Federal Reserve Bank Minneapolis' Payments, Standards, and Outreach Group

Financial Institution Payments Fraud Mitigation Survey 2017

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. Terms in italics will have definitions, and respondents can mouse over term to see the definition.

Introduction

Please complete this online survey to help us better understand new or continuing challenges that your financial institution faces with payments fraud as well as methods you use to reduce fraud risk. This survey focuses on methods used to mitigate fraud by payment type. We appreciate your willingness to complete the entire survey. Your thoughtful responses will help inform payments industry participants about effectiveness of fraud mitigation methods. As a survey participant, we will notify you when the report of results is available and you will also be invited to attend a free webinar later this year that presents the survey findings.

Payments Fraud Survey Instructions

- This survey is not meant to be taken on a Smart Phone.
- Please try to answer all questions as best you can.
- To review the questions, and terms and definitions in advance of completing the survey; see https://www.minneapolisfed.org/about/what-we-do/payments-information
- Use only the Back button located at the bottom of the screen. Do not use the "Back" button on your browser as the survey tool doesn't support this.
- The survey URL is specific to your financial institution response. Only allow people within your organization to access your response during completion.
- Be sure to save your responses before leaving the survey.
- Definitions for terms in italics are available by hovering your mouse over the term.
- If you have a question about the survey, please send your name and contact information in an email to the Payments, Standards, & Outreach Group at the Federal Reserve Bank of Minneapolis mpls.psog.events@mpls.frb.org

Confidentiality of Response

The information you are providing will be publicly shared as summary-level data. Your financial institution's specific responses will be shared with a limited number of Federal Reserve Bank staff working on this payments fraud research project.

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

Contents

Financial institution Profile

1) What is your … A response to this question is required.

1a) Financial institution name ____

1b) Main nine digit routing and transit number. (Please specify the head office number.)

_ _ _ _ - _ _ _ _ - _ Response must be numeric.

1c) State (physical location of head office) Provide drop down list of 50 states in alpha order, also include District of Columbia.

2) What is …

2a) Your name ____

2b) Your title ____

2c) Email address _____________________________________ We will use your email address to notify you when the survey results report is published.

3) Are you a subject matter expert on fraud mitigation at your financial institution?

○ Yes
○ No

4) What type of customers are the predominant users of your financial institution's payment products and services?

○ Primarily consumers
○ Primarily business/commercial
○ Both somewhat even

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

Payment Products	Offer
a) Cash	□
b) Checks	□
c) Credit cards i.e., issue cards and carry accounts receivables	□
d) Debit cards	□
e) Prepaid cards, e.g., payroll, gift, etc.	□
f) Automated Clearinghouse (ACH) origination	□
g) Automated Clearinghouse (ACH) receipt	□
h) Wire transfers	□
i) International payments	□
j) Bill payments	□
k) Person to person (P2P) payments	□
l) Consumer remote deposit capture	□
m) Commercial/Business remote deposit capture	□

Fraud by Payment Type

6) Did your financial institution experience any *payment fraud* attempts in 2016? Consider all attempts regardless of actual financial losses. A response to this question is required.
   - ○ Yes Go to Q 7
   - ○ No Go to Q 8
   - ○ Don't know Go to Q 8

7) Indicate the payment types where your financial institution experienced the highest number of fraud attempts in 2016. Consider all attempts regardless of actual financial losses. (Select and rank the three that are highest. Choose one answer per column.)

	1st choice	2nd choice	3rd choice
Checks include choice when answer to 5b is offer	○	○	○
Credit cards include choice when answer to 5c is offer	○	○	○
Debit cards – PIN based include choice when answer to 5d is offer	○	○	○
Debit cards – signature based include choice when answer to 5d is offer	○	○	○
Prepaid cards include choice when answer to 5e is offer	○	○	○
Automated Clearinghouse (ACH) credits include choice when answer to 5f or 5g is offer	○	○	○
Automated Clearinghouse (ACH) debits include choice when answer to 5f or 5g is offer	○	○	○
Wires include choice when answer to 5h is offer	○	○	○
Other, please specify ____	○	○	○

Or

7b) If your financial institution does not track fraud attempts, please choose the response below.

Do not track fraud attempts	○

8) Did your financial institution experience any *payment fraud* losses in 2016? A response to this question is required.
   - ○ Yes If yes, ask the following question 9.
   - ○ No If no, skip to Q 11.
   - ○ Don't know If don't know, skip to Q11.

9) On which payment types did fraud losses occur? (Select one answer in each row.) Ask when Q8 is Yes

	Losses	No Losses	Don’t Know
Checks (Include choice when 5b is offer)	○	○	○
Credit cards (Include choice when 5c is offer)	○	○	○
Debit cards – PIN based (Include choice when 5d is offer)	○	○	○
Debit cards – signature based (Include choice when 5d is offer)	○	○	○
Prepaid cards (Include choice when 5e is offer)	○	○	○
Automated Clearinghouse (ACH) credits (Include choice when 5 f or g is offer)	○	○	○
Automated Clearinghouse (ACH) debits (Include choice when 5f or g is offer)	○	○	○
Wires (Include choice when 5h is offer)	○	○	○
Other, please specify________________________________	○	○	○

10) For your financial institution, how have losses due to payments fraud changed in 2016 compared to 2015? (Select one answer in each row.) If response row in Q9 is “don’t know”, exclude that choice from Q10.

