The Federal Reserve Payments Study

Survey Period: Calendar Year 2018

The *Depository and Financial Institutions PaymentsSurvey* (DFIPS) includes:

- Institution's affiliates
- Institution profile
- Check profile, payments, deposits, and outgoing returns
- ACH profile, originations, receipts and outgoing returns
- Wire transfers originated and received
- Non-prepaid debit cards
- General-purpose prepaid cards
- General-purpose credit cards
- Cash withdrawals and deposits
- Alternative payment initiation methods

---- Glossary with Examples ----

Summary of definition clarifications:

Please note that the final version of the questionnaire contains more detailed definitions and examples to provide clarification about the requested data, compared to the preliminary version. No questions have been added or removed from the questionnaire. For your convenience, we have outlined all definition clarifications below so that you can easily assess if any of your responses will need to be edited.

1) Throughout the questionnaire, we have clarified the definition of U.S. domiciled accounts. These include accounts located within the 50 U.S. states, D.C., or U.S. territories such as Guam, Puerto Rico, or U.S. Virgin Islands. This clarification has been made to the instructions, as well as several examples involving domestic and foreign accountholders.

2) General-purpose credit card question 4) contains clarifying instructions and definitions. If you are able to report current-balance-only accounts but unable to segregate zero balance from non-zero balance accounts, please report 'NR' for 4a, report the total number of accounts with zero plus nonzero current balances only under item 4b, and indicate 'Includes accounts with zero balances' in the comment field. Similarly, if you can report accounts with revolving balances but are unable to segregate revolving accounts with no current activity, report 'NR' for 4c, include them in your response to 4d, and indicate 'Includes accounts with no current activity' in the comment field.

3) Throughout the General-Purpose Credit Card section, please exclude cash advances from all credit card transactions.

4) Do not include transfers made through an external party's website such as Venmo or Popmoney for any responses in the Alternative Payment Initiation Methods section.

Glossary with Examples

Note: The Institution's Affiliates section is excluded from the glossary.

Institution Profile

GENERAL TERMINOLOGY

Your institution

The participating depository institution at its highest organizational level (i.e., holding company, if applicable), including all affiliates.

Note: If your institution represents a third-party processor responding on behalf of a depository institution that was sampled for this study, please ensure that your response reflects transaction activity of accounts at the participating institution only and does not include data from other institutions for which your institution processes payments.

Transaction deposit account-type definitions

Consumer: A transaction deposit account for personal use by an individual or household from which payments are commonly made. This includes checking accounts, negotiable order of withdrawal (NOW) accounts, and share draft accounts. It **excludes** savings accounts and money market deposit accounts (MMDAs), which, although eligible for a limited number of transactions per month, should not be included. It also **excludes** certificates of deposit (CDs) as well as prepaid card accounts, which are reported in the prepaid card section of this survey.

Business/government: A transaction deposit account owned by an organization (e.g., business, government, non-depository financial institution, or not-for-profit organization) from which payments are commonly made. This includes small business accounts and commercial checking accounts – both analyzed (i.e., those for which fees can be offset by balances via an earnings credit rate) and non-analyzed. It **excludes** savings accounts and money market deposit accounts (MMDAs), which although eligible for a limited number of transactions per month, should not be included. It also **excludes** certificates of deposit (CDs) and deposits held from a depository institution for correspondent banking purposes.

Note: Please report small business accounts under business/government accounts, if possible.

Retail sweep program account-type definitions

Consumer: In a "retail sweep program," a depository institution transfers funds between a customer's transaction accounts (e.g., a consumer) and that customer's savings deposit accounts up to six times per month by means of preauthorized or automatic transfers, typically in order to reduce transaction account reserve requirements while providing the customer with access to the funds.

See http://www.federalreserve.gov/BOARDDOCS/LegalInt/FederalReserveAct/2007/20070501/20070501.pdf for a regulatory opinion of what approaches may be used to implement these programs.

Business/government: In a "retail sweep program," a depository institution transfers funds between a customer's transaction accounts (e.g., a small business) and that customer's savings deposit accounts up to six times per month by means of preauthorized or automatic transfers, typically in order to reduce transaction account reserve requirements while providing the customer with access to the funds.
See http://www.federalreserve.gov/BOARDDOCS/LegalInt/FederalReserveAct/2007/20070501/20070501.pdf for a regulatory opinion of what approaches may be used to implement these programs.

Note: Please report small business accounts under business/government accounts, if possible.

Wholesale sweep program account-type definitions

Wholesale sweep program accounts, also known as corporate sweep program accounts, are accounts in which funds from your business accountholders are swept overnight into investment instruments. Common investments used in wholesale sweeps are repurchase agreements, Master Notes, offshore Eurodollar deposits, and mutual funds.

U.S. domiciled account

Accounts located within the 50 U.S. states, D.C., or U.S. territories such as Guam, Puerto Rico, or U.S. Virgin Islands). Only report data associated with your institution's U.S. domiciled accounts, including transactions that are domestic and cross-border.

SURVEY ITEMS

1) Transaction deposit accounts (including Demand Deposit Accounts (DDAs))

Please refer to the **General Terminology** section above for the definition of transaction deposit accounts. Average of monthly totals means the average of end-of-month totals for 2018.

Include:

- Checking accounts
- NOW accounts
- Share draft accounts

Do not include:

- Non-transaction accounts (savings accounts, money market accounts, CDs)
- Prepaid card program accounts
- Credit card accounts
- Accounts of foreign governments and official institutions
- Accounts of other depository institutions
- Retail sweep program accounts (item **3)** below)
- Wholesale sweep program accounts (item **5)** below)

► **Example:** Your customer has a student checking account with an average monthly balance of $3,500 at your institution. He also has a savings account and a credit card with your institution. Please report one consumer account with a balance of $3,500. The $3,500 balance reported is the average of end-of-month totals for each of the months in 2018.

2) Did your institution or any of its affiliates employ the use of a retail sweep program (i.e., reserve sweep program) during calendar year 2018?

In order to make national aggregate estimates, we use your institution's deposit balances as a sizing measure. Understanding if your institution used a retail sweep program will help inform our estimates. In a retail sweep, depository institutions move unused funds from checkable deposit accounts (both consumer and business/government) to special purpose money market deposit accounts (MMDAs) and return the funds to checkable deposit accounts only as needed to cover payments. This practice does not adversely impact the accountholder but allows the institution to reduce nonearning assets. Do not consider wholesale sweep program accounts (i.e., corporate sweep program accounts). If your answer to this question is **No**, please report "0" for items **3)**, **4)**, and **5)**.

3) Retail sweep program accounts (i.e., reserve sweep program accounts)

Please refer to the **General Terminology** section above for the definition of retail sweep program accounts. If your answer is **No** to item **2)** above, please report "0" here. Average of monthly totals means the average of end-of-month totals for 2018.

Include:

- Savings and money market deposit accounts associated with retail sweep programs (include both consumer and business/government accounts)

Do not include:

- Checking accounts
- NOW accounts
- Share draft accounts
- Transaction deposit accounts (item **1)** above)
- Wholesale sweep program accounts (item **5)** below)
- Accounts and balances of any savings-type account not associated with transaction deposit accounts under a sweep program

► **Example**: Your customer has a student checking account with an average monthly balance of $3,500 at your institution. He also has a savings account with an average monthly balance of $15,000 with your institution, which includes a sweep to his checking account as needed to cover payments. Please report one consumer account with a balance of $15,000. The $15,000 balance reported is the average of end-of-month totals for each of the months in 2018.

