

## 2012 Payments Fraud Questionnaire

The survey will be administered online. Question numbers will not show. Information in red font represents logic in the survey tool and is not displayed. Bullet formatting – if bullets are circles, then respondent may choose one answer. If bullets are squares, respondent may choose one or more answers.

### Introduction

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

### Payments Fraud Survey Instructions

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

### Confidentiality of Response

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

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

### Organization Profile:

1. A) Is your organization a banking or financial services organization?
  - Yes **Go to Q1B**
  - No **Go to Q1C**
1. B) Please select the type of financial services organization below.
  - Bank
  - Credit Union
  - Thrift
  - Service provider
  - Insurance company and pension funds
  - Brokers, underwriters and investment company

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

- Agriculture
- Brokers, underwriters and investment company
- Business services/Consulting
- Construction
- Educational services
- Energy
- 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 \_\_\_\_\_

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

Financial institution name \_\_\_\_\_

City/Town \_\_\_\_\_

State **Choose response from drop down list.**

ZIP/Postal Code \_\_\_\_\_

Main nine digit routing and transit number. Please specify the head office number.

\_\_\_\_\_ - \_\_\_\_\_ - \_\_\_\_\_ **Response must be numeric.**

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

Company Name: \_\_\_\_\_

City/Town: \_\_\_\_\_

State **Choose response from drop down list.**

ZIP/Postal Code \_\_\_\_\_

4. What is...

Your name \_\_\_\_\_ (optional)

Your title \_\_\_\_\_ (optional)

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

E-mail address \_\_\_\_\_ (optional)

5. What best describes the type of department you work in? Select one.
- Accounts payable or receivable
  - Audit
  - Compliance/Risk Management
  - Finance
  - Operations/Payments processing function
  - Senior management over multiple departments
  - Treasury
  - Other
6. What do you estimate are your organization's 2011 annual revenues? If you don't know, please provide your best estimate.
- Under \$50 million
  - \$50 – 99 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 2011 total assets? If you don't know, please provide your best estimate. **Ask when answer to Q1B Bank, Credit Union, or Thrift.**
- Under \$50 million
  - \$50 – 99 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 bank a member of a banking association? (Select all that apply.) **A when answer to Q1B is a bank.**
- Independent Community Bankers of America (ICBA)
  - A state banking association
  - Other
  - None
9. In terms of your organization's payments volume, who are the typical counterparties? Note: Businesses includes government entities. **Skip Q9 when answer to Q1B is Bank, Credit Union, or Thrift.**
- 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 Q1B is Bank, Credit Union, or Thrift.**

| Payment Types                            | Payments Accepted/Received |
|------------------------------------------|----------------------------|
| Credit cards                             | <input type="checkbox"/>   |
| Debit cards – PIN based                  | <input type="checkbox"/>   |
| Debit cards – signature based            | <input type="checkbox"/>   |
| Prepaid cards, e.g., gift, payroll, etc. | <input type="checkbox"/>   |
| Check instruments                        | <input type="checkbox"/>   |
| Automated Clearinghouse (ACH) debits     | <input type="checkbox"/>   |
| Automated Clearinghouse (ACH) credits    | <input type="checkbox"/>   |
| Cash                                     | <input type="checkbox"/>   |
| Wire                                     | <input type="checkbox"/>   |
| Other (please specify) _____             | <input type="checkbox"/>   |

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

| Payment Types                            | Payments Disbursed/Made  |
|------------------------------------------|--------------------------|
| Credit cards                             | <input type="checkbox"/> |
| Debit cards – PIN based                  | <input type="checkbox"/> |
| Debit cards – signature based            | <input type="checkbox"/> |
| Prepaid cards, e.g., gift, payroll, etc. | <input type="checkbox"/> |
| Check instruments                        | <input type="checkbox"/> |
| Automated Clearinghouse (ACH) debits     | <input type="checkbox"/> |
| Automated Clearinghouse (ACH) credits    | <input type="checkbox"/> |
| Cash                                     | <input type="checkbox"/> |
| Wire                                     | <input type="checkbox"/> |
| Other (please specify) _____             | <input type="checkbox"/> |

