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

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	○	○	○
Debit cards – PIN based	○	○	○
Debit cards – signature based	○	○	○
Prepaid cards	○	○	○
Check instruments	○	○	○
Automated Clearinghouse (ACH)	○	○	○
Mobile payment products	○	○	○
Cash	○	○	○
Wire	○	○	○

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	○	○	○
Person to person (P2P) payments	○	○	○
Consumer remote deposit capture	○	○	○
Commercial/Business remote deposit capture	○	○	○
Other payment products, please specify ______	○	○	○

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	○	○	○
Counterfeit checks	○	○	○
Counterfeit currency	○	○	○
Counterfeit or stolen cards (debit, credit, or prepaid) used at point-of-sale (POS)	○	○	○
Counterfeit or stolen cards (debit, credit, 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	○	○	○
Cash register frauds, e.g., over or under-rings, checks or cash for deposit stolen by employee	○	○	○
Use of fraudulent credentials or other data to establish new accounts or to defraud existing accounts, etc.	○	○	○
Customer service center fraud	○	○	○
Other, please specify ___________________________________	○	○	○

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)	○	○	○
Positive identification of purchaser or valid account for in-store/in-person transactions, e.g., review picture ID	○	○	○
Card security code located on back of payment card verified, e.g., CVV2, CVC2, or CID codes verified	○	○	○
Signature verification	○	○	○
Customer (consumer or business) authentication for online transactions	○	○	○
Biometrics (e.g., use of fingerprints, hand geometry, retina patterns, voice patterns, etc.) to authenticate the person	○	○	○
Magnetic stripe authentication	○	○	○
Card chip authentication	○	○	○
PIN authentication	○	○	○
Token (USB token or fob)	○	○	○
Mobile device to authenticate person	○	○	○
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)	○	○	○
Multi-factor authentication	○	○	○
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)	○	○	○

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)	○	○	○
Positive identification of purchaser or valid account for in-store/in-person transactions, e.g., review picture ID	○	○	○
Card security code located on back of payment card verified, e.g., CVV2, CVC2, or CID codes verified	○	○	○
Signature verification	○	○	○
Customer (consumer or business) authentication for online transactions	○	○	○
Biometrics (e.g., use of fingerprints, hand geometry, retina patterns, voice patterns, etc.) to authenticate the person	○	○	○
Magnetic stripe authentication	○	○	○
Card chip authentication	○	○	○
PIN authentication	○	○	○
Token (USB token or fob)	○	○	○
Mobile device to authenticate person	○	○	○
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)	○	○	○
Multi-factor authentication	○	○	○
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)	○	○	○

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	○	○	○
Fraud detection pen for currency	○	○	○
Software that detects fraud through pattern matching, predictive analytics, anomaly detection or other indicators	○	○	○
Centralized fraud-related information database for one payment type	○	○	○
Centralized fraud-related information database for multiple payment types	○	○	○
Participate in fraudster databases and receive alerts	○	○	○
Centralized risk management department	○	○	○
Provide customer education and training on payment fraud risk mitigation	○	○	○
Provide staff education and training on payment fraud risk mitigation	○	○	○
Buy insurance coverage to minimize risk	○	○	○

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	○	○	○
Fraud detection pen for currency	○	○	○
Software that detects fraud through pattern matching, predictive analytics, anomaly detection or other indicators	○	○	○
Centralized fraud-related information database for one payment type	○	○	○
Centralized fraud-related information database for multiple payment types	○	○	○
Participate in fraudster databases and receive alerts	○	○	○
Centralized risk management department	○	○	○
Provide customer education and training on payment fraud risk mitigation	○	○	○
Provide staff education and training on payment fraud risk mitigation	○	○	○
Buy insurance coverage to minimize risk	○	○	○

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.)	○	○	○
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.)	○	○	○
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.)	○	○	○
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)	○	○	○
Restrict or limit employee use of Internet from organization's network	○	○	○
Dual controls and segregation of duties within payment initiation and receipt processes	○	○	○
Transaction limits for payment disbursements	○	○	○
Transaction limits for corporate card purchases	○	○	○
Reconcile bank accounts daily	○	○	○
Review card related reports daily	○	○	○
Address exception items timely (e.g., meet deadlines for chargebacks, returning payments, etc.)	○	○	○
Separate banking accounts by purpose or by payment type	○	○	○
Employee hotline to report potential fraud	○	○	○
Verify application of controls via audit or management review	○	○	○
Periodic internal/external audits	○	○	○
Prohibit use of personal devices for processing of organization's payment transactions	○	○	○
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.	○	○	○