4) Did your institution provide a wholesale sweep program (i.e., corporate sweep program) to your business accountholders during calendar year 2018?

Do not consider retail sweep program accounts (i.e., reserve sweep program accounts).

If your answer to this question is **No**, please report "0" for item **5)** below.

5) Wholesale sweep program accounts

Please refer to the **General Terminology** section above for the definition of wholesale sweep program accounts. If your answer is **No** to item **4)** above, please report "0" here. Average of monthly totals means the average of end-of-month totals for 2018.

Include:

- Corporate sweep accounts in which funds from your business accountholders are swept overnight into investment instruments.

Do not include:

- Checking accounts
- NOW accounts
- Share draft accounts.
- Transaction deposit accounts (item **1)** above)
- Retail sweep program accounts (item **3)** above)
- Accounts and balances of any savings-type account not associated with transaction deposit accounts under a sweep program

► **Example**: Your corporate customer has a business checking account with an average monthly balance of $3,500 at your institution. The company also has a business savings account with an average monthly balance of $50,000 with your institution, which includes an overnight sweep into an investment account. Please report one wholesale sweep program account with a balance of $50,000. The $50,000 balance reported is the average of end-of-month totals for each of the months in 2018.

Checks

GENERAL TERMINOLOGY

Checks

A negotiable instrument drawn on a depository institution. For this study, please follow these guidelines:

Checks include…	Checks do not include…
▪ Checks written by individuals, businesses or government entities ▪ Traveler's checks drawn on your institution ▪ Money orders drawn on your institution ▪ Cashier's checks drawn on your institution ▪ Official checks drawn on your institution ▪ Teller's checks drawn on your institution ▪ Payable through drafts drawn on your institution ▪ Truncated checks (i.e., image exchange)	▪ Deposit slips ▪ General ledger tickets ▪ Other non-check documents, such as payment coupons ▪ Courtesy checks on credit card accounts ▪ Checks converted to ACH (i.e., ARC, POP, BOC transactions)

Bank of first deposit

The first depository institution in which a check is deposited. The “bank of first deposit” may be a bank or credit union and may not be your institution.

“On-us” correspondent deposits

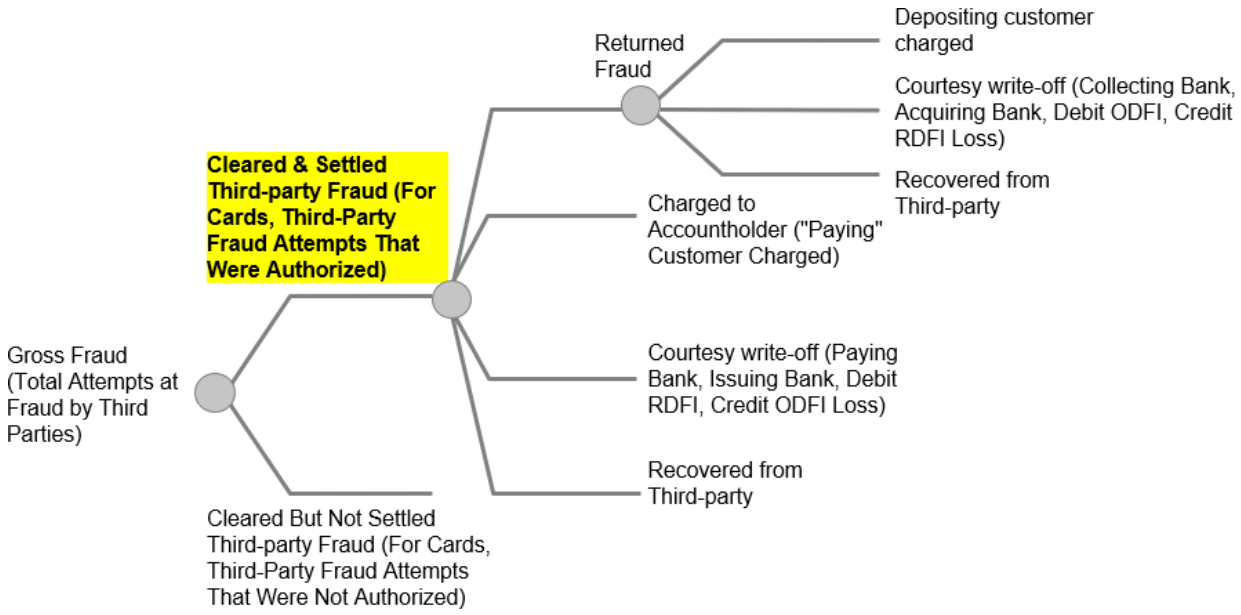
Checks drawn on your institution that are deposited at a correspondent bank. The correspondent bank will subsequently send the check to be processed by your institution, which becomes the “bank of first deposit.”

U.S. domiciled account

Accounts located within the 50 U.S. states, D.C., or U.S. territories such as Guam, Puerto Rico, or U.S. Virgin Islands). Only report data associated with your institution's U.S. domiciled accounts, including transactions that are domestic and cross-border.

Third-party fraud

The Federal Reserve Payments Study has identified a measure of fraud that can be described as cleared and settled third-party fraudulent transactions. The measure is not a loss-of-funds measure, nor is it a measure of fraud attempts; rather, it is a measure of the extent to which third-parties who are not authorized to conduct transactions are able to penetrate the payment system and effect settlement between banks, or create a book transfer of funds if the transaction happens within one 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 manages to create a 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.



SURVEY ITEMS

1) Did your institution outsource check processing to another organization (i.e., its "processor") during calendar year 2018?

If your institution cannot process checks internally and outsources this process to a third-party vendor, please answer **Yes** to this question. If your institution outsourced check processing for part of 2018, please answer **Yes**.

If your answer to this question is **No**, please skip item **1.a)** below.

Note: If your answer to this question is **Yes**, please request the necessary data from your institution's payments processor, or provide them with a PDF copy of the survey so that they may respond on your behalf. If your institution outsourced check processing for part of 2018, please also request the necessary data from your institution's payments processor and combine it with check totals that were processed by your institution.

1.a) If your answer is "Yes, in all cases," or "Yes, in some cases," to item 1.a) above, are you able to include these outsourced portions in your answer below?

If your answer is **No** to item **1.a)** above, please explain in the comments box at the end of this section.

2) Are you able to exclude non-check documents from "all checks drawn on your institution" (item 5) below)?

Non-check documents are "other" items processed on check sorters (e.g., batch headers, general ledger tickets, cash-in or cash-out tickets, deposit slips).

3) Are you able to report checks deposited at one affiliate of your institution but drawn on another affiliate of your institution as on-us volume in item 5.b) below?

Some institutions call this "on-we" volume, which should be reported entirely under item **5.b)** below if possible.

4) Did your institution process checks for an unaffiliated depository institution as part of a correspondent banking relationship during calendar year 2018?

As a "correspondent bank," your institution holds balances for an unaffiliated depository institution in a due-to account and performs check clearing services on its behalf.

► **Example:** Bank A received deposits at its branches. Rather than processing and forwarding transit checks for collection itself, Bank A deposited the checks into a due-to account at Bank B. Bank B cleared Bank A's checks on its behalf. In this example, Bank B is a correspondent processor and would answer **Yes** to this question.

5) Total checks drawn on your institution = 5.a) + 5.b)

These are all checks (or share drafts) for which your institution was the paying bank as defined by Reg. CC. **Note:** Do not double-count electronic check presentment (ECP) items if your institution received an electronic file with paper to follow. Also, if your institution performed proof-of-deposit processing, **do not over-report** item **5)** by calculating it as the difference between prime pass and transit check volumes. Prime pass volume includes non-check documents, which should be excluded here in item **5)**.