	Increased	Decreased	Stayed the Same	Don’t Know
Checks (Include choice when 5b is offer)	○	○	○	○
Credit cards (Include choice when 5c is offer)	○	○	○	○
Debit cards – PIN based (Include choice when 5d is offer)	○	○	○	○
Debit cards – signature based (Include choice when 5d is offer)	○	○	○	○
Prepaid cards (Include choice when 5e is offer)	○	○	○	○
Automated Clearinghouse (ACH) credits (Include choice when 5 f or g is offer)	○	○	○	○
Automated Clearinghouse (ACH) debits (Include choice when 5f or g is offer)	○	○	○	○
Wires (Include choice when 5h is offer)	○	○	○	○
Other, please specify___________________________	○	○	○	○

Common Fraud Schemes and Mitigation Strategies by Payment Type

11) At your financial institution is fraud prevention/investigation a centralized function, is it decentralized by payment channel/silo, or is it some of each?

○ Centralized
○ Decentralized by payment channels/silos
○ Mixed – some of each If this choice is selected, ask

11b) Which payment channels are managed separately? (Select all that apply.)

□ Debit card show choice when 5d is offer
□ Credit card show choice when 5c is offer
□ Prepaid card show choice when 5e is offer
□ Checks show choice when 5b is offer
□ ACH show choice when 5f or 5g is offer
□ Wires show choice when 5h is offer

The next series of questions will ask about fraud schemes and risk mitigation practices. We encourage you to answer questions for each payment type that your financial institution offers and for new deposit/transaction accounts. You may take as much time as you need to complete the survey by the deadline in the cover memo, saving your responses when you need to (click save at bottom of page). You may return to the survey by clicking the same survey link provided in the survey invitation email. When returning to the survey, it will resume where you left off.

If you printed a copy of the survey questions from the Minneapolis Fed website (https://www.minneapolisfed.org/about/what-we-do/payments-information) to assist you in completing the survey, this next series of questions may appear in a different order online. Questions are rotated randomly by payment type.

Order of sections should be rotated so that respondents do not see the main sections in the same order – credit cards (Q12-13), new transaction/deposit account (Q 14), debit cards (Q15-16), checks (Q17-18), ACH (Q19 -20), and wires (Q21 -22). When these are complete, go to Q23.

Credit Cards Include credit card section, Q12-Q13h, when the answer to question 5c is offer.

12) What are the three current fraud attacks most often used to initiate credit card fraud against your financial institution or your customers' accounts? (Select and rank the three that are most common. Choose one answer per column.)

	1st choice	2nd choice	3rd choice
Counterfeit credit cards used at point-of-sale	○	○	○
Lost or stolen credit cards used at point-of-sale	○	○	○
Counterfeit credit cards used at ATM, e.g., for cash advance	○	○	○
Lost or stolen credit cards used at ATM	○	○	○
Counterfeit or stolen cards or card data used online (card-not-present)	○	○	○
Counterfeit or stolen cards or card data used by telephone or mail order (card-not-present)	○	○	○
Identity theft or *synthetic identity theft* used to establish new credit card accounts or to defraud existing accounts	○	○	○
Fraudulent *credentials* or other data used to establish new credit card accounts or to defraud existing accounts	○	○	○
Account takeover of customers' accounts, e.g., changes cardholders address/contact data, takeover of merchant account with card-on-file, etc.	○	○	○
Credit card used by family member or friend	○	○	○
Other, please specify ______________________________	○	○	○

Or

12b) If you do not know, please choose the response below.

Don't know	○

13a) Which of the following account application processes does your financial institution use to mitigate credit card fraud risks? For those used, please rate effectiveness. (Select one answer in each row.)

	Use & Very effective	Use & Some what effective	Use & Some what ineffective	Don't Use	Don't know
Identity verification services to help confirm the identity of the person or business during account application process	○	○	○	○	○
Credit report inquiry during credit card account application process	○	○	○	○	○
Credit underwriting review	○	○	○	○	○
Financial or tax return review	○	○	○	○	○
Collateral pledge against activity on credit card account	○	○	○	○	○
Other, please specify ____________________	○	○	○	○	○

13b) Of the methods you rated as very effective, which is the one you think is best? Only list those from 13a where “very effective” was selected. If none, skip 13b and go to 13c.

- ○ Identity verification services to help confirm the identity of the person or business during account application process
- ○ Credit report inquiry during credit card account application process
- ○ Credit underwriting review
- ○ Financial or tax return review
- ○ Collateral pledge against activity on credit card account
- ○ List response to “other, please specify” choice here

13c) Which of the following transaction authentication methods does your financial institution use to mitigate credit card fraud risks? For those used, please rate effectiveness. (Select one answer in each row.)

	Use & Very effective	Use & Some what effective	Use & Some what ineffective	Don’t Use	Don’t know
Card security code verified during transaction *authorization*, e.g., CVV2, CVC2, or CID codes	○	○	○	○	○
Card holder address verified during transaction authorization	○	○	○	○	○
Magnetic stripe *authentication*	○	○	○	○	○
Card chip *authentication*	○	○	○	○	○
PIN *authentication*	○	○	○	○	○
Out-of-band authentication for transactions identified as high risk	○	○	○	○	○
3D Secure or its equivalent for online payments	○	○	○	○	○
Other, please specify ______________________	○	○	○	○	○

13d) Of the methods you rated as very effective, which is the one you think is best? Only list those from 13c where “very effective” was selected. If none, skip 13d and go to 13e.

