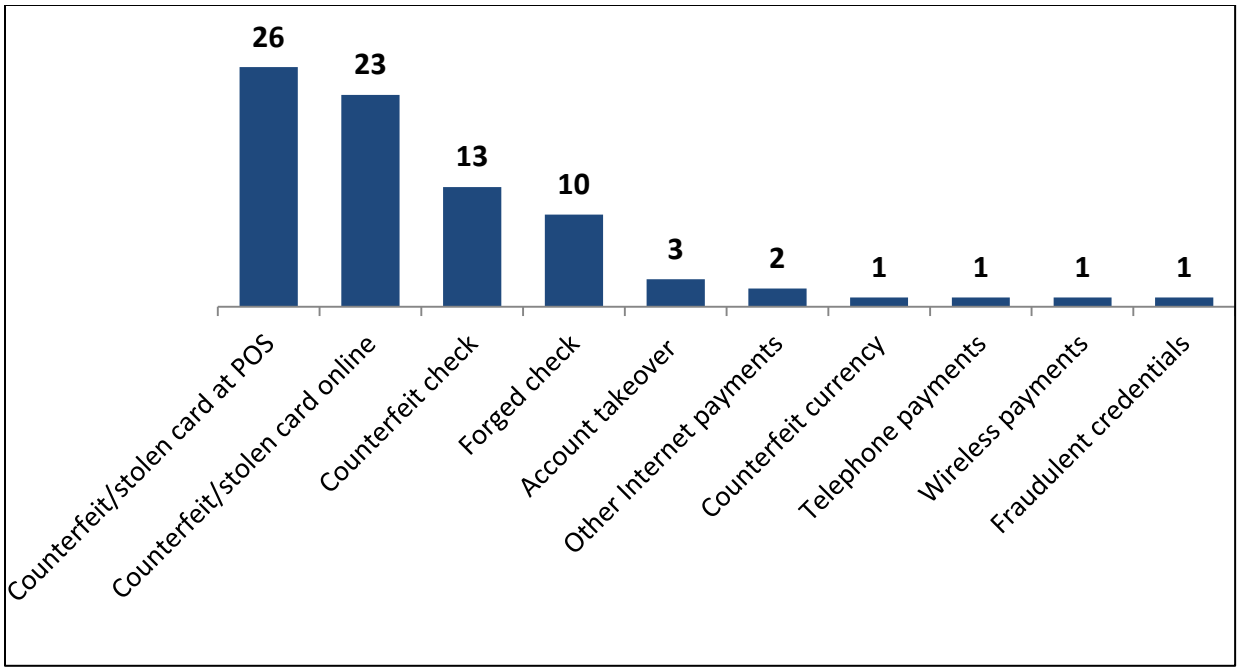
[10] http://www.theukcardsassociation.org.uk/plastic_fraud_figures/index.asp

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, 20 of the 22 respondents (FIs and non-FIs) that experienced successful payment fraud reported that 100% of their fraud came from external parties.

The top two fraud schemes against customer accounts related to card transactions, as reported in Chart J. Twenty-six of the 28 FIs had customers who experienced fraud from counterfeit or stolen cards used at point-of-sale (POS), and 23 respondents experienced fraud due to online use of counterfeit or stolen cards.

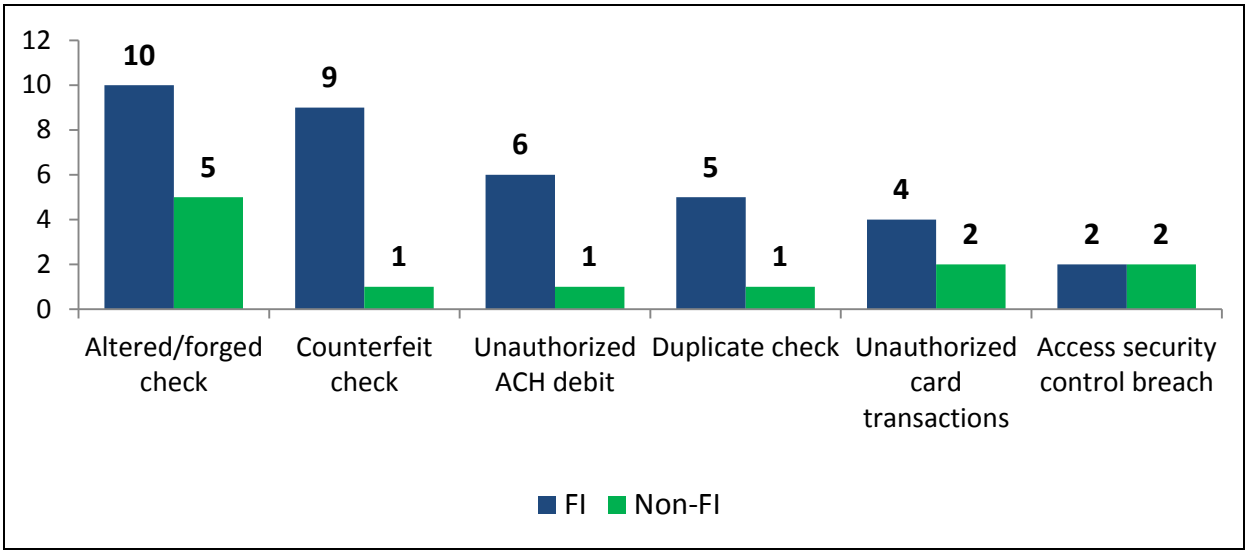
Chart J: Top Three Payment Fraud Schemes by or on behalf of FI Customers (# of FI respondents)



Q31. 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 and rank up to three that are most common.)

The two most common fraud schemes FIs experienced against their own accounts were check-related. More than half of FIs (10 out of 18) experienced fraudulent activities involving altered or forged checks and nine had counterfeit check fraud. Customer service centers or internal fraud schemes were not among the top three fraud schemes reported by any respondents

Chart K: Top Three Fraud Schemes Involving FI Accounts (# of FI respondents)



Q32. 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 and rank up to three that are most common.)

Fraudsters obtained most of the information used to initiate fraud schemes directly from consumers and physical device tampering. Controlling fraud at the consumer level is more difficult (Table 7) but education to increase consumer awareness of how to avoid payment fraud can help. Thirteen out of 29 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. Other sources of information 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. However, over one-third of the fraud sources were unknown, which is a concern for FIs trying to implement the most effective security systems.

Table 7: Information Sources Used in Fraud Schemes (# of FI Respondents)

Information Sources	FIs
"Sensitive" information obtained from lost or stolen card, check, or other physical document, mobile phone or other device while in consumer's control	13
Physical device tampering	13
Email and webpage cyber-attacks	10
Information sources are unknown	10
Data breach due to computer hacking,	8
Information about customer obtained by family or friend	6
Information obtained from a legitimate check issued by your organization	6
Social engineering used to obtain information used in the fraud scheme	5
Lost or stolen physical documentation or electronic PC/device while in control of your organization	0
Employee misuse	0

Q33. 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?

Payment Fraud Mitigation Strategies

Respondents were asked about their use and effectiveness of different types of fraud mitigation methods and tools in four areas: customer authentication methods; transaction screening and risk management methods; internal controls and procedures; and risk mitigation services offered by FIs.

Authentication Methods

Respondents were asked about 14 different customer authentication methods. The top authentication methods FI survey respondents used are multi-factor authentication (MFA), which was a new option in the 2014 survey, authentication for online transactions, mag stripe signature verification, and PIN authentication. FIs do not consider all of the methods to be equally effective. Nearly all First District respondents (29) reported that MFA, PIN authentication and authentication for online transactions are very or somewhat effective. In contrast, four FIs indicated that mag stripe signature verification was somewhat ineffective (Table 8).

The three least commonly used authentication methods reported were mag stripe/2D barcode for state ID (5 respondents), biometrics (1 respondent) and card chip authentication (0 respondent). However, 23 of 28 respondents plan to implement card chip authentication by 2016, most likely related to the card networks' EMV migration mandate. In 2012 only eight of the FIs planned to implement card chip authentication in the next two years. Looking at First District and consolidated results, the newer authentication technologies may be more effective, but are currently being used by only a small number of institutions.

Table 8: Use of Authentication Methods (# of FI Respondents)

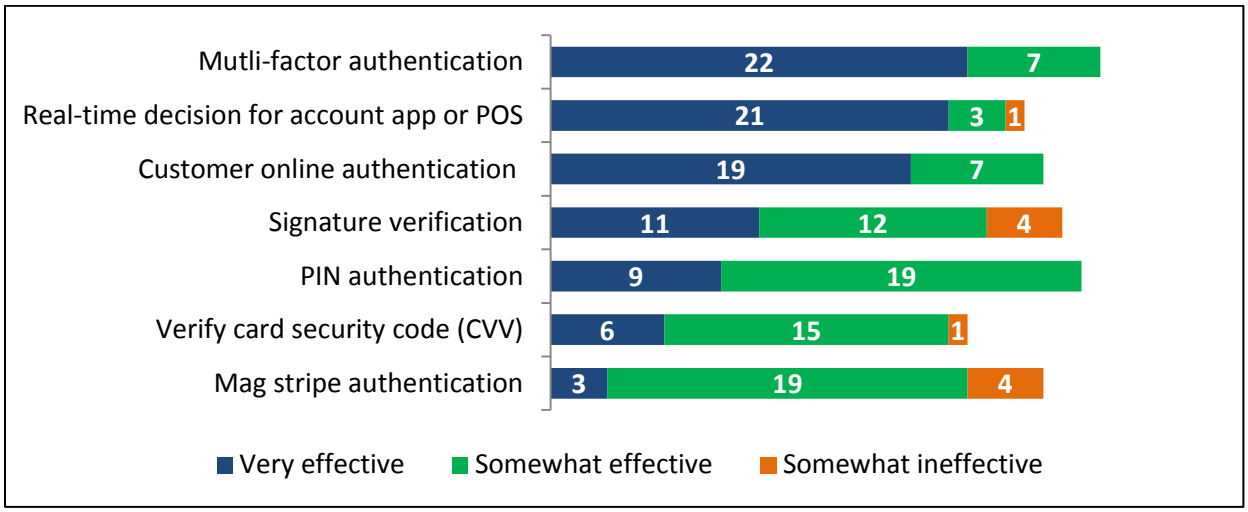
Authentication Method	Currently Use	Plan to Use	Don't Use
Multi-factor authentication	30	1	1
Customer online authentication	29	0	2
PIN authentication	29	0	3
Mag stripe authentication	28	0	2
Signature verification	28	0	3
Real-time decision for account app or POS	25	2	3
Verify card security code (CVV)	23	1	6
Out-of-band authentication	18	3	9
Purchaser ID or valid account POS	14	1	14
Physical token	12	3	14
Mobile device authentication	11	4	15
Verify customer ID with mag stripe/2D barcode	8	3	19
Biometrics	1	2	26
EMV chip card	0	23	5

Q34. Which of the following authentication methods does your organization currently use or plan to use to mitigate payment risk?