Include:

- Controlled disbursement checks, if applicable
- Checks your institution subsequently returned unpaid to the "bank of first deposit" or its designated processor (i.e., outgoing returns) or chargebacks to the depositing customer if your institution was the "bank of first deposit" (i.e., "on-us" returns)
- Official checks written by your institution (rather than by your accountholders)

Do not include:

- Checks drawn on other institutions (i.e., transit checks)
- Checks that your institution received as a "pass-through correspondent" for which another institution was the paying bank
- Non-check documents—such as batch headers, general ledger tickets, cash-in or cash-out tickets, and deposit tickets—that were processed on check sorters

► **Example:** Your customer wrote a check for $57 to pay her water bill. If your institution has a depository relationship with this water company, these checks are "on-us" deposited checks. In this example, you would report one check with a value of $57 in items **5)** and **5.b)**.

5.a) Checks drawn on your institution for which another institution was the "bank of first deposit" = 5.a.1) + 5.a.2)

These are all checks drawn on your institution for which another institution was the "bank of first deposit."

Note: Do not double-count electronic check presentment (ECP) items if your institution received an electronic file with paper to follow.

Include:

- Inclearings (**5.a.1**) and "on-us" (**5.a.2**) checks deposited by correspondent customers
- Checks received from the Federal Reserve or via clearinghouses and image exchange networks, or in direct presentment for same-day settlement
- Controlled disbursement checks if applicable

Do not include:

- Checks for which your institution was the "bank of first deposit" or checks drawn on other institutions
- Checks drawn on an unaffiliated depository institution that were deposited at your institution (i.e., outbound transit checks)
- Checks drawn on your institution for which your institution was also the "bank of first deposit" (i.e., "on-us" checks for which your institution was the "bank of first deposit," item **5.b)** below)
- Non-check documents that were processed on check sorters, such as batch headers, general ledger tickets, cash-in or cash-out tickets, deposit tickets
- Checks deposited and drawn on different affiliates of your institution (some call this "on-we" volume)

► **Example:** Your customer wrote a check for $125 to pay for her groceries. The grocery store has a depository relationship with an unaffiliated depository institution. After processing the grocer's deposit, that institution (i.e., the "collecting bank") presented the check through the Federal Reserve, through a local clearinghouse, or directly for same-day settlement to your institution for payment. In this example, you would report one check with a value of $125.

5.a.1) Inclearings

These are checks drawn on your institution for which another institution was the "bank of first deposit," and the "bank of first deposit" is not a correspondent bank of your institution.

Include:

- Checks drawn on your institution for which another institution was the "bank of first deposit," and for which your institution did not receive in a deposit for correspondent processing

Do not include:

- "On-us" checks deposited by correspondent customers
- "On-us" checks for which your institution was the "bank of first deposit"

► **Example:** Your customer wrote a check for $125 to pay for her groceries. The grocery store has a depository relationship with an unaffiliated depository institution. After processing the grocer's deposit, that institution (i.e., the "collecting bank") presented the check to your institution for payment. In this example, you would report one check with a value of $125.

5.a.2) "On-us" checks deposited by correspondent customers

These are checks drawn on your institution and subsequently received as a deposit for corresponding processing. Please refer to **4)** above for the definition of a correspondent bank.

Include:

- Checks drawn on your institution that your institution received as a deposit from another institution for correspondent processing

Do not include:

- Inclearings
- "On-us" checks for which your institution was the "bank of first deposit"

► **Example:** Your customer wrote a check for $125 to pay for her groceries. The grocery store has a depository relationship with a correspondent depository institution. After processing the grocer's deposit, the correspondent institution sent the check to be processed by your institution, which becomes the "bank of first deposit." In this example, you would report one check with a value of $125.

5.b) "On-us" checks for which your institution was the "bank of first deposit"

These are all checks drawn on your institution for which your institution was the "bank of first deposit."

Note: If your institution truncated checks at the teller line, please include those checks in this volume.

Include:

- All checks cleared between your affiliates, which include but are not limited to the following:
  - Checks deposited in your branches
  - Checks received from other internal departments (e.g., wholesale or retail lockbox, currency/coin vault operations, and loan payments processing operations)
  - Checks deposited by corporate clients (typically in the evening) directly to your item-processing operations (e.g., pre-encoded or un-encoded deposits or remote capture deposits)
  - Checks deposited and drawn on different affiliates of your institution (some call this "on-we" volume)

Do not include:

- Inclearings received from the Federal Reserve, a clearinghouse, or another institution (i.e., same-day settlement)
- Transit or non-check documents (e.g., general ledger tickets, cash-in or cash-out tickets, deposit tickets)
- Checks deposited by correspondent customers, even if they were drawn on your institution. These are "on-us" correspondent deposits and should be counted in item **5.a.2)** above

► **Example:** Your customer wrote a $65 check to her babysitter, who also happened to be your customer. When the babysitter deposited the check, your institution was both the collecting institution and the paying institution on this check. In this example, you would report one check with a value of $65.

6) Total checks drawn on your institution (repeat item 5) = 6.a) + 6.b)

Repeat item **5)** from above. These are all checks (or share drafts) for which your institution was the paying bank as defined by Reg. CC.

Note: Do not double-count electronic check presentment (ECP) items if your institution received an electronic file with paper to follow. Also, if your institution performed proof-of-deposit processing, **do not over-report** item **6)** by calculating it as the difference between prime pass and transit check volumes. Prime pass volume includes non-check documents, which should be excluded here in item **6)**.

Include:

- Controlled disbursement checks, if applicable
- Checks your institution subsequently returned unpaid to the "bank of first deposit" or its designated processor (i.e., outgoing returns) or chargebacks to the depositing customer if your institution was the "bank of first deposit" (i.e., "on-us" returns)
- Official checks written by your institution (rather than by your accountholders)

Do not include:

- Checks drawn on other institutions (i.e., transit checks)
- Checks that your institution received as a "pass-through correspondent" for which another institution was the paying bank
- Non-check documents—such as batch headers, general ledger tickets, cash-in or cash-out tickets, and deposit tickets—that were processed on check sorters

► **Example:** Sarah, your customer, wrote a check for $57 to pay her water bill. The water company is also a client of your institution, and they wrote a check to their power company for $2,000. In this example, you would report two checks with a value of $2,057 in item **6)**, one check with a value of $57 for **6.a)**, and one check with a value of $2,000 in **6.b)**.

6.a) From consumer accounts

All checks paid from consumer accounts of any kind.

Include:

- Consumer checks, no matter what kind of consumer account they were written on
- Any money orders, cashier's checks, or official checks paid on behalf of consumer accountholders through any type of account set up for that purpose
- Both inclearings and on-us checks

Do not include:

- Checks paid from business/government accounts

► **Example:** Your consumer customer, Joe, wrote a check for $1,400 to pay his rent last month. In this example, you would report one check for $1,400.

6.b) From business/government accounts

All checks paid from business/government accounts of any kind

Include:

- Checks the institution pays itself on its own accounts
- Any money orders, cashier's checks, or official checks paid on behalf of business/government accountholders through any type of account set up for that purpose, and any checks your institution paid on its own behalf.
- Small business accounts under business/government accounts
- Both inclearings and on-us checks

Do not include:

- Checks paid from consumer accounts

► **Example:** Your corporate customer, Joe's Shoes, wrote a check for $3,000 to one of his suppliers. In this example, you would report one check for $3,000.

