► Example 2: Your accountholder claimed her credit card was stolen and used to purchase a $500 TV in an electronics store. After an investigation by your institution, it was determined that this purchase was in fact made by your accountholder on her card. Since this is an example of first-party fraud (false claim of fraud), do not include this transaction in item **9**.

➲ Third-party fraudulent general-purpose credit card network transactions = Person-present transactions (item **9.a**) + Remote transactions (item **9.b**).

9.a) Person-present transactions

Only third-party fraudulent credit card transactions for which the card user was physically present along with the card at the point of sale, including POS transactions, NFC transactions, MST transactions, manually entered transactions, RFID transactions, QR code transactions, or barcode transactions. Include all third-party unauthorized credit card transactions, before any recoveries or chargebacks. Please report any fraudulent third-party credit card transactions regardless of whether or not the transaction resulted in a loss of funds. Please report the total transactions for digital wallet authentication (item **9.a.1**), EMV chip card authentication (item **9.a.2**), magnetic stripe authentication (item **9.a.3),** and all other authentication methods including keyed in transactions, RFID, manual imprint, etc. (item **9.a.4**).

If the fraudulent transaction is authorized via PIN, please report this volume under EMV chip card authentication (item **9.a.2**) if the card has a chip, or under magnetic stripe authentication (item **9.a.3**) if the card doesn't have a chip.

Include:

- Fraudulent transactions for which the card user is present
- Fraudulent mobile transactions at the point of sale (e.g., digital wallet transactions at the point of sale using near field communication, magnetic secure transmission, QR codes, or barcode technology)
- Fraudulent intermediated transactions at the point of sale (e.g., Square, Clover, iZettle, etc.)
- Fraudulent card-not-present transactions for which the card user is present at the point of sale (e.g., key-entered transactions)

Do not include:

- Fraudulent remote transactions
- Fraudulent digital wallet in-app or browser transactions
- Fraud prevented by declining a transaction
- Fraud committed by a valid card user (first-party fraud)

► Example 1: Your accountholder's credit card was stolen. The perpetrator used the card and made two purchases totaling $1,000 over the internet. He then proceeded to buy lunch for $35 at a restaurant using the stolen card. For this question, please report 1 transactions for $35. The internet transactions should be reported in item **9.b.**

► Example 2: Jane is a credit card accountholder at your institution. She is an active and good standing customer. She consistently pays off her credit card balance on time and has never maxed out her credit limit. Over time her credit limit increased to $10,000. After losing her job, she maxed out her limit and misses a payment. Eventually, she decides not to pay off any part of her outstanding balance. This is an example of first-party fraud, do not include any of these transaction in item **9.a**.

9.b) Remote transactions

Only third-party fraudulent credit card transactions for which the card user did not physically present the card to authorize the transaction. Include all third-party unauthorized credit card transactions, before any recoveries or chargebacks. Please report any fraudulent third-party credit card transactions regardless of whether or not the transaction resulted in a loss of funds. Please report the total transactions for digital wallet authentication (item **9.b.1**), manually entered online authentication (item **9.b.2**), and all other authentication methods including phone orders, mail orders, etc. (item **9.b.3**).

Include:

- Fraudulent mail-order transactions, telephone-order transactions, internet transactions, in-app transactions, or digital-wallet in-app transactions

Do not include:

- Fraudulent person-present transactions
- Fraud prevented by declining a transaction
- Fraud committed by a valid card user (first-party fraud)

► Example: Your accountholder's credit card was stolen. The perpetrator used the card and purchased a TV for $500 at a store by fraudulently signing the receipt. He then proceeded to use the stolen card to buy an item online for $250. For this question, please report 1 transaction for $250. The in-store transaction for $500 should be reported in item **9.a.**

► Example 2: Your accountholder claimed his credit card was stolen and used to purchase a $20 video game online. After an investigation by your institution, it was determined that this purchase was in fact made by your accountholder on his card. Since this is an example of first-party fraud (false claim of fraud), do not include this transaction in item **9.b**.