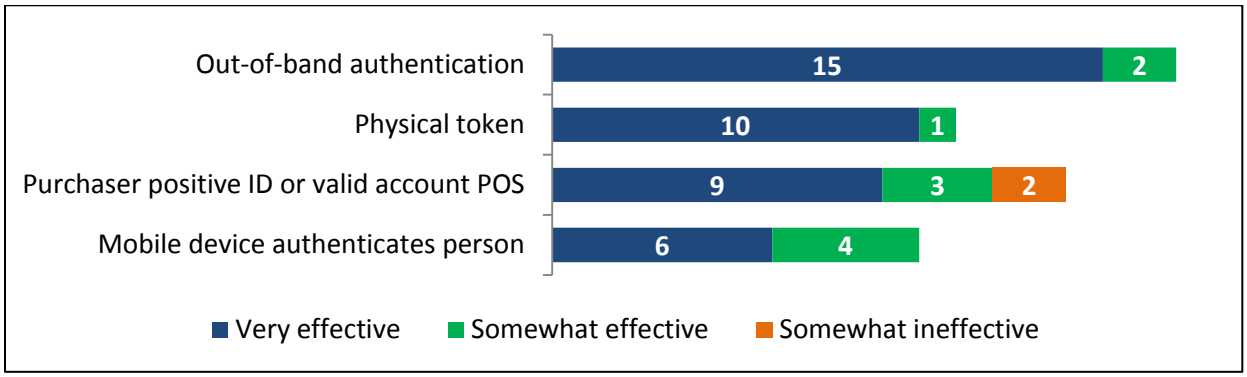
Chart L: Effectiveness of Authentication Methods (# of FI Respondents)

Chart L has been split into three sections to show the number of FI Respondents by size of group from Table 8 who use the selected methods.

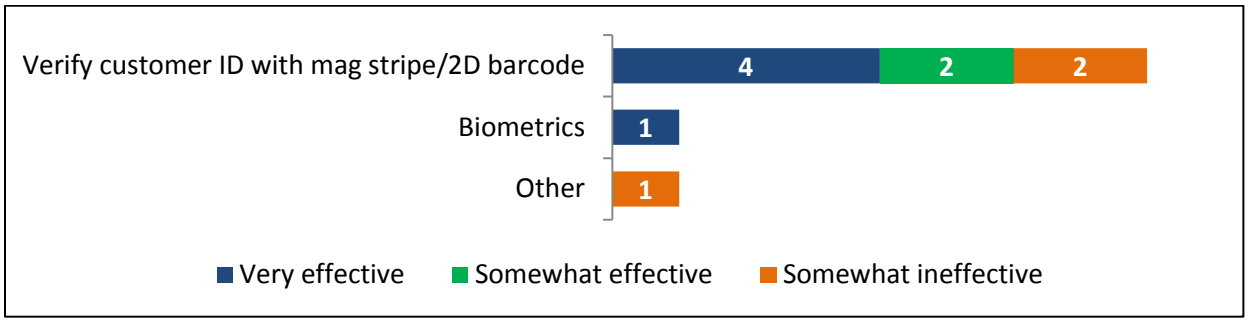
Effectiveness of Authentication Methods used by 20 or more Respondents



Effectiveness of Authentication Methods used by 10 – 19 respondents



Effectiveness of Authentication Methods used by less than 10 Respondents



Q35. Please rate the effectiveness of authentication methods currently used by your organization.

Transaction Screening and Risk Management Methods

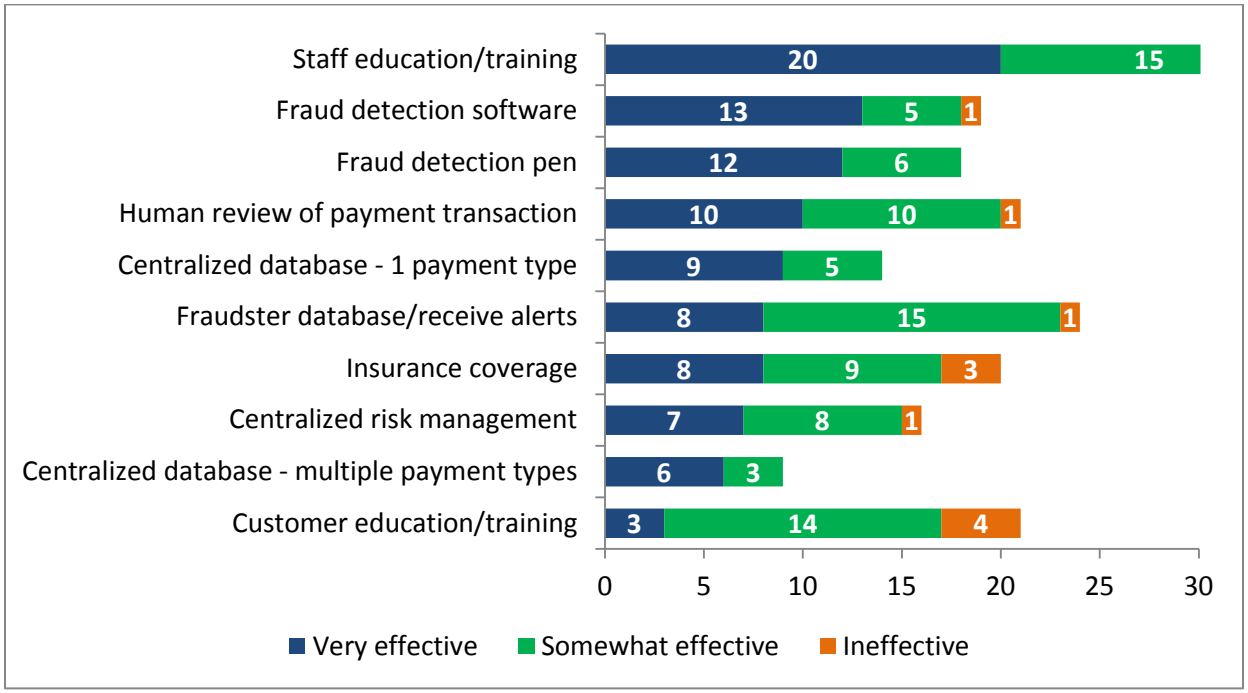
Table 9 and Chart M summarize the primary transaction screening and risk management methods that FIs have implemented or plan to implement for various payment methods. Educating staff and participating in receipt of alerts from a fraudster database are the most commonly used methods (25 and 24 FIs respectively). Customer education, human review of transactions and purchasing insurance coverage have similar adoption rates, with 21 respondents for the first two methods and 20 for the third. FIs consider most of the methods either very effective or somewhat effective. However, only three of the 21 respondents that use customer education to address payment fraud risk rated it very effective, which may indicate that FIs feel that fraud tools, such as fraud detection software (68% very effective), work better than consumer education to mitigate fraud. However, customer education used to supplement fraud tools can be effective.

Table 9: Respondents Using Transaction Screening and Risk Management Methods (# of FI Respondents)

Transaction Screening and Risk Management Methods	Currently Use	Plan to Use	Don't Use
Staff education/training	25	2	1
Fraudster database/receive alerts	24	0	3
Customer education/training	21	4	3
Human review of payment transaction	21	0	6
Insurance coverage	20	1	5
Fraud detection software	19	5	3
Fraud detection pen	18	0	7
Central risk management	16	0	10
Centralized database – 1 payment type	14	3	9
Centralized database – multiple payment types	9	4	13

Q36. Which of the following transaction screening and risk management methods does your organization currently use or plan to use to mitigate payment risk?

Chart M: Effectiveness of Transaction Screening and Risk Management (# of FI Respondents)



Q37. Please rate the effectiveness of the transaction screening and risk management methods currently used by your organization.

Internal Controls and Procedures

The "fraud triangle" comprises three factors: incentive, rationalization, and opportunity. Strong and effective internal controls and procedures are essential for effective fraud prevention, especially to mitigate internal fraud. In relation to a recent data breach, the company had the required software to prevent it; however the staff who managed the software was not able to determine timely that it had detected a breach. While such companies invest in the necessary software to prevent breaches, providing staff education and ensuring ongoing review and audit of the controls in place is essential to mitigate risk.