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

- 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.  
 Ask when answer to Q1B is Bank, Credit Union, or Thrift.

| Payment Products                          | Offer                    |
|-------------------------------------------|--------------------------|
| Credit cards                              | <input type="checkbox"/> |
| Debit cards – PIN based                   | <input type="checkbox"/> |
| Debit cards – signature based             | <input type="checkbox"/> |
| Prepaid cards, e.g., gift, payroll, etc.  | <input type="checkbox"/> |
| Check instruments                         | <input type="checkbox"/> |
| Automated Clearinghouse (ACH) Origination | <input type="checkbox"/> |
| Wire transfer                             | <input type="checkbox"/> |
| Bill payment                              | <input type="checkbox"/> |
| Lockbox services                          | <input type="checkbox"/> |
| International payments                    | <input type="checkbox"/> |
| Mobile payments                           | <input type="checkbox"/> |
| P2P payments                              | <input type="checkbox"/> |
| Remote deposit capture                    | <input type="checkbox"/> |

**Fraud by Payment Type:**

14. Indicate the payment types where your organization experienced the highest number of fraud attempts (regardless of actual financial losses) in 2011. Select up to three that you think are highest.
- Credit cards
  - Debit cards – PIN based
  - Debit cards – signature based
  - Prepaid cards
  - Checks
  - Automated Clearinghouse credits
  - Automated Clearinghouse debits
  - Cash
  - Wire
  - or
  - No payment fraud attempts experienced.

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

| Payment Product               | Fraud prevention costs | Actual fraud dollar losses | Don't use/offer payment type |
|-------------------------------|------------------------|----------------------------|------------------------------|
| Credit cards                  | <input type="radio"/>  | <input type="radio"/>      | <input type="radio"/>        |
| Debit cards – PIN based       | <input type="radio"/>  | <input type="radio"/>      | <input type="radio"/>        |
| Debit cards – signature based | <input type="radio"/>  | <input type="radio"/>      | <input type="radio"/>        |
| Prepaid cards                 | <input type="radio"/>  | <input type="radio"/>      | <input type="radio"/>        |
| Check instruments             | <input type="radio"/>  | <input type="radio"/>      | <input type="radio"/>        |
| Automated Clearinghouse (ACH) | <input type="radio"/>  | <input type="radio"/>      | <input type="radio"/>        |
| Mobile                        | <input type="radio"/>  | <input type="radio"/>      | <input type="radio"/>        |
| Wire                          | <input type="radio"/>  | <input type="radio"/>      | <input type="radio"/>        |

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

- Credit cards
- Debit cards – PIN based
- Debit cards – signature based
- Prepaid cards
- Checks
- Automated Clearinghouse credits
- Automated Clearinghouse debits
- Cash
- Wire
- or
- No payment fraud losses experienced

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

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

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

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

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

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

20. To which payment types do you attribute the 2011 increase in your organization's actual dollar losses? Select all that apply. (go to Q 25)
- Credit cards
  - Debit cards – PIN based
  - Debit cards – signature based
  - Prepaid cards
  - Checks
  - Automated Clearinghouse credits
  - Automated Clearinghouse debits
  - Cash
  - Wire
21. The percentage of dollar losses at my organization due to fraud has decreased by \_\_\_% in 2011 compared to 2010. (go to 22)
- 1 - 5%
  - 6% - 10%
  - More than 10%
  - Unsure
22. To which payment types do you attribute the 2011 decrease in your organization's actual dollar losses? Select all that apply. (go to Q23)
- Credit cards
  - Debit cards – PIN based
  - Debit cards – signature based
  - Prepaid cards
  - Checks
  - Automated Clearinghouse credits
  - Automated Clearinghouse debits
  - Cash
  - Wire
23. Did your organization make changes to its payments risk management practices that led to the decrease in 2011 payments fraud losses? If answer to Q23 is "no", then skip Q24 and go to Q25.
- Yes
  - No
24. What are the key changes made by your organization that you think have contributed to the decrease in your organization's payments fraud losses? Select all that apply. (go to Q 25)
- Staff training and education
  - Enhanced methods to authenticate customer and/or validate customer account
  - Enhanced internal controls and procedures
  - Adopted or increased use of risk management tools offered by our organization's financial institution or financial service provider, e.g., account alerts, positive pay, etc.
  - Enhanced fraud monitoring system If selected, then also list:  
To which payments does enhanced monitoring apply? Select all that apply.
    - ACH transactions
    - Card transactions
    - Check transactions
    - Wire transactions
  - Other (please describe) \_\_\_\_\_