- ○ Card security code verified during transaction authorization, e.g., CVV2, CVC2, or CID codes
- ○ Card holder address verified during transaction authorization
- ○ Magnetic stripe authentication
- ○ Card chip authentication
- ○ PIN authentication
- ○ Out-of-band authentication for transactions identified as high risk
- ○ 3D Secure or its equivalent for online payments
- ○ List response to “other, please specify” choice here

13e) Which of the following data does your financial institution incorporate into fraud screening tools to mitigate <u>credit card</u> fraud risks? For those used, please rate effectiveness. (Select one answer in each row.)

	Use & Very effective	Use & Some what effective	Use & Some what ineffective	Don't Use	Don't know
Block or score transactions from certain countries that are perceived as high risk	○	○	○	○	○
Positive and negative lists	○	○	○	○	○
Velocity of transactions	○	○	○	○	○
Merchant category code, card acceptor ID, etc.	○	○	○	○	○
Common point of compromise, e.g., specific merchant	○	○	○	○	○
Transaction value	○	○	○	○	○
Out of pattern activity	○	○	○	○	○
Behavior analytics	○	○	○	○	○
Device *velocity* checks	○	○	○	○	○
IP address verification	○	○	○	○	○
Device finger printing	○	○	○	○	○
Other, please specify ______________________	○	○	○	○	○

13f) Of the methods you rated as very effective, which is the one you think is best? Only list those from 13e where "very effective" was selected. If none, skip 13f and go to 13g.

○ Block or score transactions from certain countries that are perceived as high risk

○ Positive and negative lists

○ Velocity of transactions

○ Merchant category code, card acceptor ID, etc.

○ Common point of compromise

○ Transaction value

○ Out of pattern activity

○ Behavior analytics

○ Device velocity checks

○ IP address verification

○ Device finger printing

○ List response to "other, please specify" choice here

13g) Which of the following <u>reporting and other risk management methods</u> does your financial institution use to mitigate <u>credit card</u> fraud risks? For those used, please rate effectiveness. (Select one answer in each row.)

	Use & Very effective	Use & Some what effective	Use & Some what ineffective	Don't Use	Don't know
Provide customers online information services to view transactions, statements, etc.	○	○	○	○	○
Provide customers online services to dispute transactions	○	○	○	○	○
Provide customers alerts via text, email, or within application	○	○	○	○	○
Allow customer to turn card off when not in use	○	○	○	○	○
Block and reissue all cards known to be on breached card list	○	○	○	○	○
Apply heightened monitoring and selectively block and reissue cards known to be on breached card list	○	○	○	○	○
Manual review of suspicious transactions	○	○	○	○	○
Outsource card fraud management (no internal tools or expertise)	○	○	○	○	○
Provide customer education and training on credit card fraud risk mitigation	○	○	○	○	○
Provide staff education and training on credit card fraud risk mitigation	○	○	○	○	○
Other, please specify _______________________	○	○	○	○	○

13h) Of the methods you rated as very effective, which is the one you think is best? Only list those from 13g where "very effective" was selected. If none, skip 13h and go to the next series.

○ Provide customers online information services to view transactions, statements, etc.

○ Provide customers online services to dispute transactions

○ Provide customers alerts via text, email, or within application

○ Allow customer to turn card off when not in use

○ Block and reissue all cards known to be on breached card list

○ Apply heightened monitoring and selectively block and reissue cards known to be on breached card list

○ Manual review of suspicious transactions

○ Outsource credit card fraud management (no internal tools or expertise)

○ Provide customer education and training on credit card fraud risk mitigation

○ Provide staff education and training on credit card fraud risk mitigation

○ List response to "other, please specify" choice here

New Demand Deposit Account or Transaction Account Ask when answer to Q5 is offer 5b or 5d or 5f or 5g or 5h.

14a) Which of the following account application processes does your financial institution use to mitigate risks when establishing new demand deposit or transaction accounts? For those used, please rate effectiveness. (Select one answer in each row.) Ask when answer to Q5 is offer on 5b or 5d or 5f or 5g or 5h.

	Use & Very effective	Use & Some what effective	Use & Some what ineffective	Don't Use	Don't know
Conduct *KYC* and *CIP* review	○	○	○	○	○
Identity verification services to help confirm the identity of the person or business	○	○	○	○	○
Financial or tax return review	○	○	○	○	○
Credit report inquiry	○	○	○	○	○
Use of positive and negative lists, e.g., NACHA originator watch list	○	○	○	○	○
New customer limited to in person submission of new account application	○	○	○	○	○
Agreements that specify minimum security requirements/procedures for online banking payment origination	○	○	○	○	○
Establish exposure limits for customer use of payment products	○	○	○	○	○
Establish prefunding requirements for customer use of payment products	○	○	○	○	○
Require a reserve of funds for return items and other claims	○	○	○	○	○
Other, please specify__________________	○	○	○	○	○

14b) Of the methods you rated as very effective, which is the one you think is best? Only list those from 14a where "very effective" was selected. If none, skip 14b and go to next section.

○ Conduct KYC and CIP review

○ Identity verification services to help confirm the identity of the person or business

○ Financial or tax return review

○ Credit report inquiry

○ Use of positive and negative lists, e.g., NACHA originator watch list

○ New customer limited to in person submission of new account application

○ Account agreement and disclosures

○ Agreements that specify with minimum security requirements/procedures for online banking payment origination

○ Establish exposure limits for customer use of payment products

○ Establish prefunding requirements for customer use of payment products

○ Require a reserve of funds for return items and other claims

○ List response to "other, please specify" choice here

Debit Cards Include debit card section, Q15 – Q16f, when the answer to question 5d is offer.