Internal control procedures have a much higher overall adoption rate compared to authentication and transaction screening and risk management methods (Table 10 and Chart N). Some procedures are required by regulation or corporate policies. Of the possible internal control methods, all respondents use three methods: periodic internal/external audits; verify application controls via audit or management review; and address exception items timely. Furthermore, between 26 and 28 respondents use the same nine methods. This would indicate that implementing multiple internal controls is helpful, and controls tend to be consistent among FIs of all sizes. "Use of personal devices to process an organization's payment transactions with specific controls" and "dedicated computers to conduct transactions" had the lowest adoption rates (approximately 18 and 24 FIs respectively, do not implement these

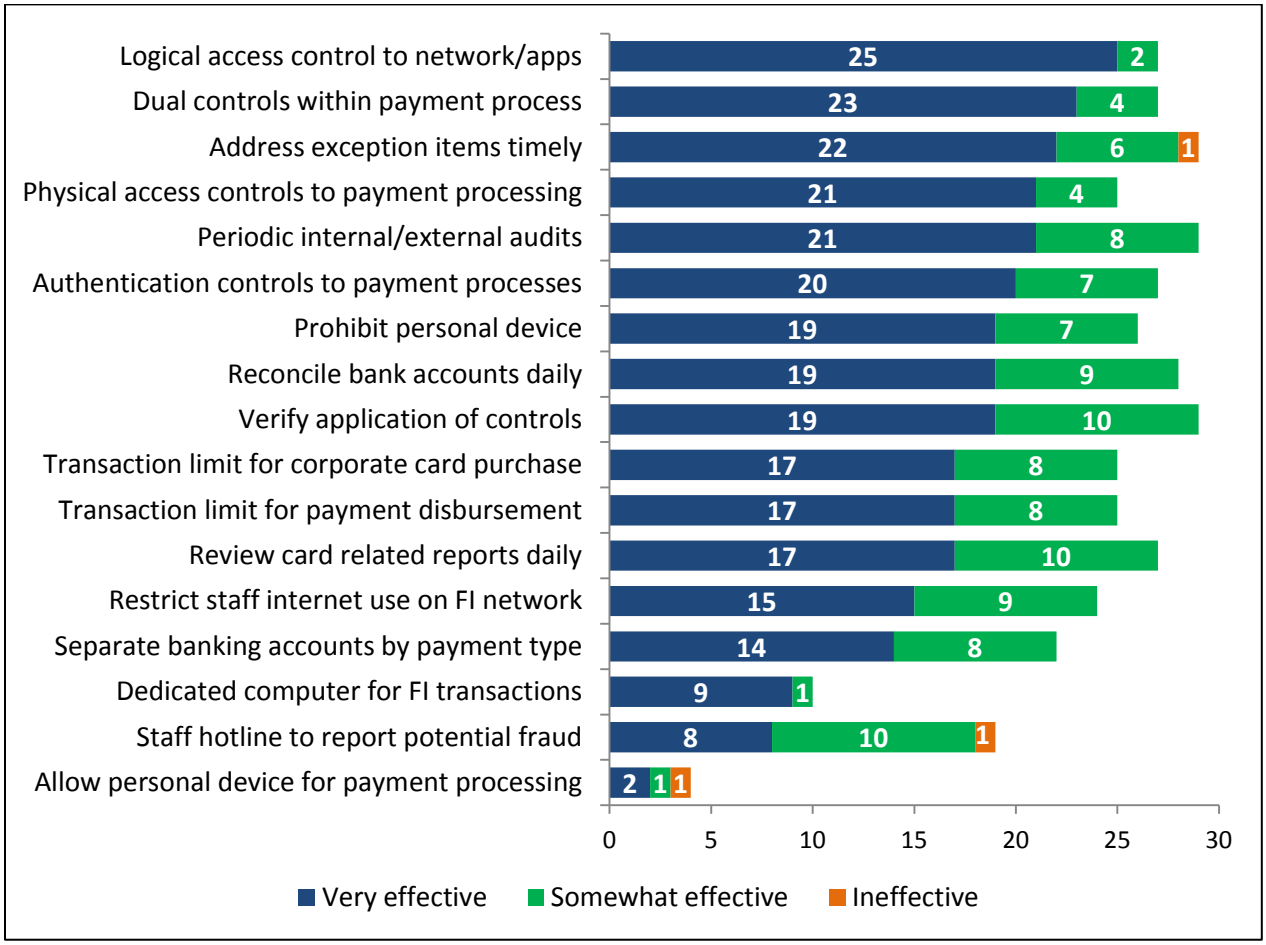
methods). Employee use of personal devices, often referred to as Bring Your Own Device (BYOD), has both the lowest use and the second highest ineffective rating. Allowing a BYOD policy requires a higher level of security, as the organization's control of personal devices on the network is lessened. Providing dedicated computers requires investment in new hardware and software, so budget constraints or resource issues could also be a barrier.

Table 10: Respondents Using Internal Control Methods (# of FI respondents)

Internal Control Methods	Currently Use	Plan to Use	Don't Use
Periodic internal/external audits	29	0	0
Verify controls via audit/management review	29	0	0
Address exception items timely	29	0	0
Reconcile bank accounts daily	28	0	1
Review card related reports daily	27	0	1
Logical access control to network/ apps	27	0	1
Dual control within payment process	27	0	2
Authentication controls to payment process	27	0	2
Prohibit personal device	26	0	3
Transaction limit for payment disbursement	26	0	3
Transaction limit for corporate card purchase	25	0	3
Physical access controls to payment processing	25	0	3
Restrict staff Internet use on FI network	24	2	2
Separate banking accounts by payment type	23	0	4
Staff hotline to report potential fraud	19	0	8
Dedicated computer for FI transactions	10	0	18
Allow personal device for payment processing	3	0	24

Q38. Which of the following internal controls and procedures does your organization currently use or plan to use?

Chart N: Effectiveness of Internal Control Methods (# of FI Respondents)



Q39. Please rate the effectiveness of the internal controls and procedures currently used by your organization.

Risk Mitigation Services Offered by FIs

Table 11 lists the risk mitigation services that FIs provide to their business customers. The most commonly provided tools are online information services and 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 is a security process that requires at least two forms of authentication to verify the legitimacy of a transaction. MFA combines what a customer knows (e.g., password or PIN) along with something you have (e.g., a mobile phone or smart card) or something you are (e.g., biometrics).

Table 11: Risk Mitigation Services Offered by FIs (# of FI Respondents)

Risk Mitigation Services	Currently Use	Plan to Use	Don't Use
Online information	26	0	1
MFA initiate payment from bank account	24	0	3
Account alert	16	2	9
Account masking	15	0	11
Payment fraud prevention training	15	3	9
ACH debit block	12	3	11
Commercial card alert	11	4	12
Fraud loss prevention	10	1	15
ACH debit filter	8	4	14
Customer card activation/deactivation	7	4	16
Check positive pay/reverse positive pay	7	6	14
ACH payee positive pay	6	6	13
Post no check	6	1	18
Check payee positive pay	6	5	15
ACH positive pay	6	7	14
Tokenization of sensitive information	5	3	19

Q42. What risk mitigation services/products does your organization currently offer or plan to offer to your business customers?

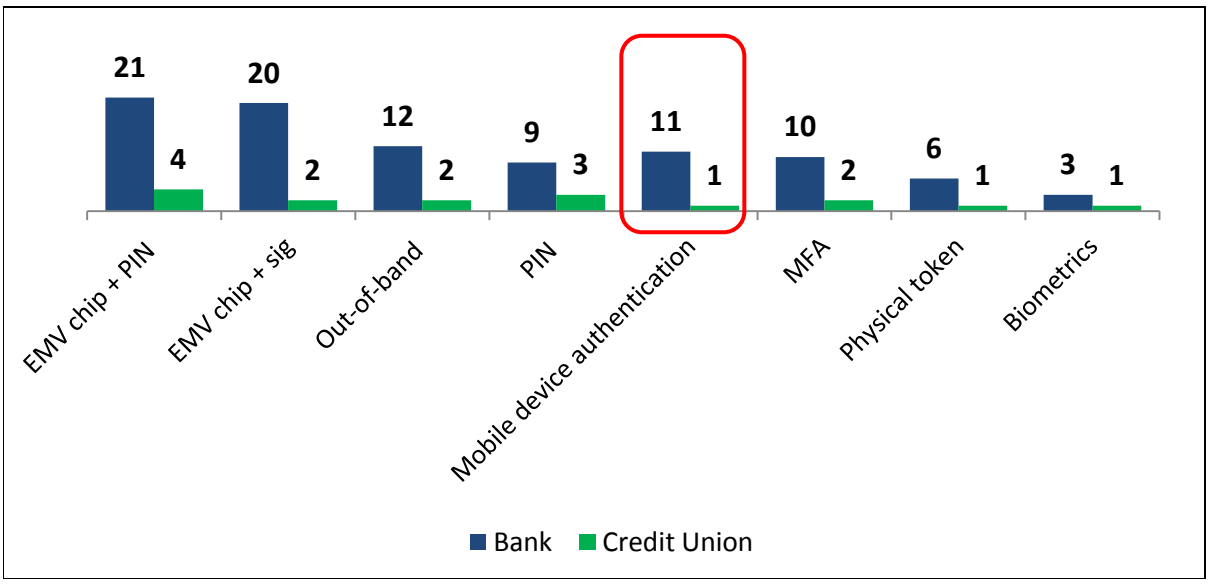
More FIs are adopting MFA to secure transactions. According to SafeNet's Global Authentication Survey, 37% of all organizations currently use MFA for their employees, and this is expected to reach 56% by 2016.[11] MFA can be achieved through different channels. For example, a smartphone can be used as another layer of authentication. Mobile authentication is gradually gaining traction into mainstream authentication and there are several different methods and technologies available in order to authenticate users with a mobile phone. These range from simple methods, such as sending one-time

[11] http://www.safenet-inc.com/news/2014/authentication-survey-2014-reveals-more-enterprises-adopting-multi-factor-authentication/#_ftn2.

passwords via text to the phone or sending a push notification to more complex forms including biometrics which is already being used on some mobile phones, such as the Samsung Galaxy S5 and the iPhone 5s. PayPal is currently testing using fingerprints for authentication with the Galaxy S5 mobile phone.[12]

Our survey results indicated a relatively low level of willingness among FI respondents to adopt mobile devices for authentication, compared to other methods (Chart O). This may be an area where further education could motivate FIs to consider using mobile phones to improve security. However, adoption of mobile devices for authentication has risen in the rankings relative to other methods since 2012, which is a positive sign for the industry. According to PayPal and the National Cyber Security Alliance, 53% of Americans are prepared to abandon passwords in exchange for new technologies such as biometrics,[13] as are 79% of British adults surveyed by Intelligent Environments.[14] Multi-factor authentication is an effective method to provide secure access to employees from remote locations. Overall, MFA helps to reduce any potential for a breach in security.