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

Only internal staff from your own organization \_\_\_\_\_ %  
Internal staff collaborating with external parties \_\_\_\_\_ %  
Only external parties \_\_\_\_\_ %  
Unknown- could not determine \_\_\_\_\_ %  
or  
No successful attempts (fill in 100% here) \_\_\_\_\_ %

**Common Fraud Schemes and Mitigation Strategies:**

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

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

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

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

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

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

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

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

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

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

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

|                                                                                                                                                 | Currently use         | Plan to use before 2014 | Don't use             |
|-------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-------------------------|-----------------------|
| Verify customer state identification card is authentic (machine read magnetic stripe or 2-D bar code)                                           | <input type="radio"/> | <input type="radio"/>   | <input type="radio"/> |
| Positive identification of purchaser or valid account for in-store/in-person transactions e.g., review picture ID                               | <input type="radio"/> | <input type="radio"/>   | <input type="radio"/> |
| Card security code located on back of payment card verified e.g., CVV2, CVC2, or CID codes                                                      | <input type="radio"/> | <input type="radio"/>   | <input type="radio"/> |
| Signature verification                                                                                                                          | <input type="radio"/> | <input type="radio"/>   | <input type="radio"/> |
| Customer (consumer or business) authentication for online transactions                                                                          | <input type="radio"/> | <input type="radio"/>   | <input type="radio"/> |
| Biometrics authentication                                                                                                                       | <input type="radio"/> | <input type="radio"/>   | <input type="radio"/> |
| Magnetic stripe authentication                                                                                                                  | <input type="radio"/> | <input type="radio"/>   | <input type="radio"/> |
| Card chip authentication                                                                                                                        | <input type="radio"/> | <input type="radio"/>   | <input type="radio"/> |
| PIN authentication                                                                                                                              | <input type="radio"/> | <input type="radio"/>   | <input type="radio"/> |
| 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 | <input type="radio"/> | <input type="radio"/>   | <input type="radio"/> |

Are the other authentication methods your organization currently uses to mitigate payment risk?

Other methods (please specify) \_\_\_\_\_

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

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

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

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

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

Other methods (please specify) \_\_\_\_\_

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

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

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

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

Are there any other internal controls and procedures your organization currently uses?