10) Third-party fraudulent general-purpose credit card network transactions

Repeat item **9** from above. All third-party unauthorized credit card transactions, before any recoveries or chargebacks, for which your institution was the card issuer. Please report any fraudulent third-party credit card transactions regardless of whether or not the transaction resulted in a loss of funds.

Include:

- Credit card transactions that were not authorized by a valid card user (third-party fraud)

Do not include:

- Fraud prevented by declining a transaction
- Fraud committed by a valid card user (first-party fraud)
- Fraudulent debit card transaction
- Fraudulent prepaid card transaction
- Fraudulent ATM withdrawals
- Credit card transactions authorized by a valid card user as part of a scam
- Fraudulent Cash advances

► Example 1: Your credit card accountholder's credit card was stolen. The perpetrator used the card and made $500 worth of one –time purchase. For this questions, please report one 1 transaction for $500.

► Example 2: Your accountholder claimed her credit card was stolen and used to purchase a $500 TV in an electronics store. After an investigation by your institution, it was determined that this purchase was in fact made by your accountholder on her card. Since this is an example of first-party fraud (false claim of fraud), do not include this transaction in item **10**.

➲ Third-party fraudulent general-purpose credit card network transactions = Digital wallet transactions (item **10.a**) + Non-digital wallet transactions (item **10.b**).

10.a) Digital wallet transactions

Only third-party fraudulent credit card transactions made via a digital wallet (e.g., Apple Pay, Android Pay, Samsung Pay, PayPal Mobile, etc.), this can include purchasing items on-line with a computer, using a smartphone to purchase something at a store (NFC, MST, QR code, and barcode transactions), or in-app. Include all third-party unauthorized credit card transactions, before any recoveries or chargebacks. Please report any fraudulent third-party credit card transactions regardless of whether or not the transaction resulted in a loss of funds.

Include:

- Fraudulent digital wallet transactions at the point of sale (e.g., near field communication, magnetic secure transmission, QR codes, or barcode technology)
- Fraudulent digital wallet browser transactions or in-app transactions

Do not include:

- Fraudulent non-digital wallet transactions
- Fraud prevented by declining a transaction
- Fraud committed by a valid card user (first-party fraud)

► Example 1: Your accountholder's smartphone was stolen. The perpetrator was able to hack into the phone and make a $150 in-app purchase with the digital wallet installed in the smartphone, charging the purchase to the credit card. For this question, please report 1 transaction for $150.

► Example 2: Your accountholder claimed his smartphone was stolen and used to make a $400 in-app purchase with the digital wallet installed in the smartphone, charging the purchase to his credit card. After an investigation by your institution, it was determined that this purchase was in fact made by your accountholder on his card. Since this is an example of first-party fraud, do not include this transaction in item **10.a**.

10.b) Non-digital wallet transactions

Only non-digital wallet general-purpose credit card transactions that were not authorized by your institution's accountholders (third-party fraud). Include all third-party unauthorized credit card transactions, before any recoveries or chargebacks. Please report any fraudulent third-party non-digital wallet credit transactions regardless of whether or not the transaction resulted in a loss of funds.

Include:

- Fraudulent mail-order transactions, telephone-order transactions, internet transactions, EMV transactions, and magnetic stripe transactions

Do not include:

- Fraudulent digital wallet transactions
- Fraud prevented by declining a transaction
- Fraud committed by a valid card user (first-party fraud)

► Example 1: Your accountholder's wallet was stolen while commuting to work. Later that day, the perpetrator made an internet purchase for $325 using your accountholder's credit card. He then proceeded to use the stolen card to buy lunch for $25. For this question, please report 2 transactions for $350.

► Example 2: Mark is a credit card accountholder at your institution. He is an active and good standing customer. He consistently pays off his credit card balance on time and has never maxed out his credit limit. One year after opening his account, he maxes out his credit limit and starts missing payments. After your institution tries to collect payments from Mark, it is discovered that his identity was falsified (synthetic ID). This is an example of first-party fraud (bust-out fraud with synthetic ID), do not include any of these transaction in item **10.b**.