Chart O: Adoption Preferences of Authentication Methods (# of FI Respondents)



Q47. What authentication methods would your organization prefer or consider adopting to help reduce payments fraud? (Select all methods preferred or considered.)

[12] According to Gartner, 30% of organizations will use biometrics for authentication for mobile devices by 2016. http://www.gartner.com/newsroom/id/2661115. The use of biometrics for authentication is partly being driven through the FIDO Alliance. https://fidoalliance.org/.

[13] http://staysafeonline.org/download/datasets/7351/2013%20NCSA%20Online%20Safety%20Study%20Fact%20Sheet.pdf

[14] Intelligent Environments surveyed 2000 individuals as part of their research into biometric security measures. http://www.finextra.com/news/fullstory.aspx?newsitemid=26308

"Tokenization of sensitive information" is a new option that was added to Question 42 in the 2014 survey. EMVCo defines tokenization as a process by which the primary account number (PAN) is replaced with a surrogate value called a *payment token*. Tokenization may be used to enhance transaction efficiency, improve transaction security, increase service transparency, or to provide a method for third-party enablement.[15] Though tokenization has been around for many years, it has only been the past couple of years which has seen a high uptake and interest from the banking industry. This may be due to the rise of CNP transactions, which can be made more secure through the use of tokens.[16]
Tokenization offers many benefits.[17] In the New England FI survey, eight respondents reported using or planning to use tokenization as part of their risk mitigation strategy. All respondents were banks of various asset sizes.

First District FIs were asked to identify new security methods needed to reduce payments fraud, as indicated in Table 12. Replacement of mag stripe technology was the top choice, selected by 26 of the 30 respondents. This requires migration to new cards with EMV chip technology, as described earlier in the report. Initially, many FIs were hesitant to commit to EMV when the major card networks first announced their EMV migration plans for the U.S. However, FI attitudes have changed in light of recent data breaches. Research from Pulse found that 86% of U.S. financial institutions plan to begin issuing EMV chip cards within the next two years. Furthermore, a group of nine Payments Security Task Force (PSTF) members—Bank of America, Capital One, Chase, Citi, Discover, ICBA, Navy Federal Credit Union, US Bank and Wells Fargo—forecast that half of their cards, (about 575 million), will be chip-enabled by the end of 2015. And according to a MasterCard survey, 57% of consumers indicated they would be interested in receiving their (EMV) card in the next 6 months.[18]

First District FIs identified authentication controls over Internet- and mobile device-initiated payments as the second and third most needed security methods respectively. Online payment fraud will not be mitigated by replacing mag-stripe cards with chip cards. Consumer education is still considered an important fraud prevention measure as well, with over half of FI respondents (16 of 30) selecting it. Non-FI respondents focused more on needing improved methods to share information about emerging fraud

[15] http://www.emvco.com/specifications.aspx?id=263
[16] Based on experience in other countries, once EMV migration occurs, hackers will begin to target CNP transactions.Tokenization will help protect against this. Recent data breaches have highlighted the risks of storing sensitive payment data at POS. While EMV will greatly reduce fraud at POS, tokenization further secures the data and removes responsibility from the individual merchants. See http://www.networkworld.com/article/2597398/tech-primers/tokenization-is-the-way-to-prevent-e-commerce-security-breaches.html.
[17] See http://www.bostonfed.org/bankinfo/payment-strategies/publications/2014/summary-of-mpiw-meeting-june-2014.htm.
[18] http://www.pymnts.com/company-spotlight/2014/why-u-s-consumers-are-itching-for-emv-cards/

and image survivable check security features for business checks to reduce fraud. Three of the seven non-FIs indicated that replacement of card magnetic stripe technology is also essential to reducing payments fraud.

Table 12: New Methods to Decrease Fraud

New Methods Needed	All FIs (*n=30*)	Non-FIs (*n=7*)
Replacement of card magnetic stripe technology	26	3
Authentication controls over Internet initiated payments	20	2
Authentication controls over mobile device initiated payments	16	1
Consumer education on fraud prevention	16	1
More aggressive law enforcement	15	2
Improved methods for information sharing on emerging fraud	10	4
Industry alert services	10	2
Tokenization of sensitive information	7	1
Industry specific education on payments fraud prevention best practices	5	2
Image survivable check security features for business checks	4	4
Other	1	1

Q46. From your organization's perspective, what new or improved methods are most needed to reduce payments fraud?

4. Barriers to Reducing Payments Fraud

FIs identified lack of staff resources as the top barrier to mitigating fraud (Table13). Since most respondents are relatively small FIs, they may lack the financial capability to dedicate special resources to managing fraud prevention and detection. The barriers are similar for both FIs and non-FIs. Only four non-FIs responded to this question with two identifying lack of staff resources and two identifying cost of implementing fraud detection tools as the top barriers to mitigating fraud.

Table 13: Main Barriers to Payments Fraud Mitigation

Barriers	# FIs (*n=26*)	# Non-FIs (*n=4*)
Lack of staff resources	13	2
Cost of implementing commercially available fraud detection tool	9	2
Unable to combine payment information for review due to operating w/ multiple business areas, states, or banks	9	1
Lack of compelling business case (cost vs. benefit) to adopt new or change existing methods	9	0
Consumer data privacy issues/concerns	9	0
Corporate reluctance to share info due to competitive issues	4	1
Cost of implementing in-house fraud detection tool/method	3	0
Other	3	0

Q48. What are the main barriers to mitigate payments fraud that your organization experiences?

5. Legal and Regulatory Considerations

Table 14 summarizes responses regarding legal and regulatory changes that could help reduce payments fraud. Highlighted changes reflect the top three actions selected by respondents in the First District and in the consolidated FI results to help reduce payments fraud. The three options 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 19 FIs in the First District.

It is interesting to note the importance non-FIs place on "Improve law enforcement cooperation on domestic and international payments fraud and fraud rings." It was selected by five of the eight non-FI respondents. It appears that non-FI respondents prefer authorities take a harder line and increase penalties against those who commit fraud, with half indicating "strengthen disincentives for committing fraud" as a legal change that would help reduce payments fraud.

Table 14: Legal and Regulatory Considerations (# of Respondents)

Legal and Regulatory Changes	First District FIs *n=30*	Consolidated FI Results *n=292*	First District Non-FIs *n=8*
Assign liability for fraud losses to the party most responsible for not acting to reduce the risk of payment fraud	23	189	3
Place responsibility to mitigate fraud and shift liability for fraudulent card payments to the entity that initially accepts the card payment	20	214	2
Place more responsibility on consumers and customers to reconcile and protect their payments data	19	210	2
Focus future legal or regulatory changes on data breaches to where the breaches occur	18	136	3
Align Regulation E and Regulation CC to reflect changes in check collection systems' use of check images and conversion of checks to ACH transactions	17	118	2
Strengthen disincentives to committing fraud through more likely prosecution and increased penalties for fraud and attempted fraud	16	175	4
Improve law enforcement cooperation on domestic and international payments fraud and fraud rings	13	146	5
Assign responsibility for mitigating fraud risk to the party best positioned to take action against fraud	11	116	3
Establish new laws/regulations to require data sharing to strengthen the management of payments fraud risk	9	63	2
Establish new laws/regulations or change existing ones in order to strengthen the management of payments fraud risk	8	80	2
Other	2	6	0

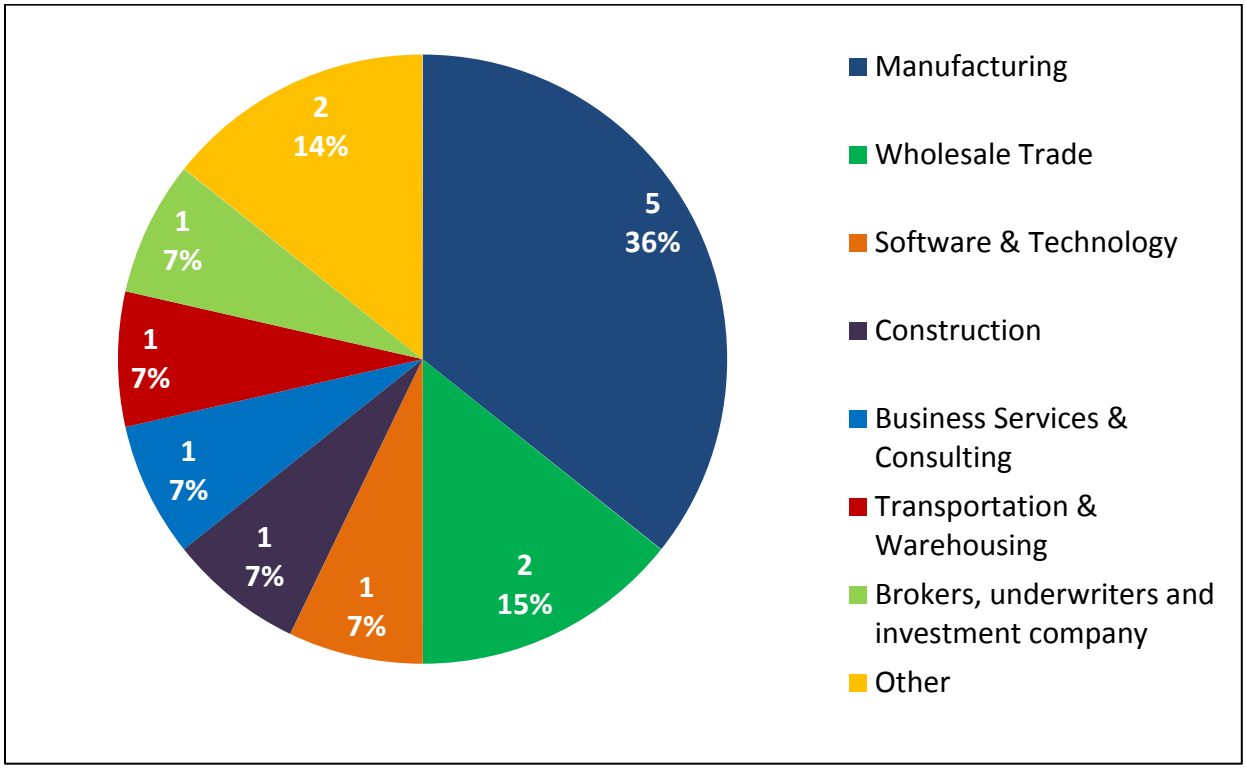
Q49. Please indicate what types of legal or regulatory changes you think would help reduce payments fraud. (Select all that apply.)