7) Third-party fraudulent checks drawn on your institution

These are all third-party, fraudulent unauthorized checks drawn on your institution that subsequently were deposited, cleared, and settled. Please report any third-party, fraudulent paid checks regardless of whether or not those funds were subsequently recovered through the check return process or by other means.

Include:

- Only fraudulent cleared and settled paid checks that were not authorized by your institution's accountholders (third-party fraud)
  - If a transit check, report only those fraudulent items that resulted in a transfer of funds to the collecting bank
  - If an on-us check for which your institution was the bank of first deposit, report only those fraudulent items that resulted in funds' being made available to the depositing customer

Do not include:

- Check fraud prevented before funds were made available to the depositing customer
  - If a transit check, a transfer of funds to the collecting bank did not occur
  - If an on-us check for which your institution was the bank of first deposit, funds were not made available to the depositing customers
- Fraud committed by your institution's accountholders (first-party fraud), or checks authorized by a valid accountholder as part of a scam

► **Example 1:** Jane and Mary are accountholders at your institution, and both of their checkbooks were stolen. The perpetrator wrote a check for $2,000 from Jane's checkbook, which your institution paid. The perpetrator also wrote a check for $1,500 from Mary's checkbook, which your institution did not pay per Mary's instructions to stop all check payments from her account due to her stolen checkbook. Susan is also an accountholder at your institution. She wrote a check for $100, which, due to a misread item, posted erroneously to her account for $110. Only the check from Jane's account is classified as a third-party fraudulent unauthorized check. In this example, you would report one transaction for $2,000.

► **Example 2:** Daniel is an accountholder at your institution. He recently bought a TV at a retailer for $1,200 and paid with a check. After the funds transferred from Daniel's account to the retailer's account, your accountholder claimed this transaction as fraudulent, stating that his checkbook was stolen and that a perpetrator had written the check. Your institution made an inquiry into the fraud claim and determined that Daniel indeed wrote the check and made a false claim of fraud. In this example, you would not report the transaction as third-party fraud since it is considered first-party fraud.

8) Total checks deposited at your institution

These include checks that were drawn on your institution (i.e., "on-us" checks for which your institution was the "bank of first deposit," item **5.b)** above and "on-us" checks deposited by correspondent customers, item **5.a.2)** above) and checks drawn on other depository institutions (i.e., transit checks).

Include:

- Checks deposited in your branches
- Checks received from other internal departments (e.g., wholesale or retail lockbox, currency/coin vault operations, and loan payments processing operations)
- Checks deposited by corporate clients (typically in the evening) directly to your item processing operations (i.e., pre-encoded or un-encoded deposits or remote capture deposits)
- Checks deposited by correspondent banking customers

► **Example:** A customer deposits a check by using your institution's app on his smartphone for $100. Another customer walks into one of your institution's branches and deposits a check for $250. In this example, both types of checks would be included for a total of two deposits in the amount of $350.

9) Third-party fraudulent checks deposited at your institution

These are all third-party, fraudulent unauthorized checks deposited at your institution that subsequently were cleared and settled. Please report any third-party, fraudulent paid checks regardless of whether or not those funds were subsequently recovered through the check return process or by other means.

Include:

- Only fraudulent cleared and settled paid checks that were not authorized by the institution accountholders (third-party fraud)
- If a transit check, report only those fraudulent items that resulted in a transfer of funds to the collecting bank
- If an on-us check for which your institution was the bank of first deposit, report only those fraudulent items that resulted in funds' being made available to the depositing customer

Do not include:

- Check fraud prevented before funds were made available to the depositing customer
  - If a transit check, a transfer of funds to the collecting bank did not occur
  - If an on-us check for which your institution was the bank of first deposit, funds were not made available to the depositing customers
- Fraud committed by your institution's accountholders (first-party fraud), or checks authorized by a valid accountholder as part of a scam

► **Example 1:** Dan is an accountholder at a different institution. Dan's checkbook was stolen and the perpetrator deposited one of the stolen checks for $2,000 into an account at your institution, which then cleared and settled. Dan's institution notified yours about the fraudulent check that had been deposited. In this example, you would report one check for $2,000.

► **Example 2:** Sarah is an accountholder and your institution, and she deposited a check for $500 in her bank account. After the check had cleared, Sarah contacted your institution claiming that the deposit had mis-read her check, and $5,000 should have been deposited into her account. Your institution investigated the claim and determined that the check had not been misread, and the correct amount of $500 had been deposited into her account. In this example, you would not report the transaction as third-party fraud since it is considered first-party fraud.

10) Total outgoing and "on-us" returned checks = 10.a) + 10.b)

These are all checks drawn on your institution that your institution returned unpaid.

Include:

- All checks drawn on your institution that it returned unpaid, whether to another institution or to your own accountholders

Do not include:

- Checks drawn on another institution and returned to your institution unpaid (i.e., incoming returns)

► **Example:** Your customer wrote a check for $98 that was deposited (at your institution or another) and presented for payment. Your customer's account had insufficient funds and no overdraft protection. Your institution returned the check unpaid. In this example, you would report one check with a value of $98.

10.a) Checks your institution returned unpaid to the collecting institution

These checks were drawn on your institution but were returned to another institution unpaid.

Include:

- Checks drawn on your institution for which another institution was the "bank of first deposit" that your institution returned unpaid

Do not include:

- "On-us" checks your institution returned unpaid to your institution's accountholders

► **Example:** Your customer wrote a check for $98 that was deposited at another institution and presented for payment. Your customer's account had insufficient funds and no overdraft protection. Your institution returned the check unpaid to the collecting institution. In this example, you would report one check with a value of $98.

10.b) "On-us" checks your institution returned unpaid to your institution's accountholder

All "on-us" checks for which your institution was the "bank of first deposit" that it returned unpaid. These are a subset of items charged back to depositing accountholders. Some institutions call these "chargebacks."

Include:

- All "on-us" checks for which your institution was the "bank of first deposit" that it returned unpaid to the depositing accountholders. Some institutions call these "chargebacks."

Do not include:

- Checks your institution returned unpaid to another institution

► **Example:** Your customer wrote a check for $200 that was deposited at your institution and presented for payment. Your customer's account had insufficient funds and no overdraft protection. Your institution returned the check unpaid to your accountholder. In this example, you would report one check with a value of $200.

11) Total outgoing and "on-us" returned checks (repeat item 10) = 11.a) + 11.b) + 11.c) + 11.d)

Repeat item **10)** above. These are all checks drawn on your institution that your institution returned unpaid.

Include:

- All checks drawn on your institution that it returned unpaid, whether to another institution or to your own accountholders

Do not include:

- Checks drawn on another institution and returned to your institution unpaid (i.e., incoming returns)

► **Example:** Your customer wrote a check for $98 that was deposited (at your institution or another) and presented for payment. Your customer's account had insufficient funds and no overdraft protection. Your institution returned the check unpaid. In this example, you would report one check with a value of $98.

11.a) Unauthorized returned checks = 11.a.1) + 11.a.2) + 11.a.3)

These include checks drawn on your institution that it returned unpaid, whether to another institution or to your own accountholders, because they were unauthorized.