15) What are the three current fraud attacks most often used to initiate debit card fraud against your financial institution or your customers' accounts? (Select and rank the three that are most common. Choose one answer per column.)

	1st choice	2nd choice	3rd choice
Counterfeit debit cards used at point-of-sale	○	○	○
Lost or stolen debit cards used at point-of-sale	○	○	○
Counterfeit debit cards used at ATM, e.g., for cash withdrawal	○	○	○
Lost or stolen debit cards used at ATM	○	○	○
Counterfeit or stolen cards or card data used online (card-not-present)	○	○	○
Counterfeit or stolen cards or card data used in telephone or mail order (card-not-present)	○	○	○
Identity theft or *synthetic identity theft* used to establish new debit card account/demand deposit accounts or defraud existing accounts	○	○	○
Fraudulent *credentials* or other data used to establish new debit card accounts or to defraud existing accounts	○	○	○
Account takeover of customers' accounts, e.g., changes cardholders address/contact data, takeover of merchant account with card-on-file, etc.	○	○	○
Debit card used by family member or friend	○	○	○
Other, please specify _______________________________	○	○	○

Or

15b) If you do not know, please choose the response below.

Don't know	○

16a) Which of the following transaction authentication methods does your financial institution use to mitigate debit card fraud risks? For those used, please rate effectiveness. (Select one answer in each row.)

	Use & Very effective	Use & Some what effective	Use & Some what ineffective	Don't Use	Don't know
Card security code verified during transaction *authorization*, e.g., CVV2, CVC2, or CID codes	○	○	○	○	○
Card holder address verified during transaction *authorization*	○	○	○	○	○
Magnetic stripe *authentication*	○	○	○	○	○
Card chip *authentication*	○	○	○	○	○

PIN *authentication*	○	○	○	○	○
Out-of-band authentication for transactions identified as high risk	○	○	○	○	○
3D Secure or its equivalent for online payments	○	○	○	○	○
Other, please specify ______________________	○	○	○	○	○

16b) Of the methods you rated as very effective, which is the one you think is best? Only list those from 16a where "very effective" was selected. If none, skip 16b and go to 16c.

○ Card security code verified during transaction authorization, e.g., CVV2, CVC2, or CID codes

○ Card holder address verified during transaction authorization

○ Magnetic stripe authentication

○ Card chip authentication

○ PIN authentication

○ Out-of-band authentication for transactions identified as high risk

○ 3D Secure or its equivalent for online payments

○ List response to "other, please specify" choice here

16c) Which of the following data does your financial institution incorporate into fraud screening tools to mitigate debit card fraud risks? For those used, please rate effectiveness. (Select one answer in each row.)

	Use & Very effective	Use & Some what effective	Use & Some what ineffective	Don't Use	Don't know
Block or score transactions from certain countries that are perceived as high risk	○	○	○	○	○
Positive and negative lists	○	○	○	○	○
Velocity of transactions	○	○	○	○	○
Merchant category code, card acceptor ID, etc.	○	○	○	○	○
Common point of compromise, e.g., specific merchant	○	○	○	○	○
Transaction value	○	○	○	○	○
Out of pattern activity	○	○	○	○	○
Behavior analytics	○	○	○	○	○
Device *velocity* checks	○	○	○	○	○
IP address verification	○	○	○	○	○
Device finger printing	○	○	○	○	○
Other, please specify	○	○	○	○	○

16d) Of the methods you rated as very effective, which is the one you think is best? Only list those from 16c where "very effective" was selected. If none, skip 16d and go to 16e.

○ Block or score transactions from certain countries that are perceived as high risk
○ Positive and negative lists
○ Velocity of transactions
○ Merchant category code, card acceptor ID, etc.
○ Common point of compromise
○ Transaction value
○ Out of pattern activity
○ Behavior analytics
○ Device velocity checks
○ IP address verification
○ Device finger printing
○ List response to "other, please specify" choice here

16e) Which of the following reporting and other risk management methods does your financial institution use to mitigate debit card fraud risks? For those used, please rate effectiveness. (Select one answer in each row.)

	Use & Very effective	Use & Some what effective	Use & Some what ineffective	Don't Use	Don't know
Provide customers online information services to view transactions, statements, etc.	○	○	○	○	○
Provide customers online services to dispute transactions	○	○	○	○	○
Provide customers alerts via text, email, or within application	○	○	○	○	○
Allow customer to turn card off when not in use	○	○	○	○	○
Block and reissue all cards known to be on breached card list	○	○	○	○	○
Apply heightened monitoring and selectively block and reissue cards known to be on breached card list	○	○	○	○	○
Only issue non-reloadable prepaid cards include choice when 5e is offer	○	○	○	○	○
Limit load value on prepaid cards include choice when 5e is offer	○	○	○	○	○
Manual review of suspicious transactions	○	○	○	○	○
Outsource debit card fraud management (no internal tools or expertise)	○	○	○	○	○

Provide customer education and training on debit card fraud risk mitigation	○	○	○	○	○
Provide staff education and training on debit card fraud risk mitigation	○	○	○	○	○
Other, please specify ______________________	○	○	○	○	○

16f) Of the methods you rated as very effective, which is the one you think is best? Only list those from 16e where "very effective" was selected. If none, skip 16f and go to the next series.