Cash

GENERAL TERMINOLOGY

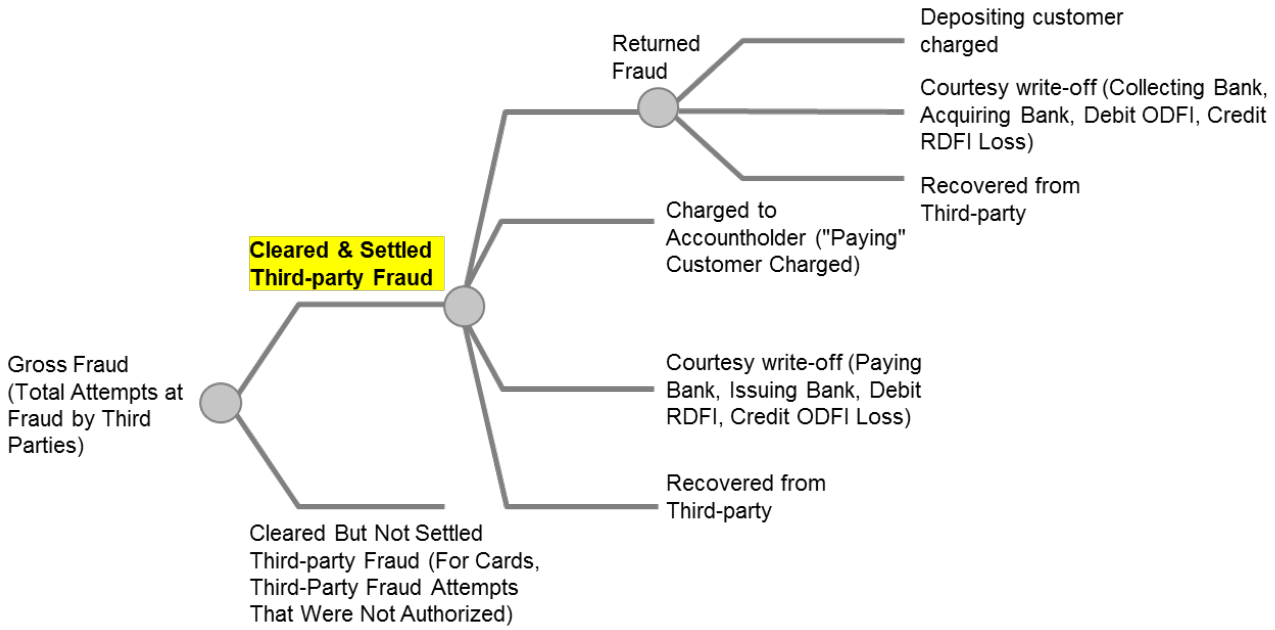
Cash withdrawals –
Cash withdrawals made by your accountholders at your ATMs, "foreign" ATMs, wholesale vaults, over-the-counter, or from remote currency management terminals (RCMTs). For this study, please follow these guidelines:

Cash withdrawals include…	Cash Withdrawals do not include…
▪ All cash withdrawals by your accountholders (including, as appropriate for the particular survey question, withdrawals made in other countries) ▪ All notes and coin ▪ Credit card cash advances	▪ Cash withdrawals or other transactions by individuals or businesses other than your accountholders ▪ Deposit transactions ▪ Inquiries ▪ Funds transfers ▪ Statement prints ▪ Purchases (e.g., stamps, tickets) ▪ Any other non-withdrawal transactions

Remote currency management terminal (RCMT) –
A cash accepting (or recycling) terminal deployed by your institution at a commercial customer's site (e.g., restaurants, gas stations, convenience stores) to allow that customer to deposit cash remotely, typically with provisional ledger credit, without visiting a bank branch, cash vault, or requiring pick-up by an armored courier.

Cash advances –
A service provided by credit card and charge card issuers that allows cardholders to withdraw cash, either through an ATM or over the counter at a bank or other financial agency, up to a prescribed limit. For a credit card, this will be the credit limit (or some percentage thereof). It also includes convenience checks drawn on a credit card account and balance transfers.