Include:

- All unauthorized checks drawn on your institution that it returned unpaid, whether to another institution or to your own accountholders

Do not include:

- Checks drawn on another institution and returned to your institution unpaid (i.e., incoming returns)

► **Example:** Mary is an accountholder at your institution, and her checkbook was stolen. The perpetrator also wrote a check for $1,500 from Mary's checkbook, which your institution did not pay per Mary's instructions to stop all check payments from her account due to her stolen checkbook. Susan is also an accountholder at your institution. She wrote a check for $100, which, due to a misread item, posted erroneously to her account for $110. Only the check from Mary's account is classified as an unauthorized returned check. In this example, you would report one transaction for $1,500.

11.a.1) Remotely created checks

These are remotely created checks that your institution returned as unpaid. The checks are created by either your own institution or another institution on behalf of a salesperson and presented to your consumer's account, which your consumer subsequently reported as unauthorized.

Include:

- Remotely created checks that your institution returned unpaid because they were reported as unauthorized

Do not include:

- Checks that were returned unpaid because there were flagged as forgery/suspected forgery
- Checks that were returned unpaid because they were flagged as unauthorized for a reason other than remotely created

► **Example:** Sam is an accountholder at your institution, and his mobile banking account was hacked. The perpetrator created a check remotely for $2,000 from Sam's account, which your institution did not pay per Sam's instructions to stop all check payments from his account due to his account being hacked. In this example, you would report one transaction for $2,000.

11.a.2) Forgery/suspected forgery

These are checks that were deposited (at either your institution or another) and presented for payment, but were flagged by your institution as a forgery/suspected forgery, and which your institution subsequently returned as unpaid.

Include:

- Checks that were returned unpaid because there were flagged as forgery/suspected forgery

Do not include:

- Remotely created checks that your institution returned unpaid because they were reported as unauthorized
- Checks that were returned unpaid because they were flagged as unauthorized for a reason other than forgery/suspected forgery

► **Example:** Joe is an accountholder at your institution, and his checkbook was stolen. The perpetrator wrote a check for $3,000 from Joe's checkbook, which your institution did not pay due to suspected forgery on the check. In this example, you would report one transaction for $3,000.

11.a.3) Other unauthorized

These are checks that were deposited (at either your institution or another) and presented for payment, but were flagged by your institution for reasons not listed under items **11.a.1)** or **11.a.2)**, which your institution subsequently returned as unpaid. These items are classified under return code "N" for altered/fictitious item/suspected counterfeit/counterfeit.

Include:

- Checks that were returned unpaid because they were flagged as unauthorized for a reason other than remotely created or forgery/suspected forgery (i.e., altered/fictitious item/suspected counterfeit/counterfeit)

Do not include:

- Remotely created checks that your institution returned unpaid because they were reported as unauthorized
- Checks that were returned unpaid because there were flagged as forgery/suspected forgery

► **Example:** Chris is an accountholder at your institution, and he noticed a $1,500 check had been issued from his account that he did not write. Given his checkbook is not missing, Chris suspects that his online banking account number was used for a counterfeit check, but the actual fraudulent method is unknown. Your institution verified that this was in fact a fraudulent check. In this example, you would report one transaction for $1,500.

11.b) Nonsufficient funds

These are checks drawn on your institution that it returned unpaid, whether to another institution or to your own accountholders, due to nonsufficient funds.

Include:

- All checks drawn on your institution that it returned unpaid because there were nonsufficient funds

Do not include:

- Checks drawn on another institution and returned to your institution unpaid (i.e., incoming returns)

► **Example:** Your customer wrote a check for $98 that was deposited (at your institution or another) and presented for payment. Your customer's account had insufficient funds and no overdraft protection. Your institution returned the check unpaid. In this example, you would report one check with a value of $98

11.c) Duplicate presentment

These are checks drawn on your institution that it returned unpaid, whether to another institution or to your own accountholders, because it was suspected to be a duplicate check.

Include:

- All checks drawn on your institution that it returned unpaid because of duplicate presentment

Do not include:

- Checks drawn on another institution and returned to your institution unpaid (i.e., incoming returns)

► **Example:** Your customer wrote a check for $150 that was deposited (at your institution or another) and presented for payment. This was erroneously presented twice at the collecting institution, for a total of two checks for a total of $300. Your institution returned the duplicate check unpaid. In this example, you would report one check with a value of $150.

11.d) Other (including administrative returns)

These are checks drawn on your institution that it returned unpaid, whether to another institution or to your own accountholders, due to other reasons not included in items 11.a), 11.b), or 11.c) above. Include returned checks for administrative reasons.

Include:

- Uncollected funds hold
- Stop payment
- Closed account
- Unable to locate account
- Frozen or blocked account
- Stale date or expired check
- Post dated check
- Endorsement missing
- Endorsement irregular
- Signature missing
- Signature irregular
- Non Cash Item
- Altered or fictitious item
- Item exceeds dollar limit
- Not authorized
- Refer to maker

Do not include:

- Checks drawn on another institution and returned to your institution unpaid (i.e., incoming returns)

► **Example:** Your customer wrote a check for $1,000 that was deposited at your institution. The check was missing an endorsement signature by the depositor, so the check was returned. In this example, you would report one check with a value of $1,000.

ACH Profile

GENERAL TERMINOLOGY

ACH payments

Transactions in this category are entries, originated or received by your institution, that are processed through an Automated Clearinghouse (ACH) platform according to NACHA rules and format conventions. For this study, please follow these guidelines:

ACH entries include…	ACH entries do not include…
▪ Debits received and credits sent ▪ Debits originated and credit received ▪ Direct exchange ▪ On-us entries ▪ Network entries ▪ Returns (only for item 18)	▪ Addenda records ▪ Zero-dollar items (e.g., NOCs, Prenotes) ▪ Deletes/reversals

Originating Depository Financial Institution (ODFI)

The depository institution that initiates and warrants electronic payments through the ACH network (or on-us) on behalf of its customers. Some institutions refer to forward originations as "live items."

Receiving Depository Financial Institution (RDFI)

The depository institution that accepts and posts ACH transactions to customer accounts.

Network ACH entry

An ACH entry that is cleared through a network operator (i.e., the Federal Reserve or Electronic Payments Network [EPN]).

In-house, on-us ACH entry (cleared within your institution and not through the Federal Reserve or EPN)

An ACH entry for which your institution is both the ODFI and the RDFI without the use of a network operator (i.e., the Federal Reserve or EPN) for clearing or settlement. On-us entries result in the movement of funds from one account to another within your institution.

Direct Exchange ACH entry

An ACH entry that is exchanged directly between your institution and another without the use of a network operator (i.e., the Federal Reserve or EPN). Some institutions call these "Direct Send" entries. Please consider all Direct Exchange ACH entries that result in payments from accounts at your institution.

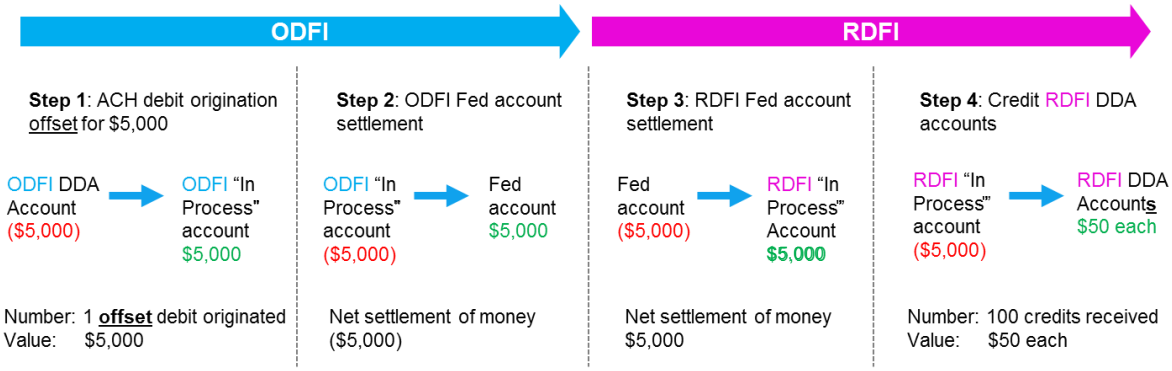
Offset ACH entry

An on-us ACH entry used to effect settlement by an ODFI. For example, when acting as ODFI for 100 $50 credit entries for a corporate accountholder, an ODFI might originate a single $5,000 debit entry to draw funds from the originator's funding account. An offset ACH entry is similar to an "accounting movement of money" to settle a corresponding ACH entry.