○ Provide customers online information services to view transactions, statements, etc.

○ Provide customers online services to dispute transactions

○ Provide customers alerts via text, email, or within application

○ Allow customer to turn card off when not in use

○ Block and reissue all cards known to be on breached card list

○ Apply heightened monitoring and selectively block and reissue cards known to be on breached card list

○ Only issue non-reloadable prepaid cards

○ Limit load value on prepaid cards

○ Manual review of suspicious transactions

○ Outsource debit card fraud management (no internal tools or expertise)

○ Provide customer education and training on debit card fraud risk mitigation

○ Provide staff education and training on debit card fraud risk mitigation

○ List response to "other, please specify" choice here

Checks Include checks section, Q17 – Q18h, when the answer to question 5b is offer.

17) What are the three current fraud attacks most often used to initiate check fraud against your financial institution or your customers' accounts? (Select and rank the three that are most common. Choose one answer per column.)

	1st choice	2nd choice	3rd choice
Altered or forged checks presented for payment	○	○	○
Altered or forged checks deposited (over-the-counter, ATM, RDC, etc.)	○	○	○
Counterfeit checks presented for payment	○	○	○
Counterfeit checks deposited (over-the-counter, ATM, RDC, etc.)	○	○	○
Duplicate checks presented for payment	○	○	○
Duplicate checks deposited (over-the-counter, ATM, RDC, etc.)	○	○	○
Check kiting	○	○	○
Abuse of power of attorney to defraud vulnerable adult	○	○	○
Use of fraudulent *credentials* or other data to establish new accounts or to defraud existing accounts	○	○	○
Account takeover of customers' accounts	○	○	○

Business email compromise schemes	○	○	○
Identity theft or *synthetic identity theft* used to establish new banking/demand deposit account or to defraud existing accounts	○	○	○
Other, please specify _________________________________	○	○	○

Or

17b) If you do not know, please choose the response below.

Don't know	○

18a) Which of the following transaction authentication methods does your financial institution use to mitigate check fraud risks? For those used, please rate effectiveness.

	Use & Very effective	Use & Some what effective	Use & Some what ineffective	Don't Use	Don't know
Signature verification	○	○	○	○	○
Positive pay services	○	○	○	○	○
Payee *positive pay services*	○	○	○	○	○
Access *credentials* for remote deposit capture Include this choice when answer to 5l or 5m is offer	○	○	○	○	○
Post no check services	○	○	○	○	○
Other, please specify ______________________	○	○	○	○	○

18b) Of the methods you rated as very effective, which is the one you think is best? Only list those from 18a where "very effective" was selected. If none, skip 18b and go to 18c.

○ Signature verification

○ Positive pay services

○ Payee positive pay services

○ Access credentials for remote deposit capture

○ Post no check services

○ List response to "other, please specify" choice here

18c) Which of the following transaction fraud screening and scoring methods does your financial institution use to mitigate check fraud risks? For those used, please rate effectiveness. (Select one answer in each row.)

	Use & Very effective	Use & Some what effective	Use & Some what ineffective	Don't Use	Don't know
Shared database screen/score deposit items	○	○	○	○	○
Positive and negative lists	○	○	○	○	○
Out of pattern activity	○	○	○	○	○
Behavior analytics	○	○	○	○	○
Velocity of items deposited or paid	○	○	○	○	○
Value of items deposited or paid	○	○	○	○	○
Large dollar item review on deposited or paid items	○	○	○	○	○
Kite detection software	○	○	○	○	○
Duplicate check detection on deposit items	○	○	○	○	○
Duplicate check detection on paid items	○	○	○	○	○
Manual review	○	○	○	○	○
Other, please specify ____________________	○	○	○	○	○

18d) Of the methods you rated as very effective, which is the one you think is best? Only list those from 18c where "very effective" was selected. If none, skip 18d and go to 18e.

○ Shared database screen/score deposit items

○ Positive and negative lists

○ Out of pattern activity

○ Behavior analytics

○ Velocity of items deposited or paid

○ Value of items deposited or paid

○ Large dollar item review on deposited or paid items

○ Kite detection software

○ Duplicate check detection on deposit items

○ Duplicate check detection on paid items

○ Manual review

○ List response to "other, please specify" choice here

18e) Which of the following transaction fraud screening and scoring methods does your financial institution use to mitigate check remote deposit capture (RDC) fraud risks? For those used, please rate effectiveness. (Select one answer in each row.) Ask when Q 5l or Q5m is offer.

	Use & Very effective	Use & Some what effective	Use & Some what ineffective	Don't Use	Don't know
Velocity checks on RDC items	○	○	○	○	○
IP address verification	○	○	○	○	○
Device finger printing	○	○	○	○	○
Limit on number of RDC items deposited	○	○	○	○	○
Limit on RDC per item value	○	○	○	○	○
Limit on total RDC deposit value	○	○	○	○	○
Apply same screens/scoring methods as used in non-RDC check deposits	○	○	○	○	○
Other RDC methods, please specify ___________	○	○	○	○	○

18f) Of the methods you rated as very effective, which is the one you think is best? Only list those from 18e) where "very effective" was selected. If none, skip 18f and go to 18g.

○ Velocity checks on RDC items

○ IP address verification

○ Device finger printing

○ Limit on number of RDC items deposited

○ Limit on RDC per item value

○ Limit on total RDC deposit value

○ Apply same screens/scoring methods as used in non-RDC check deposits

○ List response to "other, please specify" choice here

18g) Which of the following reporting and other risk management methods does your financial institution use to mitigate check fraud risks? For those used, please rate effectiveness. (Select one answer in each row.)