6. Non-FIs

Respondent Profile

Fourteen non-financial institutions (non-FIs) responded to the 2014 survey, which is the first time the First District received any non-FI responses. Chart P shows the breakdown by industry sector. Non-FIs represent 29% of the total survey respondents. Seven of the non-FI respondents reported revenues of $100-500M and five reported revenues of $500M or more.

Chart P: Company Sector

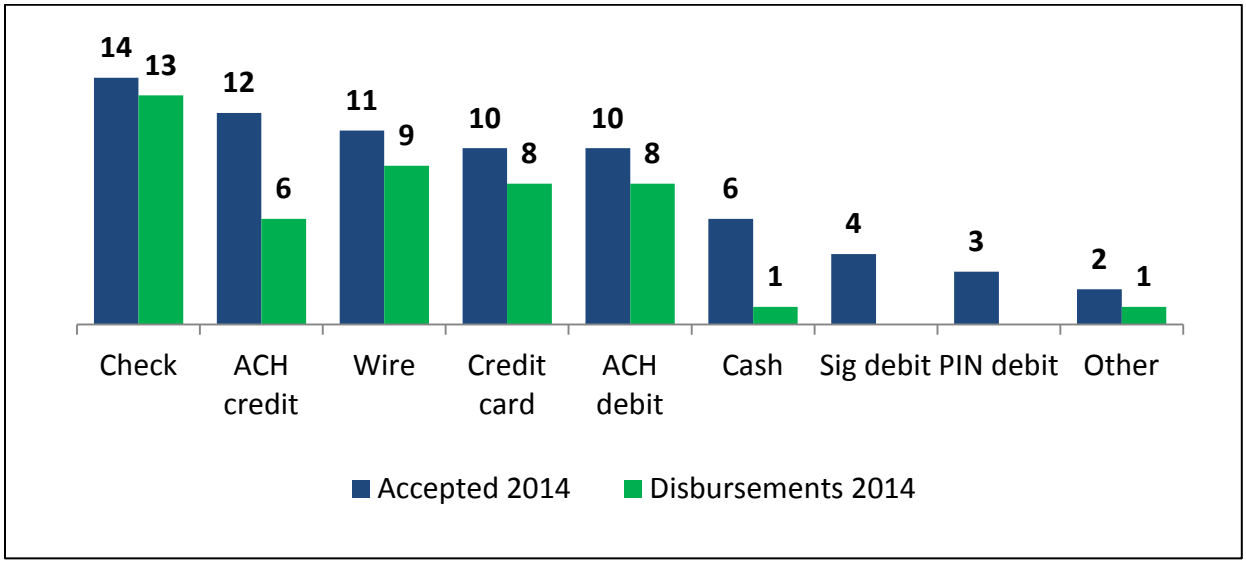


Q1a. How do you classify your organization?

Payment Products Accepted and Disbursed by Non-FIs in New England

Chart Q displays the methods that non-FIs in the First District accept and use to disburse payments. All respondents accept and disburse checks. Interestingly, none of the respondents use debit cards to make payments, while only one respondent uses cash. None of the respondents use prepaid cards.

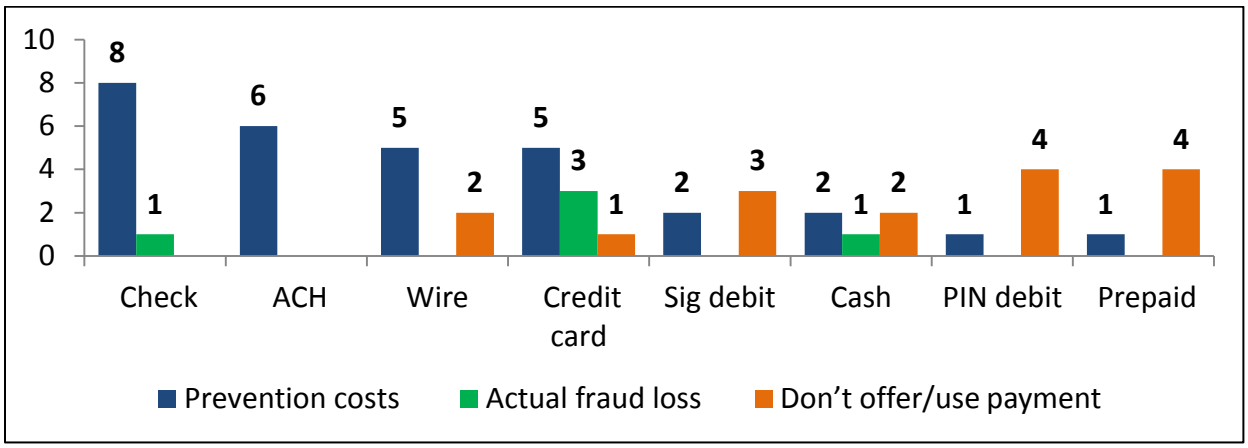
Chart Q: Payment Products and Services Non-FIs Accept and Disburse (# of Non-FI respondents)



Q10. What types of payments does your organization accept?
Q11. What types of payments does your organization use to disburse payments?

Only seven non-FI respondents experienced payment fraud attempts in 2014. Four non-FIs indicated the highest number of fraud attempts on credit cards and checks, while one reported the highest number of fraud attemps on wire. Only one non-FI experienced actual dollar losses due to fraud, specifically check fraud, and the loss amounted to less than 0.3% of annual revenue. There are three payment types where at least one non-FI reported actual fraud losses exceeding prevention costs – check, credit card and cash (see green bars in Chart R).

Chart R: Fraud Prevention Costs vs Actual Dollar Fraud Losses (# of Non-FI respondents)



Q16. For these payment types, which is a greater expense for your organization– fraud prevention costs or actual dollar losses?

Payments made using counterfeit checks was the top fraud scheme for non-FI respondents, reported by 4 out of 6 respondents. Payments with altered or forged checks and counterfeit or stolen cards at POS were the second and third most common fraud schemes; each reported by two non-FIs. Counterfeit or stolen cards used online, use of fraudulent credentials/data and cash register frauds were each selected by one non-FI.

Three non-FIs reported that fraudsters obtained most of the information used to initiate fraud schemes from unknown sources and from the legitimate checks issued by that organization. Social engineering was the second most-common source of information in fraud schemes as indicated by 2 of the 7 respondents.

Table 15: Information Sources Used in Fraud Schemes (# of Non-FI Respondents)

Information Sources	**All Non-FIs** *n=7*
Unknown	3
Information obtained from a legitimate check issued by your organization	3
Social engineering	2
"Sensitive" information obtained from lost or stolen card, check, or other physical document or device while in consumer's control	1
Information about customer obtained by family or friend	1
Employee with legitimate access to organization or customer information (employee misuse)	1
Lost or stolen physical documentation or electronic devices while in control of the organization	1

Q33. 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?

Payment Fraud Mitigation Strategies

For non-FIs, "verify CVV codes on the payment card" is the most used authentication method (used by 6) followed by token authentication (used by 4). One non-FI reported plans to implement each of the following authentication methods: PIN, card chip (EMV) and mag-stripe signature verification and another respondent uses "validate ship to info."

Non-FIs currently using PIN authentication, verify customer ID is authentic, real time decision support, and positive ID of purchaser indicated that these authentication methods were *very effective*.

Table 16: Use of Authentication Methods (# of Non-FI Respondents)

Authentication Method	Currently Use	Plan to Use	Don't Use
Verify card security code (CVV)	6	0	3
Physical token	4	0	4
Customer authentication online transaction	3	0	5
PIN authentication	2	1	3
Real-time decision for account app or POS	2	0	5
Verify customer ID with mag strip/2D barcode	1	0	5
Purchaser positive ID or valid account POS	1	0	5
Mag stripe authentication	0	1	5
EMV chip card	0	1	5

Q34. Which of the following authentication methods does your organization currently use or plan to use to mitigate payment risk?

Table 17 summarizes the main transaction screening and risk management methods that non-FIs have implemented or plan to implement. Nine respondents currently use human review of payment transactions. Very few non-FI respondents currently use other transaction screening methods to mitigate payment risk.

Table 17: Use of Transaction Screening and Risk Management (*# of Non-FI Respondents*)

Transaction Screening and Risk Management Methods	Currently Use	Plan to Use	Don't Use
Human review of payment transaction	9	0	0
Central risk management	3	0	3
Insurance coverage	2	1	5
Fraud detection software	2	0	6
Fraud detection pen	2	0	5
Staff education/training	1	1	4
Customer education/training	1	1	4
Fraudster database/receive alerts	1	0	6
Centralized database – multiple payment types	1	0	6

Q36. Which of the following transaction screening and risk management methods does your organization currently use or plan to use to mitigate payment risk?