Using the example above, if a business account at your institution pays payroll to 100 employees for $50 each (ODFI credit origination), this payment generates 100 credit originations for a total of $5,000. The offset transaction is one debit origination for a total of $5,000. The number of offset transactions may vary depending on the institution. Some institutions might do a one-to-one offset transaction per payment origination.

Example assumptions

- None of the employees bank at the same institution as the employer, thus all ACH entries must go through the ACH network
- Employer's bank (ODFI) = Bank A
- Employees' bank (RDFI) = Bank B
- ODFI offsets in-house on-us



"In Process" accounts are also known by some institutions as "settlement accounts" or "due-from accounts."

Balanced file

Files containing offsetting entries that automatically credit or debit the customer's demand deposit account (DDA) for the debit and/or credit transactions on the file. The debit and credit offset entries should equal the value of the credit- and debit-originated entries respectively in the received file from the accountholder.

Unbalanced file

Files that do not have an offsetting entry that automatically credits or debits the customer's DDA account for the debit and/or credit originated. After receiving the file from the accountholder, the ODFI will then originate the offset entries to balance the file. Most institutions prefer to receive unbalanced files.

Same-day ACH entry

An entry in which the effective entry date is the same banking day as the date on which the entry is transmitted by the ODFI to its ACH operator, and that is transmitted by the ACH operator's deadline for same-day processing and settlement. A same-day entry must be for an amount of $25,000 or less. An IAT (international ACH) or ENR (automated enrollment) entry cannot be a same-day entry. Network ACH same-day credit entries became effective as of September 23, 2016. Network ACH same-day debit entries became effective as of September 15, 2017. However, some institutions may have used proprietary systems prior to these dates.

Consumer account

An ACH account for personal use by an individual or household from which payments can be made.

Business/government account

An ACH account owned by an organization (i.e., business, government or not-for-profit organization) from which payments can be made.

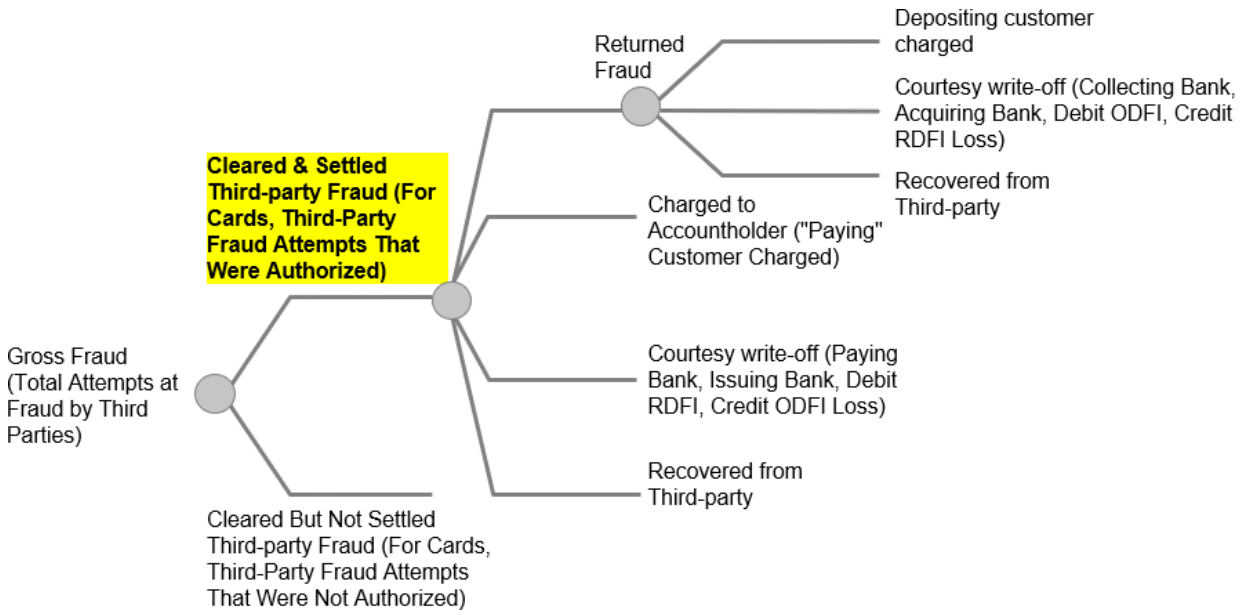
Note: Please report small business accounts under business/government accounts, if possible.

U.S. domiciled account

Accounts located within the 50 U.S. states, D.C., or U.S. territories such as Guam, Puerto Rico, or U.S. Virgin Islands). Only report data associated with your institution's U.S. domiciled accounts, including transactions that are domestic and cross-border.

Third-party fraud

The Federal Reserve Payments Study has identified a measure of fraud that can be described as cleared and settledthird-party fraudulent transactions. It is not a loss-of-funds measure, nor is it a measure of fraud attempts; rather, it isa measure of the extent to which third parties who are not authorized to conduct transactions are able to penetrate the payment system and effect settlement between banks or create a book transfer of funds if the fraud happens within one institution. The definition includes third-party fraud with all types of outcomes, which may or may not include a loss to various entities but constitutes a fraud attempt that manages to create a 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.



SURVEY ITEMS

1) Did your institution post transactions from other payment instruments to your Demand Deposit Account (DDA) system using your ACH platform during calendar year 2018?

If your answer is **Yes**, please do not include these transactions in the items below.

Note: Rather than maintaining an interface between your institution's DDA system and a particular transaction processing system (e.g., signature-based debit card or wire transfer), your institution creates a separate ACH entry to post each of those non-ACH transactions.

2) Did your institution originate forward ACH credits (not including returns or offset entries) during calendar year 2018?

Answer **Yes** if ACH credit originations are a product offered to accountholder customers (i.e., your institution is an ODFI). Answer **No** if not, or if your institution only originates ACH credits for the purpose of returning credits received from another institution (i.e., your institution is not an ODFI) or offsetting debit originations.

Note: If your answer is **No**, please report **No** for item **5**) below, and report "0" for items **6)** and its subsets, item **7)** and its subsets, and item **8)** and its subsets, and item **9)** and its subsets below.

3) Did your institution originate forward ACH debits (not including returns or offset entries) during calendar year 2018?

Answer **Yes** if ACH debit originations are a product offered to accountholder customers (i.e., your institution is an ODFI). Answer **No** if not, or if your institution only originates ACH debits for the purpose of returning debits received from another institution (i.e., your institution is not an ODFI) or offsetting credit originations. If you do not originate debit entries, then you will not receive in-house on-us debit entries).