Other internal controls or procedures (please specify) \_\_\_\_\_

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

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

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

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

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

Other services (please specify) \_\_\_\_\_

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

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

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

|                                                                             | Currently offer       | Plan to offer before 2014 | Don't offer           |
|-----------------------------------------------------------------------------|-----------------------|---------------------------|-----------------------|
| Check positive pay/reverse positive pay                                     | <input type="radio"/> | <input type="radio"/>     | <input type="radio"/> |
| Check payee positive pay                                                    | <input type="radio"/> | <input type="radio"/>     | <input type="radio"/> |
| Post no check services                                                      | <input type="radio"/> | <input type="radio"/>     | <input type="radio"/> |
| ACH debit blocks                                                            | <input type="radio"/> | <input type="radio"/>     | <input type="radio"/> |
| ACH debit filters                                                           | <input type="radio"/> | <input type="radio"/>     | <input type="radio"/> |
| ACH positive pay                                                            | <input type="radio"/> | <input type="radio"/>     | <input type="radio"/> |
| ACH payee positive pay                                                      | <input type="radio"/> | <input type="radio"/>     | <input type="radio"/> |
| Account masking services                                                    | <input type="radio"/> | <input type="radio"/>     | <input type="radio"/> |
| Account alert services                                                      | <input type="radio"/> | <input type="radio"/>     | <input type="radio"/> |
| Card alert services for commercial/corporate cards                          | <input type="radio"/> | <input type="radio"/>     | <input type="radio"/> |
| Online information services, e.g., statements, check images                 | <input type="radio"/> | <input type="radio"/>     | <input type="radio"/> |
| Multi-factor authentication controls to initiate payments from bank account | <input type="radio"/> | <input type="radio"/>     | <input type="radio"/> |

Are there other risk mitigation services/products that your organization currently offers your business customers?  
 Other services or products (please specify) \_\_\_\_\_

39. From your organization's perspective, what new or improved methods are most needed to reduce payments fraud? Select those you think would be most helpful.
- Authentication controls over Internet initiated payments
  - Authentication controls over mobile device initiated payments
  - Replacement of card, magnetic stripe technology
  - Improved methods for information sharing on emerging fraud tactics e.g., those being conducted by criminal rings
  - More aggressive law enforcement
  - Image survivable check security features for business checks
  - Industry alert services
  - Industry specific education on payments fraud prevention best practices
  - Consumer education of fraud prevention
  - Other (please specify) \_\_\_\_\_

40. What authentication methods would your organization prefer or consider adopting to help reduce payments fraud? Select all methods your organization would most likely prefer or consider for adoption.
- Biometrics
  - Chip for dynamic authentication (e.g., EMV)
  - Chip and PIN requirement
  - PIN requirement
  - Token (USB token or fob)
  - Mobile device to authenticate person
  - Out-of-band/channel authentication (email, text, fax, or phone) to authorize payment
  - Multi-factor authentication
  - Other (please specify) \_\_\_\_\_

41. What are the main barriers to mitigate payments fraud that your organization experiences? Select all that you consider to be the main barriers.
- Consumer data privacy issues/concerns
  - Corporate reluctance to share information due to competitive issues
  - Cost of implementing in-house fraud detection tool/method **If selected ask:**  
Please describe what tool/method your organization wants to implement, but cannot afford to do so  
\_\_\_\_\_
  - Cost of implementing commercially available fraud detection tool/service **If selected ask:**  
Please describe what tool/service your organization wants to implement, but cannot afford to do so  
\_\_\_\_\_
  - Lack of compelling business case (cost vs. benefit) to adopt new or change existing methods
  - Lack of staff resources
  - Unable to combine payment information for review due to payments operations performed in multiple business areas, multiple states, with multiple banks, etc. Corporate reluctance to share information due to competitive issues
  - Other (please specify) \_\_\_\_\_
42. Please indicate what types of legal or regulatory changes you think would help reduce payments fraud. Select all that apply.
- Establish new laws/regulations or change existing ones in order to strengthen the management of payments fraud risk
  - Increase penalties for fraud and attempted fraud
  - Strengthen disincentives to committing fraud through more likely prosecution
  - Improve law enforcement cooperation on domestic and international payments fraud and fraud rings
  - Assign responsibility for mitigating fraud risk to the party best positioned to take action against fraud
  - Assign liability for fraud losses to the party most responsible for not acting to reduce the risk of payment fraud
  - Place more responsibility on consumers and customers to reconcile and protect their payments data
  - Place responsibility to mitigate fraud and shift liability for fraudulent card payments to the entity that initially accepts the card payment
  - Focus future legal or regulatory changes on data breaches to where the breaches occur
  - Align Regulation E and Regulation CC to reflect changes in check collection systems' use of check images and conversion of checks to ACH

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