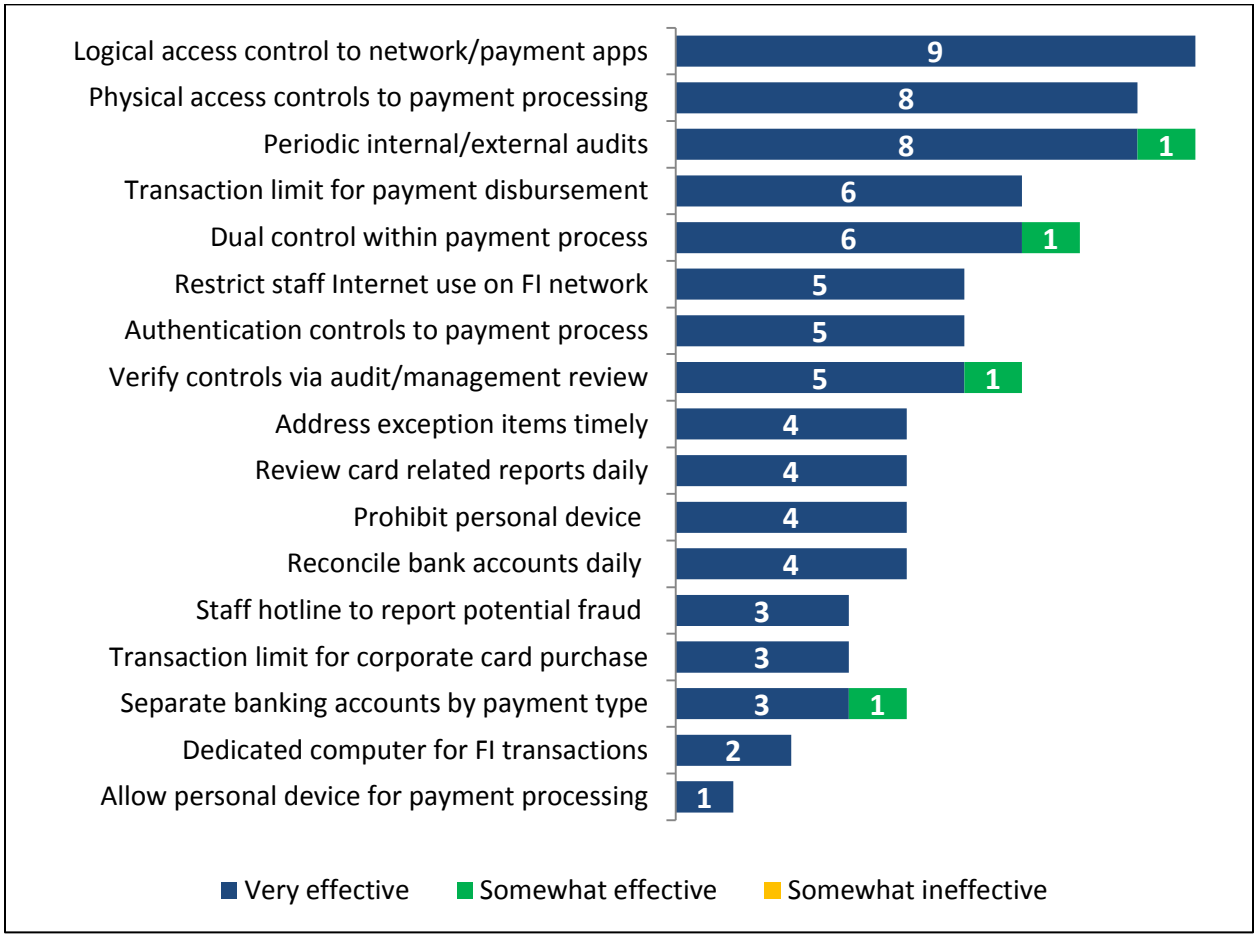
Strong and effective internal controls and procedures are essential for effective fraud prevention. As was the case for FIs, there is a much higher adoption rate of internal fraud controls for non-FIs (Table 18). Periodic internal/external audits and logical access controls to network payments apps are the most commonly used methods, with 9 respondents using this method. Similar to FIs, a dedicated computer to conduct transactions with an FI and the use of personal devices for transactions are the least used.

Table 18: Use of Internal Control Methods (*# of Non-FI Respondents*)

Internal Control Methods	Currently Use	Plan to Use	Don't Use
Periodic internal/external audits	9	0	1
Logical access control to network/apps	9	0	1
Physical access controls to payment processing	8	0	2
Dual control within payment process	7	0	2
Authentication controls to payment process	6	0	4
Verify controls via audit/management review	6	0	2
Transaction limit for corporate card purchase	6	0	2
Restrict staff internet use on FI network	5	0	3
Reconcile bank accounts daily	4	1	3
Review card related reports daily	4	1	3
Address exception items timely	4	0	4
Transaction limit for payment disbursement	4	0	4
Prohibit personal device	4	0	3
Separate banking accounts by payment type	4	0	2
Staff hotline to report potential fraud	3	0	4
Dedicated computer for FI transactions	2	1	5
Allow personal device for payment processing	1	0	4

Q38. Which of the following internal controls and procedures does your organization currently use or plan to use?

Chart S: Effectiveness of Internal Control Methods (*#of non-FI Respondents*)



Q39. Please rate the effectiveness of the internal controls and procedures currently used by your organization

7. Conclusions

Overall, the 2014 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 continue to be the payment instruments most vulnerable to fraud attempts and losses.

- More than half of FIs reported that signature debit card losses from fraud exceeded their investment in mitigation methods to prevent such fraud. This seems to suggest a cost-effective opportunity to increase related fraud prevention investments to reduce actual debit card losses.

- Most FIs reported very low fraud losses as a percentage of annual revenue, showing that good controls are effective at mitigating fraud.

- Strategies to detect and prevent fraud effectively require the use of multiple mitigation methods and tools. No one method can address everything. Most FIs primarily use internal controls and procedures to mitigate fraud. 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.

- Three 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.

- Twenty-six FI and three non-FI respondents indicated the need for alternatives to mag-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: 2014 Payments Fraud Questionnaire

Federal Reserve Bank of Boston, Chicago, Dallas, Minneapolis and Richmond
Payments Fraud Questionnaire 2014

The survey will be administered online. Question numbers will not show. Information in blue font represents logic in the survey tool and is not displayed. Bullet formatting – if bullet is a circle, then it represents a radio button and limits selection to one answer. If bullets are squares, this means the respondent may select more than one answer.

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 as best you can. If you are unsure, please provide your best estimate.
- The survey should take about 20 - 30 minutes to complete. To review the questions in advance of completing the 2014 survey; see http://www.minneapolisfed.org/about/whatwedo/paymentsinformation.cfm
- It is best if you do not exit the survey until all questions have been completed. If needed, to return to the survey use the "Save" button 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 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, Dallas, Minneapolis and Richmond.

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

Organization Profile:

1a. How do you classify your organization? (Please select one answer.) A response to this question is required. List in alpha order.

- Agriculture
- Brokers, underwriters and investment company
- Business services/Consulting
- Construction
- Educational services
- Energy
- Financial Institution or Service Provider (If selected, go to 1b.)
- Government
- Health services
- Hospitality/Travel
- Insurance company and pension funds
- Manufacturing
- Nonprofit
- Real estate/Rental/Leasing
- Retail trade
- Software/Technology
- Telecommunications
- Transportation/Warehousing
- Wholesale trade
- Other, please specify _____

Ask 1b when organization selected Financial Institution or Service Provider.

1b. Please select the type of financial services organization from the list below. A response to this question is required.

- Bank respondents selecting *Bank* will be asked "FI" questions
- Credit Union respondents selecting *Credit Union* will be asked "FI" questions
- Thrift respondents selecting *Thrift* will be asked "FI" questions
- Service Provider, e.g., payments processor respondents selecting *service provider* will be asked select FI questions where indicated

2. What is your … Only ask Q2 when answer to Q1 is financial institution (Bank, Credit Union, Thrift) and go to Q4 next.
   Financial institution name _____
   City/Town ___ _____
   State Provide drop down list of 50 states in alpha order, also include District of Columbia.
   ZIP/Postal Code _ _ _ _ _ Limited to 5 digits
   Main nine digit routing and transit number. (Please specify the head office number.)
   _ _ _ _ - _ _ _ _ - _ Response must be numeric.

3. What is your… Skip Q3 when answer to Q1 is financial institution (Bank, Credit Union, Thrift).
   Company Name: _____
   City/Town: _____
   State Provide drop down list of 50 states in alpha order, also include District of Columbia.
   ZIP/Postal Code _ _ _ _ _ Limited to 5 digits

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.)
   - Accounts payable or receivable
   - Audit
   - Compliance/Risk Management/ Fraud Management
   - Finance
   - Operations/Payments processing function
   - Management over multiple departments
   - Treasury
   - Other, please specify _____

6. What do you estimate are your organization's 2013 annual revenues? (If you don't know, please provide your best estimate.)
   - Under $10 million
   - $10 million to $24.9 million
   - $25 million to $49.9 million
   - $50 – 99.9 million
   - $100 – 249.9 million
   - $250 - 499.9 million
   - $500 - 999.9 million
   - $1 – 4.9 billion
   - $5 – 9.9 billion
   - $10 billion or more
   - Not applicable

7. What is the size of your financial institution based on year-end 2013 total assets? (If you don't know, please provide your best estimate.) Only ask Q7 when answer to Q1 is financial institution (Bank, Credit Union, or Thrift).
   - Under $50 million
   - $50 – 99.9 million
   - $100 – 249.9 million
   - $250 - 499.9 million
   - $500 - 999.9 million
   - $1 – 4.9 billion
   - $5 – 9.9 billion
   - $10 billion or more

8. Are you or your organization a member of a trade association that provides education on payments and/or payments risk? (Select all that apply.)
   - ☐ American Bankers Association (ABA)
   - ☐ Association for Financial Professionals (AFP)
   - ☐ Credit Union National Association (CUNA)
   - ☐ Independent Community Bankers of America (ICBA)
   - ☐ NACHA The Electronic Payments Association
   - ☐ National Association of Federal Credit Unions (NAFCU)
   - ☐ Regional payments association (e.g., NEACH,SFE, SWACHA, WACHA,UMACHA, etc.)
   - ☐ State banking association
   - ☐ State AFP or treasury management association
   - ☐ Other, please specify _____
   - ☐ None

Ask 8a when respondent selected "regional payments association in Q8

8a. Please select the regional payments association to which you are a member. (Select all that apply.)