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.)	○	○	○
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.)	○	○	○
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.)	○	○	○
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)	○	○	○
Restrict or limit employee use of Internet from organization's network	○	○	○
Dual controls and segregation of duties within payment initiation and receipt processes	○	○	○
Transaction limits for payment disbursements	○	○	○
Transaction limits for corporate card purchases	○	○	○
Reconcile bank accounts daily	○	○	○
Review card related reports daily	○	○	○
Address exception items timely (e.g., meet deadlines for chargebacks, returning payments, etc.)	○	○	○
Separate banking accounts by purpose or by payment type	○	○	○
Employee hotline to report potential fraud	○	○	○
Verify application of controls via audit or management review	○	○	○
Periodic internal/external audits	○	○	○
Prohibit use of personal devices for processing of organization's payment transactions	○	○	○
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.	○	○	○

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	○	○	○
Check payee positive pay	○	○	○
Post no check services	○	○	○
ACH debit blocks	○	○	○
ACH debit filters	○	○	○
ACH positive pay	○	○	○
ACH payee positive pay	○	○	○
Account masking services	○	○	○
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)	○	○	○
Account alert services	○	○	○
Card alert services for commercial/corporate cards	○	○	○
Fraud loss prevention services e.g., insurance	○	○	○
Online information services, e.g., statements, check images	○	○	○
Multi-factor authentication controls to initiate payments from bank account	○	○	○
Payment fraud prevention training (e.g., classes, webinars, workshops, print or online materials, etc.)	○	○	○

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	○	○	○
Check payee positive pay	○	○	○
Post no check services	○	○	○
ACH debit blocks	○	○	○
ACH debit filters	○	○	○
ACH positive pay	○	○	○
ACH payee positive pay	○	○	○
Account masking services	○	○	○
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)	○	○	○
Account alert services	○	○	○
Card alert services for commercial/corporate cards	○	○	○
Fraud loss prevention services e.g., insurance	○	○	○
Online information services, e.g., statements, check images	○	○	○
Multi-factor authentication controls to initiate payments from bank account	○	○	○
Payment fraud prevention training (e.g., classes, webinars, workshops, print or online materials, etc.)	○	○	○

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	○	○	○
Check payee positive pay	○	○	○
Post no check services	○	○	○
ACH debit blocks	○	○	○
ACH debit filters	○	○	○
ACH positive pay	○	○	○
ACH payee positive pay	○	○	○
Account masking services	○	○	○
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)	○	○	○
Account alert services	○	○	○
Card alert services for commercial/corporate cards	○	○	○
Customer activates/de-activates debit or credit card as needed for use or to block use	○	○	○
Fraud loss prevention services, e.g., insurance	○	○	○
Online information services, e.g., statements, check images	○	○	○
Multi-factor authentication controls to initiate payments from bank account	○	○	○
Payment fraud prevention training (e.g., classes, webinars, workshops, print or online materials, etc.)	○	○	○

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	○	○	○
Check payee positive pay	○	○	○
Post no check services	○	○	○
ACH debit blocks	○	○	○
ACH debit filters	○	○	○
ACH positive pay	○	○	○
ACH payee positive pay	○	○	○
Account masking services	○	○	○
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)	○	○	○
Account alert services	○	○	○
Card alert services for commercial/corporate cards	○	○	○
Customer activates/de-activates debit or credit card as needed for use or to block use	○	○	○
Fraud loss prevention services, e.g., insurance	○	○	○
Online information services, e.g., statements, check images	○	○	○
Multi-factor authentication controls to initiate payments from bank account	○	○	○
Payment fraud prevention training (e.g., classes, webinars, workshops, print or online materials, etc.)	○	○	○

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	○	○	○
ACH debit blocks	○	○	○
Account masking services	○	○	○
Account alert services	○	○	○
Card alert services for debit or credit cards	○	○	○
Customer activates/de-activates debit or credit card as needed for use or to block use	○	○	○
Fraud loss prevention services, e.g., insurance	○	○	○
Online information services, e.g., statements, check images	○	○	○
Multi-factor authentication controls to initiate payments from bank account	○	○	○
Payment fraud prevention training (e.g., classes, webinars, workshops, print or online materials, etc.)	○	○	○

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	○	○	○
ACH debit blocks	○	○	○
Account masking services	○	○	○
Account alert services	○	○	○
Card alert services for debit or credit cards	○	○	○
Customer activates/de-activates debit or credit card as needed for use or to block use	○	○	○
Fraud loss prevention services, e.g., insurance	○	○	○
Online information services, e.g., statements, check images	○	○	○
Multi-factor authentication controls to initiate payments from bank account	○	○	○
Payment fraud prevention training (e.g., classes, webinars, workshops, print or online materials, etc.)	○	○	○

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.