Third-party fraud –
The Federal Reserve Payments Study has identified a measure of fraud that can be described as cleared and settled third-party fraud transactions. It is not a loss of funds measure, nor is it a measure of fraud attempts. It is a measure of the extent that third-parties not authorized to conduct transactions are able to penetrate the system and effect settlement between banks, or create a book transfer of funds if it happens within an institution. The definition includes third-party fraud with all types of outcomes that may or may not include a loss to various entities, but constitutes a fraud attempt that manage to create funds transfer, if only temporary. The definition is depicted below within the hierarchy of fraud attempts visible to your institution. The definition of fraud in this study is highlighted in yellow to show that cleared and settled third-party fraud includes at least six different categories of fraud outcomes.



Cash Withdrawals

SURVEY ITEMS

1) Did your institution outsource vault operations during calendar year 2016? If your answer is "No," please skip item 1.a below.

► Example: Your corporate customer is located in a state where your institution does not have a physical presence. To provide vault services to this customer, your institution outsources these services to an armored cash handling services company.

1.a) If your answer is "Yes" to item 2 above, are you able to report outsourced vault operations volumes?

Note: If your answer to this question is **No**, please report **NR** for item **5.b** below. If your answer is **Yes, in some cases**, please explain in the comments box at the end of the page in the questionnaire.

2) Did your institution offer remote currency management terminals (RCMTs) or "smart safes" to your merchant customers during calendar year 2016?

Note: If your answer to this question is **Yes**, please report these volumes for item **5.b** below.

3) Did your institution use cash recyclers at your teller window in order to process cash deposits or withdrawals during calendar year 2016?

Note: If your answer to this question is **Yes**, please include in volumes in item **5.b**.

4) Did your institution take part in a branch-sharing agreement during calendar year 2016?

Note: If your answer is **Yes**, please be sure to include only your portion of cash withdrawals in the volumes you report below.

5) Total cash withdrawals by your institution's accountholders

Total cash withdrawals made from accounts at your institution.

Include:

- Cash withdrawals from deposit, prepaid, and credit card program accounts
- Cash withdrawals at ATMs
- Cash withdrawals that were made over the counter at your institution's branches
- Cash orders at wholesale vaults
- Cash withdrawals at RCMTs
- Cash advances from credit cards

➲ Total cash withdrawals = Total ATM cash withdrawals (item **5.a**) + Non-ATM cash withdrawals (item **5.b**)

5.a) Total ATM cash withdrawals (your institution's accountholder, any ATM)

All cash withdrawals made from accounts at your institution from any ATM, including those at your institution's ATM terminals or "foreign" ATMs. A "foreign" ATM is an ATM operated by an unaffiliated depository institution or ATM operator that is not sponsored by your institution.

Include:

- Your institution's prepaid and debit card accountholder's ATM cash withdrawals at any ATM
- Cash advances from credit cards at ATM terminals

Do not include:

- Withdrawals at your institution's ATMs that were made by another institution's accountholders
- Deposit transactions
- RCMT withdrawals, teller vault activity, or other non-withdrawal transactions (e.g., inquiries, statement print-outs, purchases of stamps, tickets)

Note: Please count only cash withdrawals made from accounts at your institution at any ATM.

► Example: Glen is a checking accountholder at your institution and Jennifer is not. Glen withdrew $100 cash from his checking account using your ATM on Monday and $200 using another institution's ATM on Friday. Jennifer withdrew $400 from your ATM on Tuesday. For this question, please report 2 ATM withdrawals for a total of $300.

➲ Total ATM cash withdrawals = On-us ATM withdrawals (item **5.a.1**) + Foreign ATM withdrawals (item **5.a.2**).

5.a.1) On-us ATM withdrawals (your institution's accountholder, your institution's ATM)

All cash withdrawals made from accounts at your institution at your institution's ATM terminals. Include withdrawals made from accounts at your institution at fee-free ATM networks in which your institution participates.