Note: If your answer is **No**, please report "0" for item **10), 11),** and **14.b)** below. If your answer is **Don't Know**, please report **NR** for item **10), 11),** and **14.b)** below. This applies to **14.b)** because your institution is both the ODFI and RDFI for in-house on-us non-offset debit entries. Therefore, if your institution cannot determine ODFI debits, then you will not be able to accurately calculate when your institution was both the ODFI and RDFI for debit entries.

4) Did your institution originate offset ACH debit or credit entries during calendar year 2018?

Offset entries are internal settlements for ACH transactions by an ODFI. In most cases, institutions offset (or move) the funds from the accountholder's DDA to an "in process" account before the funds are settled with the Fed, EPN, or internally. If your answer is **No**, please skip items **4.a)** and **4.b)** below.

► **Example:** Your corporate customer paid 20 of its employees $1,000 each electronically through ACH. To make the total payment of $20,000, your institution originated one debit ACH entry for $20,000 to "move" the money from your accountholder's DDA to your institution's "in-process" account. (An in-process account is a suspense account owned by your institution that settles internally or with the network operator—i.e., the Federal Reserve or EPN.) Your institution then effected a net settlement of money with the network operator (i.e., the Federal Reserve or EPN) between incoming and outgoing payments.

4.a) If your answer is "Yes" to item 4) above, are you able to exclude offset ACH volumes from balanced files in your answer below?

Even if you are not able to exclude all offset volumes from balanced files, please report the number and value of your institution's forward ACH entries for items **6)**, **7)**, **8)**, **10)**, **12)**, **14)**, **15)**, and **16)** and its subsets.

4.b) If you answer is "Yes" to item 4) above, are you able to exclude offset ACH volumes from unbalanced files in your answers below?

Even if you are not able to exclude all offset volumes from unbalanced files, please report the number and value of your institution's forward ACH entries for items **6)**, **7)**, **8)**, **10)**, **12)**, **14)**, **15)**, and **16)** and its subsets.

5) Did your institution offer same-day settlement of ACH credit originations during calendar year 2018?

The effective date for network same-day settlement of credits was September 23, 2016. If your answer is **No**, please report "0" for items **8.a)** and **9.a)** below.

ACH Originations

Please include all transactions that involve a forward transfer of value. Do not include those transactions that do not involve a forward transfer of value. This allocation maps to the following SEC code breakout:

SEC Codes to Include: ARC, BOC, CCD, CIE, CTX, IAT, POP, POS, PPD, RCK, SHR, TEL, TRC, WEB, XCK
SEC Codes to Exclude: ACK, ADV, ATX, COR, DNE, ENR, MTE, RET, TRX

6) Total forward ACH credits your institution originated (ODFI credits) = 6.a) + 6.b) + 6.c)

These are all network, on-us, and direct exchange ACH credit entries for which your institution was the ODFI. If your answer is **No** to item **2)** above, please report "0" ACH credit entries originated by your institution here.

Include:

- In-house, on-us forward credit entries for which your institution was both the ODFI and RDFI
- Network forward ACH credits originated
- Network on-us credit entries for which your institution was both the ODFI and RDFI
- All direct exchange ACH credit entries for which you are the ODFI

Do not include:

- Returns
- Network offset ACH credit entries originated
- In-house, on-us offset ACH credit entries originated
- Direct exchange offset ACH credit entries originated
- ACH entries received from other institutions
- Debit ACH entries originated
- Addenda records
- Zero-dollar entries

► **Example:** Your corporate customer paid 10 of its employees $300 each electronically through the ACH. Your institution originated the credit entries on behalf of your customer and sent them through your chosen network operator (i.e., the Federal Reserve or EPN). In this example, you would report ten transactions for $3,000.

6.a) Network ACH credit entries originated

These are credit entries for which your institution was the ODFI, and the credit entry was cleared through a network operator (i.e., the Federal Reserve or EPN). Please refer to the **General Terminology** section above for the definition of "Network" entries.

Include:

- All ACH credit entries cleared through a network operator, for which your institution was the ODFI

Do not include:

- Returns
- Network offset ACH credit entries originated
- ACH entries cleared directly between your institution and another (i.e., direct exchange ACH entries)

► **Example:** Your corporate customer paid five of its employees $500 each electronically through the ACH network. Your institution originated the credit entries on behalf of your customer and sent them through your chosen network operator (i.e., the Federal Reserve or EPN). In this example, you would report five transactions for $2,500.

6.b) In-house on-us ACH credit entries originated

These are all ACH credit entries that were not cleared through the Federal Reserve or EPN and for which your institution was both the ODFI and RDFI, for the purpose of moving funds from one account to another at your institution.

Include:

- All ACH credit entries not cleared through a network operator, for which your institution was the ODFI and RDFI

Do not include:

- Returns
- In-house on-us offset ACH credit entries originated

► **Example:** Your corporate customer paid 200 of its employees $800 each electronically through the ACH using your institution as its ODFI. Ten of these employees have deposit accounts at your institution. To credit those 10 employees' accounts, your institution originated in-house on-us credit entries to avoid clearing fees from the Federal Reserve or EPN. In this example, you would report ten transactions for $8,000.

6.c) Direct exchange ACH credit entries originated

These are all ACH credit entries that were originated but not cleared through the Federal Reserve or EPN. Please refer to the **General Terminology** section above for the definition of "Direct Exchange" entries.

Include:

- All direct exchange ACH credit entries, for which your institution was the ODFI

Do not include:

- Returns
- ACH entries received from other institutions
- Debit ACH entries originated
- Network entries originated, such as ACH credits your institution originated through the Federal Reserve or EPN (item **6.a)** above)
- In-house on-us entries, such as in-house on-us credits your institution originated (item **6.b)** above)
- Addenda records
- Zero-dollar entries

► **Example:** Your institution is part of a regional processing center, and you transact via direct exchange with other institutions that are part of the regional processing center. Your corporate customer paid 10 of its employees $750 each electronically through the ACH. These employees bank at institutions that are also part of the regional processing center. In order to avoid clearing fees from the Federal Reserve or EPN, your institution directs the transaction through the regional processing center to the RDFI via direct exchange. In this example, you would report ten transaction for $7,500.

7) Total forward ACH credits your institution originated (ODFI credits) (repeat item 6) =7.a) + 7.b)

Repeat item **6)** above. These are all network, on-us, and direct exchange ACH credit entries for which your institution was the ODFI. If your answer is **No** to item **2)** above, please report "0" ACH credit entries originated by your institution here.

Include:

- In-house on-us forward credit entries for which your institution was both the ODFI and RDFI
- Network forward ACH credits originated
- Network on-us credit entries for which your institution was both the ODFI and RDFI
- All direct exchange ACH credit entries for which you were the ODFI

Do not include:

- Returns
- Network offset ACH credit entries originated
- In-house on-us offset ACH credit entries originated
- ACH entries received from other institutions
- Debit ACH entries originated
- Addenda records
- Zero-dollar entries

► **Example:** Your corporate customer paid 10 of its employees $300 each electronically through the ACH. Your institution originated the credit entries on behalf of your customer and sent them through your chosen network operator (i.e., the Federal Reserve or EPN). In this example, you would report ten transactions for $3,000.

7.a) From consumer accounts

These are credit entries for which your institution was the ODFI and were originated from consumer accounts. Please refer to the **General Terminology** section above for the definition of consumer accounts.

Include:

- All ACH credit originations from consumer accounts, for which your institution was the ODFI

Do not include:

- Any ACH credit originations from business/government accounts, for which your institution was the ODFI.