	Use & Very effective	Use & Some what effective	Use & Some what ineffective	Don't Use	Don't know
Routinely apply standard check holds on funds availability	○	○	○	○	○
Apply exception holds on funds availability	○	○	○	○	○
Monitor customer return item rates	○	○	○	○	○
Prohibit customer/payee from creating and depositing *remotely created checks*	○	○	○	○	○

Provide customers online information services to view check images, statements, etc.	○	○	○	○	○
Provide customers alerts via text, email, or within application	○	○	○	○	○
Submit data to *shared database* and receive alerts	○	○	○	○	○
Provide customer education and training on check fraud risk mitigation	○	○	○	○	○
Provide staff education and training on check fraud risk mitigation	○	○	○	○	○
Other, please specify________________________	○	○	○	○	○

18h) Of the methods you rated as very effective, which is the one you think is best? Only list those from 18g where "very effective" was selected. If none, skip 18h and go to the next section.

○ Routinely apply standard check holds on funds availability

○ Apply exception holds on funds availability

○ Monitor customer return item rates

○ Prohibit customer/payee from creating and depositing remotely created checks

○ Provide customers online information services to view check images, statements, etc.

○ Provide customers alerts via text, email, or within application

○ Submit data to shared database and receive alerts

○ Provide customer education and training on check fraud risk mitigation

○ Provide staff education and training on check fraud risk mitigation

○ List response to "other, please specify" choice here

ACH Include ACH section, Q19 – Q20f, when the answer to question 5f or 5g is offer.

19) What are the three current fraud attacks most often used to initiate ACH fraud against your financial institution or your customers' accounts? (Select and rank the three that are most common. Choose one answer per column.)

	1st choice	2nd choice	3rd choice
Fraudulent or unauthorized ACH debits against consumer accounts	○	○	○
Fraudulent or unauthorized ACH debits against business accounts	○	○	○
Use of fraudulent *credentials* or other data to defraud existing accounts	○	○	○
Account takeover of customers' accounts	○	○	○
Business email compromise schemes	○	○	○
Originator company employee frauds, e.g., payroll, invoice payment	○	○	○
Insider fraud	○	○	○
Identity theft or *synthetic identity* theft used to defraud existing accounts	○	○	○
Abuse of power of attorney to defraud vulnerable adult	○	○	○
Other, please specify ________________________________	○	○	○

Or

19b) If you do not know, please choose the response below.

Don't know	○

20a) Which of the following ACH originator/sender authentication methods does your financial institution use to mitigate ACH fraud risks? For those used, please rate effectiveness. (Select one answer in each row.) Ask Q20a when FI answer to ACH origination Q5f or Q5g is offer. If Q5f and Q5g are blank, go to 20c.

	Use & Very effective	Use & Some what effective	Use & Some what ineffective	Don't Use	Don't know
Out of band authentication with originating company/*third party* sender (ask when Q5f is offer)	○	○	○	○	○
Multi-factor authentication with originating company/*third party* sender (ask when Q5f is offer)	○	○	○	○	○
Multi-factor authentication for consumer billpay (ask when Q5j is offer)	○	○	○	○	○
ID and Password for consumer billpay (ask when Q5j is offer)	○	○	○	○	○
Evaluate new credential requests for originator before issuing (ask when Q5f or Q5fg is offer)	○	○	○	○	○
IP address verification (ask when Q5f or Q5fg is offer)	○	○	○	○	○
Dual control for originating company file initiation (ask when Q5f is offer)	○	○	○	○	○
Other, please specify ____________________	○	○	○	○	○

20b) Of the methods you rated as very effective, which is the one you think is best? Only list those from 20a) where "very effective" was selected. If none, skip 20b and go to 20c.

○ Out of band authentication with originating company/third party sender

○ Multi-factor authentication with originating company/third party sender

○ Multi-factor authentication for consumer billpay

○ ID and Password for consumer billpay

○ Evaluate new credential requests for originator before issuing

○ IP address verification

○ Dual control for originating company file initiation

○ List response to "other, please specify" choice here

20c) Which of the following transaction fraud screening and scoring methods does your financial institution use to mitigate ACH fraud risks? For those used, please rate effectiveness. (Select one answer in each row.) Ask this section when FI offers ACH 5f or 5g

	Use & Very effective	Use & Some what effective	Use & Some what ineffective	Don't Use	Don't know
Shared database to screen/score ACH debits received	○	○	○	○	○
Velocity of ACH transactions	○	○	○	○	○
Transaction value	○	○	○	○	○
Out of pattern activity	○	○	○	○	○
Rules based fraud detection	○	○	○	○	○
Anomaly/behavior analytics	○	○	○	○	○
ACH filters/positive pay services	○	○	○	○	○
ACH block services	○	○	○	○	○
Suspend originated files exceeding exposure limits	○	○	○	○	○
OFAC monitoring	○	○	○	○	○
Manual review	○	○	○	○	○
Other, please specify	○	○	○	○	○

20d) Of the methods you rated as very effective, which is the one you think is best? Only list those from 20c) where "very effective" was selected. If none, skip 20d and go to 20e.