Include

- Your institution's prepaid, debit, and credit card accountholder's ATM cash withdrawals at your institution's ATM (include cash advances from credit card accountholders)

Do not include:

- Withdrawals made from accounts at another institution
- Withdrawals made from accounts at your institution at "foreign" ATMs
- Non-withdrawal transactions made from accounts at your institution

Note: Please count only withdrawals made from accounts at your institution at your institution's ATM terminals.

► Example: Your customer used her Visa Check card to withdraw $200 from an ATM located in a grocery store but owned and operated by your institution. Please report 1 transaction for $200.

5.a.2) "Foreign" ATM withdrawals (your institution's accountholder, "foreign" ATM). A "foreign" ATM is any ATM not owned or operated by your institution

All cash withdrawals made at another institution's ATMs from accounts at your institution.

Include:

- Your institution's prepaid, debit, and credit card accountholder's ATM cash withdrawals at a "foreign" ATM (include cash advances from credit card accountholders)

Do not include:

- Any transactions at your institution's ATM terminals, regardless of the location of an account
- Over-the-counter cash withdrawals
- Non-withdrawal transactions

Note: Please count only withdrawals made from accounts at your institution at ATM terminals operated by other depository institutions or ATM operators that are not sponsored by your institution.

► Example: Your customer used her Visa Check card to withdraw $50 from an ATM located in a grocery store and owned and operated by another institution. Please report 1 transaction for $50.

5.b) Non-ATM cash withdrawals (your institution's accountholders)

All non-ATM cash withdrawals made from accounts at your institution, including those made at your institution or at another institution.

Include:

- Over-the-counter cash withdrawals; all cash withdrawal transactions made from accounts at your institution over the counter at a branch location
- Cash orders at wholesale vaults; all cash withdrawals made at wholesale vaults from accounts at your institution including those made out of outsourced vaults
- Cash withdrawals made at remote currency management terminals (RCMTs); All cash withdrawals made at remote currency management terminals, i.e., "smart safes" and "cash recyclers," that were deployed by your institution and resided at a client site (e.g., gas station, restaurant)
- Cash advances from credit cards not from ATMs

Do not include:

- Cash withdrawals at ATM terminals
- Withdrawals at your institution that were made by another institution's accountholders
- Deposit transactions
- Teller vault activity or other non-withdrawal transactions (e.g., inquiries, statement print-outs, purchases of stamps, tickets)
- Transactions that involved armored couriers or tellers withdrawing cash from RMCTs for the purpose of non-customer withdrawals

► **Example 1:** Your accountholder deposits a $100 check by providing it to teller at one of your institution's branch locations. She requests $25 cash back. Report 1 withdrawal for $25.

► **Example 2:** A local retailer for which your institution provides banking services used an armored courier service to deposit $5,000 in cash and coin at your cash vault. The retailer also ordered $1,500 in various denominations of cash straps and coin rolls in order to make change in its store(s). For this question, please include 1 cash order for $1,500.

► **Example 3:** Your customer, a gas station, has installed a cash recycler provided by your institution at one of its stores. In the evening, a gas station clerk deposited $500 in the cash recycler. The next morning, another clerk withdrew $1,000 from the same recycler. For this question, please report 1 withdrawal for $1,000.

6) Total cash withdrawals by your institution's accountholders

Repeat item **5** from above. Total cash withdrawals made from accounts at your institution.

Include:

- Cash withdrawals from both deposit, prepaid, and credit card program accounts
- Cash withdrawals at ATMs
- Cash withdrawals that were made over the counter at your institution's branches
- Cash orders at wholesale vaults
- Cash withdrawals at RCMTs
- Cash advances from credit cards

➲ Total cash withdrawals by your institution's accountholders = Cash withdrawals from deposit accounts (item **6a**) + Cash withdrawals from prepaid card program accounts (item **6b**) + Cash withdrawals from credit cards (item **6c**)

6.a) Cash withdrawals from deposit accounts

All cash withdrawals from consumer and business/government deposit accounts at your institution.