- ☐ ALACHA
- ☐ EPCOR
- ☐ EastPay
- ☐ GACHA
- ☐ MACHA
- ☐ NEACH
- ☐ SFE
- ☐ SOCACHA
- ☐ SWACHA
- ☐ TACHA
- ☐ The Payments Authority
- ☐ UMACHA
- ☐ WACHA
- ☐ WesPay
- ☐ Other, please specify _____

9. In terms of your organization's payments volume, who are the typical counterparties? Note: Businesses includes government entities. Skip Q9 when answer to Q1 is financial institution (Bank, Credit Union, or Thrift).
   - ○ Primarily payments to/from consumers
   - ○ Primarily payments to/from other businesses
   - ○ Payments to/from both consumers and businesses

10. What types of payments does your organization accept? Skip Q10 when answer to Q1 is financial institution (Bank, Credit Union, 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 Q1 is financial institution (Bank, Credit Union, 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? Only ask Q12 when answer to Q1 is financial institution (Bank, Credit Union, Thrift).

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

13. Which of the following payments products does your financial institution offer? (Select all that apply.) Only ask Q13 when answer to Q1 is financial institution (Bank, Credit Union, 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	☐
Lockbox services	☐
Cash	☐
International payments	☐

Payment Products	Offer an Online Service	Offer a Mobile Service
Bill payments	☐	☐
Person to person (P2P) payments	☐	☐
Consumer remote deposit capture	☐	☐
Commercial/Business remote deposit capture	☐	☐
Other payment products, please specify _____	☐	☐

Fraud by Payment Type:

14. Did your organization experience any payment fraud attempts in 2013? A response to this question is required.
    - ○ Yes Go to Q15
    - ○ No Go to Q16
    - ○ Don't know Go to Q16

15. Indicate the payment types where your organization experienced the highest number of fraud attempts (regardless of actual financial losses) in 2013. (Select and rank up to three that are highest.)

	1st choice	2nd choice	3rd choice
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) credits	o	o	o
Automated Clearinghouse (ACH) debits	o	o	o
Cash	o	o	o
Wire	o	o	o

Everyone who is asked Q15 should also get asked Q16.

16. 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 payment products	o	o	o
Cash	o	o	o
Wire	o	o	o

17. For mobile payment products, which is a greater expense for your organization– fraud prevention costs or actual fraud dollar losses? (Choose one response per row.) Only ask Q17 when respondent selected "fraud prevention costs" or "actual fraud dollar losses" for Mobile payments row in Q16.

Payment Product	Fraud prevention costs	Actual fraud dollar losses	Don't use/offer as a mobile payment service
Bill payments	o	o	o
Person to person (P2P) payments	o	o	o
Consumer remote deposit capture	o	o	o
Commercial/Business remote deposit capture	o	o	o
Other payment products, please specify _____	o	o	o

18. Did your organization experience any payment fraud losses in 2013? A response to this question is required.

- ○ Yes Go to Q19
- ○ No Go to Q22
- ○ Don't know Go to Q27

19. Indicate the payment types where your organization has experienced the highest dollar losses due to fraud in 2013. (Select and rank up to three that are highest.)

	1st choice	2nd choice	3rd choice
Credit cards	○	○	○
Debit cards – PIN based	○	○	○
Debit cards – signature based	○	○	○
Prepaid cards	○	○	○
Check instruments	○	○	○
Automated Clearinghouse (ACH) credits	○	○	○
Automated Clearinghouse (ACH) debits	○	○	○
Cash	○	○	○
Wire	○	○	○

20a. Please indicate which payment type has the highest loss rate based on the volume of transactions for that payment type.

- ○ 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 _____

20b. Please indicate which payment type has the highest loss rate based on the value of transactions for that payment type.

- ○ 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 _____

21. For your organization, please estimate the financial losses experienced due to payments fraud during 2013 as a percent of the company's total revenue.

- ○ less than .3%
- ○ .3% - .5%
- ○ .6% - 1.0%
- ○ 1.1% - 5.0%
- ○ over 5%

22. For your organization, how has the percentage of financial losses due to payments fraud changed in 2013 compared to 2012? A response to this question is required.

- ○ Increased very substantially (more than 10%)
- ○ Increased substantially (5% to 10%)
- ○ Increased somewhat (1% to 5%)
- ○ Stayed the same
- ○ Decreased somewhat (-1% to -5%)
- ○ Decreased substantially (-5% to -10%)
- ○ Decreased very substantially (-10% or more)
- ○ Don't know

ASK Q23 if answer is "increased" in Q 22

23. To which payment types do you attribute the 2013 increase in your organization's actual dollar losses? (Select all that apply.) (go to Q 27)

- ☐ Credit cards
- ☐ Debit cards – PIN based
- ☐ Debit cards – signature based
- ☐ Prepaid cards
- ☐ Check instruments
- ☐ Automated Clearinghouse (ACH) credits
- ☐ Automated Clearinghouse (ACH) debits
- ☐ Cash
- ☐ Wire

ASK Q24 if answer is "decreased" in Q22

24. To which payment types do you attribute the 2013 decrease in your organization's actual dollar losses? (Select all that apply.) (go to Q25)

- ☐ Credit cards
- ☐ Debit cards – PIN based
- ☐ Debit cards – signature based
- ☐ Prepaid cards
- ☐ Check instruments
- ☐ Automated Clearinghouse (ACH) credits
- ☐ Automated Clearinghouse (ACH) debits
- ☐ Cash
- ☐ Wire

ASK Q25 if answer is "decreased" in Q22

25. Did your organization make changes to its payments risk management practices that led to the decrease in 2013 payments fraud losses? A response to this question is required. If answer to Q25 is "no", then skip Q26 and go to Q27.

- ○ Yes – Go to Q26
- ○ No – Go to Q27
- ○ Don't know – Go to Q28

26. 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 Q28)

- ☐ 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
  - ☐ Debit card transactions
  - ☐ Credit card transactions
  - ☐ Check transactions
  - ☐ Wire transactions
- ☐ Other, please describe _____

ASK Q27 if answer is "increased" or "stayed the same" in Q22, Ask if answer is "no"/"DON'T KNOW to question 25.

27. Did your organization make changes that helped to control your organization's payments fraud losses? (Select all that apply.)

- ○ Yes (go to Q27A)
- ○ No (go to Q28)

27A. Which of the following changes did your organization make that helped to control your organization's payments fraud losses? (Select all that apply.)

- ☐ 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
  - ☐ Debit card transactions
  - ☐ Credit card transactions
  - ☐ Check transactions
  - ☐ Wire transactions
- ☐ Other, please describe _____

28. Did your organization experience any payment fraud attempts that were successful in 2013 (i.e., fraudster had financial gain)? . A response to this question is required.

- o Yes (go to Q29)
- o No (go to Q30)
- o Don't know (go to Q30)

29. 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.) An error message will be provided when response does not total 100%.

Only internal staff from your own organization_____%
Internal staff collaborating with external parties _____%
Only external parties _____%
Unknown- could not determine_____%

Common Fraud Schemes and Mitigation Strategies:

30. For payments received by your organization, what are the three current fraud schemes that fraudsters are using most often to initiate payments fraud? (Select and rank up to three that are most common.) SKIP Q30 when answer to Q1 is financial institution (Bank, Credit Union, or Thrift) or service provider.

	1st choice	2nd choice	3rd choice
Altered or forged checks	o	o	o
Counterfeit checks	o	o	o
Counterfeit currency	o	o	o
Counterfeit or stolen cards (debit, credit, or prepaid) used at point-of-sale (POS)	o	o	o
Counterfeit or stolen cards (debit, credit, or prepaid) used online	o	o	o
Other Internet initiated payments, e.g., unauthorized ACH WEB transactions	o	o	o
Fraudulent checks converted to ACH payments, e.g., point-of-purchase (POP), back office conversion (BOC), or account receivable conversion (ARC)/lockbox	o	o	o
Telephone-initiated payments, e.g., unauthorized ACH TEL payment or remotely created checks	o	o	o
Wireless-initiated payments, e.g., payments initiated through mobile device (PDA, cell phone) or other contactless card	o	o	o
Cash register frauds, e.g., over or under-rings, checks or cash for deposit stolen by employee	o	o	o
Use of fraudulent credentials or other data to establish new accounts or to defraud existing accounts, etc.	o	o	o
Customer service center fraud	o	o	o
Other, please specify _____	o	o	o

31. 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 and rank up to three that are most common.) Only ask Q31 when answer to Q1 is financial institution (Bank, Credit Union, or Thrift) or service provider.

	1st choice	2nd choice	3rd choice
Altered or forged checks	○	○	○
Counterfeit checks	○	○	○
Duplicate checks presented	○	○	○
Counterfeit currency	○	○	○
Counterfeit or stolen cards (credit, debit, or prepaid) used at point-of-sale	○	○	○
Counterfeit or stolen cards (credit, debit, or prepaid) 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 checks	○	○	○
Wireless-initiated payments, e.g., payments initiated through mobile device (PDA, cell phone) or other 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	○	○	○
Customer service center fraud	○	○	○
Other, please specify _____	○	○	○

32. 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 and rank up to three that are most common.) Ask all this question

	1st choice	2nd choice	3rd choice
Altered or forged checks	○	○	○
Counterfeit checks drawn against your own accounts	○	○	○
Duplicate checks presented	○	○	○
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 your organization due to internal fraud scheme	○	○	○
Customer service center fraud	○	○	○
Other, please specify _____	○	○	○

33. 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 and rank up to three that are most common.) Ask all this question

	1st choice	2nd choice	3rd choice
Information about customer obtained by family or friend	○	○	○
"Sensitive" information obtained from lost or stolen card, check, or other physical document, mobile phone or other 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 your 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	○	○	○
Social engineering used to obtain information used in the fraud scheme	○	○	○
Information sources are unknown	○	○	○

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

34. 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 in Q34

	Currently use	Plan to use before 2016	Don't use
Verify customer state identification card is authentic (e.g., machine read magnetic stripe or 2-D bar code of driver's license or other state issued ID)	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 verified	O	O	O
Signature verification	O	O	O
Customer (consumer or business) authentication for online transactions	O	O	O
Biometrics (e.g., use of fingerprints, hand geometry, retina patterns, voice patterns, etc.) to authenticate the person	O	O	O
Magnetic stripe authentication	O	O	O
Card chip authentication	O	O	O
PIN authentication	O	O	O
Token (USB token or fob)	O	O	O
Mobile device to authenticate person	O	O	O
Out-of-band authentication (e.g., an online banking user is accessing their online bank account with a login and a one-time password is sent to their mobile phone via SMS that is entered into the online channel to identify them)	O	O	O
Multi-factor 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

34a. Are there any other authentication methods your organization currently uses to mitigate payments risk?
Other authentication methods , please specify _____

35. Please rate the effectiveness of authentication methods currently used by your organization. Only allow a response to row in Q35 when Q34 answer in the same row is "currently use".