○ Shared database to screen/score ACH debits received
○ Velocity of ACH transactions
○ Transaction value
○ Out of pattern activity
○ Rules based fraud detection
○ Anomaly/behavior analytics
○ ACH filters/positive pay services
○ ACH block services
○ Suspend originated files exceeding exposure limits
○ OFAC monitoring
○ Manual review
○ List response to "other, please specify" choice here

20e) Which of the following reporting and other risk management methods does your financial institution use to mitigate ACH fraud risks? For those used, please rate effectiveness. (Select one answer in each row.)

	Use & Very effective	Use & Some what effective	Use & Some what ineffective	Don't Use	Don't know
Provide ACH originator alerts, e.g., notice of new payee added	○	○	○	○	○
Provide ACH receiver alerts, e.g., ACH debit alerts	○	○	○	○	○
Provide ACH originator services to establish batch-level thresholds to hold batches for added authorizations if thresholds hit. Threshold can be dollars, volume, date, etc.	○	○	○	○	○
Provide customers alerts via text, email, or within application	○	○	○	○	○
Monitor customer return item rates	○	○	○	○	○
Provide customers online information services to view transactions, statements, etc.	○	○	○	○	○
Provide customers online services to dispute transactions	○	○	○	○	○
Limit ACH origination to domestic transactions Ask when answer to 5f is offer	○	○	○	○	○
Provide account masking services	○	○	○	○	○
Outsource ACH processing and risk management	○	○	○	○	○
Provide customer education and training on ACH fraud risk mitigation	○	○	○	○	○
Provide staff education and training on ACH fraud risk mitigation	○	○	○	○	○
Established procedures for identifying *money mule* accounts	○	○	○	○	○
Funds availability delay when reasonably suspect ACH credit received is unauthorized	○	○	○	○	○
Other, please specify ______________________	○	○	○	○	○

20f) Of the methods you rated as very effective, which is the one you think is best? Only list those from 20e where "very effective" was selected. If none, skip 20f and go next section.

○ Funds availability delay when reasonably suspect ACH credit received is unauthorized

○ Provide ACH originator alerts, e.g., notice of new payee added

○ Provide ACH originator services to establish batch-level thresholds to hold batches for added authorizations if thresholds hit. Threshold can be dollars, volume, date, etc.

○ Provide ACH receiver alerts, e.g., ACH debit alerts

○ Provide customers alerts via text, email, or within application

○ Monitor customer return item rates

○ Provide customers online information services to view transactions, statements, etc.

○ Provide customers online services to dispute transactions

○ Limit ACH origination to domestic transactions

○ Provide account masking services

○ Outsource ACH processing and risk management

○ Provide customer education and training on ACH fraud risk mitigation

○ Provide staff education and training on ACH fraud risk mitigation

○ Established procedures for identifying *money mule* accounts

○ List response to "other, please specify" choice here

Wire Include Wire section, Q21 – Q22f when the answer to question 5h is offer.

21) What are the three current fraud attacks most often used to initiate wire fraud against your financial institution or your customers' accounts? (Select and rank the three that are most common. Choose one answer per column.)

	1st choice	2nd choice	3rd choice
Account takeover of customers' accounts	○	○	○
Business email compromise schemes	○	○	○
Originator company employee frauds, e.g., invoice payment	○	○	○
Use of fraudulent *credentials* or other data to defraud existing accounts	○	○	○
Insider fraud	○	○	○
Identity theft or synthetic identity theft used to defraud existing accounts	○	○	○
Consumer victim frauds, e.g., advance payment schemes	○	○	○
Abuse of power of attorney to defraud vulnerable adult	○	○	○
Other, please specify ________________________________	○	○	○

21b) If you do not know, please choose the response below.

Don't know	○

22a) Which of the following transaction authentication methods does your financial institution use to mitigate wire fraud risks? For those used, please rate effectiveness. (Select one answer in each row.)

	Use & Very effective	Use & Some what effective	Use & Some what ineffective	Don't Use	Don't know
Out of band authentication with originating company	○	○	○	○	○
Multi-factor authentication with originating company	○	○	○	○	○
Signature verification	○	○	○	○	○
Telephone callback verification	○	○	○	○	○
Evaluate new credential requests for originator before issuing	○	○	○	○	○
IP address verification	○	○	○	○	○
Device finger printing	○	○	○	○	○
Dual control/approval for originating company wire initiation	○	○	○	○	○
Limit consumer initiated wires to in person requests with valid government issued ID	○	○	○	○	○
Other, please specify ______________________	○	○	○	○	○

22b) Of the methods you rated as very effective, which is the one you think is best? Only list those from 22a) where "very effective" was selected. If none, skip 22b and go to 22c.

○ Out of band authentication with originating company

○ Multi-factor authentication with originating company

○ Signature verification

○ Telephone callback verification

○ Evaluate new credential requests for originator before issuing

○ IP address verification

○ Device finger printing

○ Dual control/approval for originating company wire initiation

○ Limit consumer initiated wires to in person requests with valid government issued ID

○ List response to "other, please specify" choice here

22c) Which of the following transaction fraud screening and scoring methods does your financial institution use to mitigate wire fraud risks? For those used, please rate effectiveness. (Select one answer in each row.)

	Use & Very effective	Use & Some what effective	Use & Some what ineffective	Don’t Use	Don’t know
Velocity of wire transactions	○	○	○	○	○
Transaction value	○	○	○	○	○
Out of pattern activity	○	○	○	○	○
Rules based fraud detection	○	○	○	○	○
Anomaly/behavior analytics	○	○	○	○	○
Suspend originated wires exceeding exposure limits	○	○	○	○	○
OFAC monitoring	○	○	○	○	○
Manual review	○	○	○	○	○
Other, please specify ______________________	○	○	○	○	○

22d) Of the methods you rated as very effective, which is the one you think is best? Only list those from 22c where “very effective” was selected. If none, skip 22d and go to 22e.