Do not include:

- Cash withdrawals from prepaid card program accounts
- Cash advances from credit cards

► Example: Your checking accountholder withdrew $100 in cash from an ATM using her debit card. Later that day she also withdrew $200 in cash over the counter from one of your bank branches. Please report 2 transactions for $300.

6.b) Cash withdrawals from prepaid card program accounts

All cash withdrawals from prepaid card program accounts at your institution.

Do not include:

- Cash withdrawals from deposit accounts
- Cash advances from credit cards

► Example: Your accountholder withdrew $60 in cash at an ATM using a Visa branded gift card issued by your institution. Please report 1 transaction for $60.

6.c) Cash withdrawals from credit cards (cash advances)

All cash withdrawals from credit card accounts at your institution (credit cards issued by your institution).

Do not include:

- Cash withdrawals from deposit or prepaid accounts

► Example: Your accountholder withdrew $70 in cash at an ATM using a Visa credit card issued by your institution. Please report 1 transaction for $70.

7) Third-party fraudulent ATM cash withdrawals (your institution's accountholder, any ATM)

All ATM cash withdrawals that were not authorized by your institution's accountholders (third-party fraud). Please report any third-party fraudulent ATM cash withdrawals regardless of whether or not those funds were subsequently recovered.

Do not include:

- Fraud committed by a valid accountholder (first-party fraud)
- Fraudulent withdrawals at your institution's ATMs that were made by another institution's accountholders
- Deposit transactions
- Unauthorized non-withdrawal transactions at an ATM

► Example 1: Your accountholder's debit card was stolen by a perpetrator who watched her enter her PIN at the point-of-sale. The perpetrator used the card and PIN and made a one-time $200 ATM withdrawal. For this question, please report 1 transaction for $200.

► Example 2: Your accountholder claimed her debit card was stolen by a perpetrator and was used to withdraw $100 from an ATM. However, after an investigation conducted by your institution this was determined to be a false claim, and this money was actually withdrawn by your accountholder. Since this is an example of first-party fraud (false claim of fraud), do not include this transaction in item **7.**

Cards with ATM access

8) Total number of general purpose cards with ATM access

Include both typical ATM and ATM-only cards with ATM access.

For **cards in force**, report credit, debit, and prepaid cards with access to withdrawal money from ATMs, which had been issued by your institution, activated by your institution's accountholders, and had not expired at the end of the time period.

For **cards in force with ATM withdrawal activity**, report credit, debit, and prepaid cards with access to withdrawal money from ATMs, which had been issued by your institution, and had at least one ATM withdrawal activity during the time period.
Please report the average of the end-of-month totals for 2016 for debit cards (item **8.a**), prepaid cards (item **8.b**), and credit cards with ATM access (item **8.c**).

Note: Average of monthly totals means the average of end-of-month totals for each of the months in 2016.

Include:

- Debit, Prepaid, and Credit cards with ATM access

Do not include:

- Signature-only debit, prepaid, or credit cards (i.e., debit or prepaid cards that can only be used at the point-of-sale to make purchases by signing for the transaction)
- Debit, prepaid, or credit cards issued by an unaffiliated depository institution.

► Example 1: Your institution issued 1,000 debit cards to your customers. Of those 1,000 cards, 950 cards were activated and 750 were used to withdraw cash from ATMs. For this question, please report 950 cards in force with ATM access, and 750 cards in force with ATM withdrawal activity.

► Example 2: Your institution issued 1,000 prepaid cards to your customers. Of those 1,000 cards only 500 of them have the ability withdraw money from ATMs (reloadable prepaid cards). 450 of the 500 prepaid cards were used to withdraw cash from ATMs during 2016. For this question, please report 500 cards in force with ATM access, and 450 cards in force with ATM withdrawal activity.

➲ Total number of general purpose cards with ATM access = Number of general-purpose debit cards with ATM access (item **8a**) + Number of general-purpose prepaid cards with ATM access (item **8b**) + Number of general-purpose credit cards with ATM access (item **8c**)

Alternative Payment Initiation Methods

SURVEY ITEMS

1) Did your institution offer online or mobile consumer bill payments during calendar year 2016?