	Very effective	Some what effective	Some what ineffective
Verify customer state identification card is authentic (e.g., machine read magnetic stripe or 2-D bar code of driver's license or other state issued ID)	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 verified	O	O	O
Signature verification	O	O	O
Customer (consumer or business) authentication for online transactions	O	O	O
Biometrics (e.g., use of fingerprints, hand geometry, retina patterns, voice patterns, etc.) to authenticate the person	O	O	O
Magnetic stripe authentication	O	O	O
Card chip authentication	O	O	O
PIN authentication	O	O	O
Token (USB token or fob)	O	O	O
Mobile device to authenticate person	O	O	O
Out-of-band authentication (e.g., an online banking user is accessing their online bank account with a login and a one-time password is sent to their mobile phone via SMS that is entered into the online channel to identify them)	O	O	O
Multi-factor 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

36. 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 in Q36

	Currently use	Plan to use before 2016	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, anomaly detection 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
Buy insurance coverage to minimize risk	O	O	O

36a. Are there any other transaction screening and risk management methods your organization currently uses to mitigate payments risk?

Other transaction screening and risk management methods, please specify _____

37. Please rate the effectiveness of the transaction screening and risk management methods currently used by your organization. Only allow a response to row in Q37 when Q36 answer in the same row is "currently use".

	Very effective	Some what effective	Some what 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, anomaly detection 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
Buy insurance coverage to minimize risk	O	O	O

38. Which of the following internal controls and procedures does your organization currently use or plan to use? Limit response to one per row in Q38

	Currently use	Plan to use before 2016	Don't use
Physical access controls to payment processing functions (e.g., controls that limit physical access to a place or resource such as restricted access or locked room where payment processes are performed, using a safe for storage of blank check stock, etc.)	o	o	o
Logical access controls to your computing network and payment processing applications (e.g., technical controls that enforce restrictions on who or what can access computing resources. Access is the ability to read, create, modify or delete records, files, execute a program, use an external connection, etc.)	o	o	o
Dedicated computer used to conduct transactions with financial institution or financial service provider (e.g., computer used only for payment processing and cannot be used for other purposes like ordering offices supplies, using email, web browsing, etc.)	o	o	o
Authentication and authorization controls to payment processes (authentication is proving that the users are who they claim to be and authorization is the permission to use a resource given by the application or system owner)	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 (e.g., meet deadlines for chargebacks, returning payments, etc.)	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
Prohibit use of personal devices for processing of organization's payment transactions	o	o	o
Allow use of personal devices for processing of organization's payment transactions with specific controls, e.g., dollar limits, type of transaction, dual controls, etc.	o	o	o

38a. Are there any other internal controls and procedures your organization currently uses to mitigate payments risk?

Other internal controls and procedures please specify _____

39. Please rate the effectiveness of the internal controls and procedures currently used by your organization. Only allow a response to row in Q39 when Q38 answer in the same row is "currently use".

	Very effecti ve	Some what effective	Some what ineffective
Physical access controls to payment processing functions (e.g., controls that limit physical access to a place or resource such as restricted access or locked room where payment processes are performed, using a safe for storage of blank check stock, etc.)	O	O	O
Logical access controls to your computing network and payment processing applications (e.g., technical controls that enforce restrictions on who or what can access computing resources. Access is the ability to read, create, modify or delete records, files, execute a program, use an external connection, etc.)	O	O	O
Dedicated computer used to conduct transactions with financial institution or financial service provider (e.g., computer used only for payment processing and cannot be used for other purposes like ordering offices supplies, using email, web browsing, etc.)	O	O	O
Authentication and authorization controls to payment processes (authentication is proving that the users are who they claim to be and authorization is the permission to use a resource given by the application or system owner)	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 (e.g., meet deadlines for chargebacks, returning payments, etc.)	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
Prohibit use of personal devices for processing of organization's payment transactions	O	O	O
Allow use of personal devices for processing of organization's payment transactions with specific controls, e.g., dollar limits, type of transaction, dual controls, etc.	O	O	O

40. What risk mitigation services offered by your financial institution/service provider does your organization currently use or plan to use? Skip Q40-41 if answer to Q1 is financial institution (Bank, Credit Union, Thrift) or service provider. For all other responses to Q1 ask Q40 and 41. Limit response to one per row in Q40.

	Currently use	Plan to use before 2016	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
Tokenization of sensitive information (e.g., cardholder primary account number is replaced with a randomized token that represents the cardholder data reducing transmission and storage of actual cardholder sensitive data)	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
Payment fraud prevention training (e.g., classes, webinars, workshops, print or online materials, etc.)	O	O	O

40a. Are there any other risk mitigation services your organization currently uses to mitigate payments risk?
Other risk mitigation services, please specify _____

41. Please rate the effectiveness of risk mitigation services currently used by your organization. Only allow a response to row in Q41 when Q40 answer in the same row is "currently use".

	Very effective	Some what effective	Some what 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
Tokenization of sensitive information (e.g., cardholder primary account number is replaced with a randomized token that represents the cardholder data reducing transmission and storage of actual cardholder sensitive data)	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
Payment fraud prevention training (e.g., classes, webinars, workshops, print or online materials, etc.)	o	o	o

42. What risk mitigation services/products does your organization currently offer or plan to offer to your business customers? Ask Q42 only when the answer to Q1 is financial institution (Bank, Credit Union, Thrift) or service provider. Selection is limited to one per row in Q42.

	Currently Offer	Plan to Offer before 2016	Don't Offer
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
Tokenization of sensitive information (e.g., cardholder primary account number is replaced with a randomized token that represents the cardholder data reducing transmission and storage of actual cardholder sensitive data)	O	O	O
Account alert services	O	O	O
Card alert services for commercial/corporate cards	O	O	O
Customer activates/de-activates debit or credit card as needed for use or to block use	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
Payment fraud prevention training (e.g., classes, webinars, workshops, print or online materials, etc.)	O	O	O

42A. Are there any other risk mitigation service/products your organization currently offers to your business customers?

Other risk mitigation service/products, please specify _____

43. Please rate the effectiveness of risk mitigation services currently offered by your organization to your business customers. Only allow a response to row in Q43 when Q42 answer in the same row is "currently offer".

	Very effective	Some what effective	Some what 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
Tokenization of sensitive information (e.g., cardholder primary account number is replaced with a randomized token that represents the cardholder data reducing transmission and storage of actual cardholder sensitive data)	o	o	o
Account alert services	o	o	o
Card alert services for commercial/corporate cards	o	o	o
Customer activates/de-activates debit or credit card as needed for use or to block use	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
Payment fraud prevention training (e.g., classes, webinars, workshops, print or online materials, etc.)	o	o	o

44. What risk mitigation services/products does your organization currently offer or plan to offer to your consumer customers? Ask Q44 only when the answer to Q1 is financial institution (Bank, Credit Union, Thrift) or service provider. Selection is limited to one per row in Q44.

	Currently Offer	Plan to Offer before 2016	Don't Offer
Post no check services	O	O	O
ACH debit blocks	O	O	O
Account masking services	O	O	O
Account alert services	O	O	O
Card alert services for debit or credit cards	O	O	O
Customer activates/de-activates debit or credit card as needed for use or to block use	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
Payment fraud prevention training (e.g., classes, webinars, workshops, print or online materials, etc.)	O	O	O

44a. Are there any other risk mitigation service/products your organization currently offers to your consumer customers?

Other risk mitigation service/products, please specify _____

45. Please rate the effectiveness of risk mitigation services currently offered by your organization to your consumer customers. Only allow a response to row in Q45 when Q44 answer in the same row is "currently offer".

	Very effective	Some what effective	Some what ineffective
Post no check services	O	O	O
ACH debit blocks	O	O	O
Account masking services	O	O	O
Account alert services	O	O	O
Card alert services for debit or credit cards	O	O	O
Customer activates/de-activates debit or credit card as needed for use or to block use	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
Payment fraud prevention training (e.g., classes, webinars, workshops, print or online materials, etc.)	O	O	O

46. 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 with EMV chip technology
- ☐ Tokenization of sensitive information, e.g., cardholder primary account number is replaced with a randomized token that represents the cardholder data reducing transmission and storage of actual cardholder data
- ☐ 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 _____

47. 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
- ☐ EMV chip and signature requirement
- ☐ EMV chip and PIN requirement
- ☐ PIN requirement
- ☐ Physical token (USB token or fob)
- ☐ Mobile device to authenticate person
- ☐ Out-of-band authentication
- ☐ Multi-factor authentication
- ☐ Other, please specify _____

48. 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 regulatory restrictions/other concerns if customer data shared with others to help mitigate fraud
- ☐ 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 _____

49. 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
- ☐ Establish new laws/regulations to require data sharing to strengthen the management of payments fraud risk
- ☐ Strengthen disincentives to committing fraud through more likely prosecution and increased penalties for fraud and attempted fraud
- ☐ 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 transactions
- ☐ Other, please specify_____

50. Is there anything else that you would like to share as part of this survey?

_____

Place at end of survey:

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.