○ Velocity of wire transactions

○ Transaction value

○ Out of pattern activity

○ Rules based fraud detection

○ Anomaly/behavior analytics

○ Suspend originated wires exceeding exposure limits

○ OFAC monitoring

○ Manual review

○ List response to “other, please specify” choice here

22e) Which of the following reporting and other risk management methods does your financial institution use to mitigate wire fraud risks? For those used, please rate effectiveness. (Select one answer in each row.)

	Use & Very effective	Use & Some what effective	Use & Some what ineffective	Don’t Use	Don’t know
Provide customers online information services to view transactions, statements, etc.	○	○	○	○	○
Provide customers online services to dispute transactions	○	○	○	○	○
Provide customers alerts via text, email, or	○	○	○	○	○

within application					
Provide recurring wire templates to wire originators with role based security for changes	○	○	○	○	○
Limit wire origination to domestic transactions	○	○	○	○	○
Complete standard list of questions with consumer initiated wires, e.g., source of funds, relationship to receiver, purpose of payment, etc.	○	○	○	○	○
Refuse to send consumer initiated wire when suspect fraud scheme	○	○	○	○	○
Outsource wire processing and risk management	○	○	○	○	○
Provide customer education and training on wire fraud risk mitigation	○	○	○	○	○
Provide staff education and training on wire fraud risk mitigation	○	○	○	○	○
Established procedures for identifying *money mule* accounts	○	○	○	○	○
Funds availability delay when reasonably suspect wire received is unauthorized	○	○	○	○	○
Other, please specify _______________________	○	○	○	○	○

22f) Of the methods you rated as very effective, which is the one you think is best? Only list those from 22e where "very effective" was selected. If none, skip 22f and go to next section.

○ Provide customers online information services to view transactions, statements, etc.

○ Provide customers online services to dispute transactions

○ Provide customers alerts via text, email, or within application

○ Provide recurring wire templates to wire originators with role based security for changes

○ Limit wire origination to domestic transactions

○ Complete standard list of questions with consumer initiated wires, e.g., source of funds, relationship to receiver, purpose of payment, etc.

○ Refuse to send consumer initiated wire when suspect fraud scheme

○ Outsource wire processing and risk management

○ Provide customer education and training on wire fraud risk mitigation

○ Provide staff education and training on wire fraud risk mitigation

○ Established procedures for identifying *money mule* accounts

○ Funds availability delay when reasonably suspect wire received is unauthorized

○ List response to "other, please specify" choice here

Internal Controls and Procedures

23a) Which of the following internal controls and procedures does your financial institution currently use to mitigate fraud risks? For those used, please rate effectiveness. (Select one answer in each row.)

	Use & Very effective	Use & Some what effective	Use & Some what ineffective	Don't Use	Don't know
Physical access controls to payment processing functions	○	○	○	○	○
Logical access controls to your computing network and payment processing applications	○	○	○	○	○
Dedicated computer used to conduct transactions with payments network operator, correspondent bank, or financial service provider	○	○	○	○	○
Authentication and authorization controls to payment processes	○	○	○	○	○
Restrict or limit employee use of Internet from financial institution's network	○	○	○	○	○
Dual controls and segregation of duties within payment initiation and receipt processes	○	○	○	○	○
Transaction/file approval limits	○	○	○	○	○
Address exception items timely, e.g., meet deadlines for chargebacks, returning payments, etc.	○	○	○	○	○
Prohibit use of personal devices for processing of financial institution's payment transactions	○	○	○	○	○
Other, please specify ____________	○	○	○	○	○

23b) Of the methods you rated as very effective, which is the one you think is best? Only list those from 23a where "very effective" was selected. If none, skip 23b and go to Q24.

○ Physical access controls to payment processing functions

○ Logical access controls to your computing network and payment processing applications

○ Dedicated computer used to conduct transactions with payments network operator, correspondent bank, or financial service provider

○ Authentication and authorization controls to payment processes

○ Restrict or limit employee use of Internet from financial institution's network

○ Dual controls and segregation of duties within payment initiation and receipt processes

○ Transaction/file approval limits

○ Address exception items timely, e.g., meet deadlines for chargebacks, returning payments, etc.

○ Prohibit use of personal devices for processing of financial institution's payment transactions

○ List response to "other, please specify" choice here

Opportunities and Barriers

24) What are the main barriers to mitigate payments fraud that your financial institution experiences? (For each payment type, select all that you consider to be the main barriers.)

	All Payment Types	ACH	Checks	Credit Cards	Debit Cards	Wires
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 fraud detection tool/method	□	□	□	□	□	□
Lack of staff resources	□	□	□	□	□	□
Availability of tools needed to mitigate fraud	□	□	□	□	□	□
Access to information-sharing on emerging fraud tactics and ways to mitigate associated risks	□	□	□	□	□	□
Other, please specify ______________________	□	□	□	□	□	□

25) From your financial institution's perspective, what new or improved methods are most needed to reduce payments fraud? Please describe____

26) Is there anything else that you would like to share as part of this survey? ______________________________

If we have questions about your survey responses, staff from the Federal Reserve Bank of Minneapolis Payments, Standards, and Outreach Group may call you. Please provide your telephone number (___)____-____________

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.