Include:

- All online and mobile bill payment transactions paid from consumer accounts at your institution and initiated via your institution's website or mobile application

Do not include:

- Payments made through the biller's website

Note: If your answer to this question is **No**, please report "0" for item **2** below.

► Example: Your accountholder paid his utility bill through his PC by initiating a payment from his account via your institution's website. Another accountholder paid his rent by initiating a payment from his account via your institution's website using his smartphone. A third accountholder paid his rent by initiated a payment via your institution's mobile application rather than your institution's website. Any one of these examples would result in a **Yes** response to this question.

2) Total online or mobile bill payment transactions initiated by your institution's consumer accountholders

All online and mobile bill payment transactions paid from consumer accounts at your institution and initiated via your institution's website, mobile application, or SMS/text message.

Include:

- Online and mobile bill payment transactions initiated through a web browser (including a mobile browser), a mobile application, or SMS/text message

Do not include:

- Payments made through the biller's website
- Person-to-person transfers (e.g., clearXchange, PopMoney) reported in item **4** below

Note: If your answer is **No** to item **1** above, please report "0" here.

► Example: Your accountholder paid his $50 utility bill through his PC by initiating a payment from his account via your institution's website. Please report 1 transaction for $50.

3) Did your institution offer an online or mobile person-to-person (P2P), business-to-person (B2P), or business-to-business (B2B) funds transfer system during calendar year 2016?

Include:

- All online, mobile, and SMS/text message funds transfer transactions from customer to customer (i.e., P2P, B2P, and B2B)

Note: If your answer to this question is **No**, please report "0" for items **4**, **5**, and **6** below.

► Example: Your accountholder initiated payment from his account to another person's account at another institution via Popmoney on the mobile version of your intuition's website. Another accountholder at your institution initiated payment from his account to another person's account at another institution via clearXchange on your institution's mobile application. Either of these examples would result in a **Yes** response to this question.

4) Total online or mobile person-to-person (P2P) transfers

All person-to-person transfers completed on behalf of your institution's consumer accountholders and initiated through your institution's website, mobile application, or via SMS/text message to another consumer account.

Include:

- Person-to-person transfers initiated through a web browser (including a mobile browser), your institution's mobile application, or via SMS/text message

Do not include:

- Any bill payment transactions

Note: If your answer is **No** to item **3** above, please report "0" here.

► Example: Your accountholder initiated a $200 payment from his account to another person's account at another institution through your institution's mobile application on his tablet by entering the recipient's phone number or e-mail address. Please report 1 transaction for $200.

5) Total online or mobile business/government-to-person (B2P) transfers

All business/government-to-person transfers completed on behalf of your institution's business/government accountholders initiated through your institution's website, mobile application, or via SMS/text message to another consumer account.

Include:

- Business/government-to-person transfers initiated through a web browser (including a mobile browser), your institution's mobile application, or via SMS/text message
- Transfers from small business accounts to consumer accounts

Note: If your answer is **No** to item **3** above, please report "0" here.

► Example: Your customer, a small business owner pays his employee her monthly wages ($4,000) by initiating payment from his account to his employee's account using your institution's online platform on a web browser on his PC. Please report 12 transactions (1 for each month), totaling $48,000.

6) Total online or mobile business/government-to-business/government (B2B) transfers

All business/government-to-business/government transfers completed on behalf of your institution's business/government accountholders initiated through your institution's website, mobile application, or via SMS/text message to another business/government account.

Include:

- Business/government-to-business/government transfers initiated through a web browser (including a mobile browser), your institution's mobile application, or via SMS/text message
- Transfers from small business accounts to other small business accounts
- Transfers from small business accounts to corporate accounts and vice versa

Note: If your answer is **No** to item **3** above, please report "0" here.

► Example: Your customer, a small business owner paid his vendor $800 by initiating payment from his account using your institution's online platform through a mobile application. Please report 1 transaction for $800.