► **Example:** Your consumer customer, Joe, initiated a one-time payment for $1,000 to his friend through ACH. Your institution originated the credit entries on behalf of your customer and sent them through your chosen network operator (i.e., the Federal Reserve or EPN). In this example, you would report one entry for $1,000.

7.b) From business/government accounts

These are credit entries for which your institution was the ODFI and were originated from business/government accounts. Please refer to the **General Terminology** section above for the definition of business/government accounts.

Include:

- All credit originations from business/government accounts, for which your institution was the ODFI

Do not include:

- Any credit originations from consumer accounts, for which your institution was the ODFI

► **Example:** Your corporate customer, Bob's Hotel, paid 20 of its employees $1,500 each electronically through the ACH. Your institution originated the credit entries on behalf of your customer and sent them through your chosen network operator (i.e., the Federal Reserve or EPN). In this example, you would report twenty transactions for $30,000.

8) Total forward ACH credits your institution originated (ODFI credits) (repeat item 6) = 8.a) + 8.b)

Repeat item **6)** above. These are all network, on-us, and direct exchange ACH credit entries for which your institution was the ODFI. If your answer is **No** to item **2)** above, please report "0" ACH credit entries originated by your institution here.

Include:

- In-house on-us forward credit entries for which your institution was both the ODFI and RDFI
- Network forward ACH credits originated
- Network on-us credit entries for which your institution was both the ODFI and RDFI
- All direct exchange ACH credit entries for which you were the ODFI

Do not include:

- Returns
- Network offset ACH credit entries originated
- In-house on-us offset ACH credit entries originated
- ACH entries received from other institutions
- Debit ACH entries originated
- Addenda records
- Zero-dollar entries

► **Example:** Your corporate customer paid 10 of its employees $300 each electronically through the ACH. Your institution originated the credit entries on behalf of your customer and sent them through your chosen network operator (i.e., the Federal Reserve or EPN). In this example, you would report 10 transactions for $3,000.

8.a) Same-day settlement

These are credit entries for which your institution was the ODFI and for which the payment was settled on the same day. Please refer to the **General Terminology** section above for the definition of same-day ACH entries. If your answer is **No** to item **5)** above, please report "0" here.

Include:

- All ACH credit originations settled same-day, for which your institution was the ODFI

Do not include:

- Any ACH credit originations settled non-same-day, for which your institution was the ODFI

► **Example:** Your corporate customer, Joe's Plumbing, initiated a one-time bill payment for $2,500 to one of its vendors, ABC Supplies, through the ACH network. The vendor does not bank with your institution. Since the payment of this bill was urgent, your customer decided to use the same-day settlement option your institution began offering on September 23, 2016. Since the ACH credit was sent to an unaffiliated institution, your institution sent the ACH entries through a network operator (i.e., the Federal Reserve or EPN). In this example, you would report one entry for $2,500.

8.b) Non-same-day settlement

These are credit entries for which your institution was the ODFI and for which the payment was settled on a later day after the transaction cleared.

Include:

- All ACH credit originations settled non-same-day, for which your institution was the ODFI

Do not include:

- Any ACH credit originations settled same-day, for which your institution was the ODFI

► **Example:** Your corporate customer paid 50 of its employees $2,400 each electronically through the ACH. Your institution originated the credit entries on behalf of your customer and sent them through your chosen network operator (i.e., the Federal Reserve or EPN). The settlement of money occurred on a different day from the transmission of the file. In this example, you would report fifty transactions for $120,000.

9) Third-party fraudulent forward ACH credit entries your institution originated (fraudulent ODFI credits) = 9.a) + 9.b)

These include only third-party, fraudulent, unauthorized ACH credit entries that cleared and settled, for which your institution was the ODFI, and that resulted in transfer of funds to the RDFI. These entries are typically fraudulent payments resulting from an account takeover by an unauthorized third party. Please report any third-party ACH transactions, regardless of whether your accountholder recovered the funds. If your answer is **No** to item **2)** above, please report "0" ACH credit entries originated by your institution here.

Include:

- Only fraudulent, cleared and settled ACH credit transactions originated by your institution that were not authorized by your institution's accountholders (third-party fraud). If the fraudulent transaction was on-us, "cleared and settled" means that the funds were made available to the receiving accountholder.
- Fraudulent on-us ACH credit transactions

Do not include:

- ACH fraud attempts that were prevented before all funds were made available to the RDFI
- Returns solely for reason codes R05, R07, R10, R29, or R51 (i.e., verify with your fraud department that the unauthorized transaction was actual fraud and that the transaction settled with the RDFI)
- Fraud committed by your institution's accountholders (first-party fraud)
- Fraud committed by a valid accountholder (first-party fraud)
- Fraudulent ACH credit entries originated and authorized by a valid accountholder as part of a scam
- Fraudulent ACH credit entries that were originated by your institution and cleared and settled, but the funds were frozen and did not become available to the perpetrator at any time
- Fraudulent ACH credit entries received by your institution in which another institution was the ODFI
- Fraudulent ACH debit entries

► **Example 1:** A small business accountholder at your institution originated vendor payments via ACH through your online portal. His PC was compromised by malware, and his login credentials were stolen. The perpetrator originated 10 payments for $10,000 each to an account he maintains under a false name. The funds were then made available to the perpetrator's account after the transactions cleared and settled. In this example, you would report ten transactions for $100,000.

► **Example 2:** A small business accountholder at your institution originated salary payments via ACH through your online portal. The owner of the company fell out of favor with a recently fired employee, Joe. To wrongly retrieve the last salary payment to Joe, the owner of the company claimed that the last ACH transfer of funds to Joe was fraudulent. Your institution opened a fraud claim and verified that the transaction was not fraudulent. Since this is an example of first-party fraud (false claim of fraud), do not include this transaction in item **9)**.

9.a) Same-day settlement

These include only third-party, fraudulent, unauthorized ACH credit entries for which your institution was the ODFI and that resulted in a transfer of funds to the RDFI on the same day the ACH file was sent. Please report any third-party ACH transactions, regardless of whether or not your accountholder recovered the funds. If your answer is **No** to item **5)** above, please report "0" ACH credit entries your institution originated here.

Include:

- All third-party, fraudulent, ACH credit transactions cleared and settled on the same-day, for which your institution was the ODFI

Do not include:

- ACH fraud prevented before all funds were made available to the RDFI
- Fraudulent ACH credit entries received by your institution in which another institution was the ODFI
- Fraudulent ACH credit entries originated and settled non-same-day

► **Example 1:** A small business accountholder at your institution originates vendor payments via ACH through your online portal. His PC was compromised by malware, and his login credentials were stolen. The perpetrator originated five payments for $1,000 each to an account he maintains under a false name. The funds were made available to the perpetrator's account on the same day the transactions cleared. In this example, you would report five transactions for $5,000.

► **Example 2:** A small business accountholder at your institution originates vendor payments via ACH through your online portal. He recently acquired an expensive tool for his business and paid for it via ACH, and the funds settled on the same day the file was transferred. The tool malfunctioned after five days of use, and the vendor did not offer a warranty. Your accountholder claimed the ACH payment as fraud, since he felt the vendor was unethical by not offering to send a replacement tool or a refund. Since this is an example of first-party fraud (false claim of fraud), do not include this transaction in item **9.a**).

9.b) Non-same-day settlement

These include only third-party, fraudulent, unauthorized ACH credit entries for which your institution was the ODFI and that resulted in a transfer of funds to the RDFI on a different day from when the ACH file was sent. Please report any third-party ACH transactions, regardless of whether or not your accountholder recovered the funds.

Include:

- All third-party, fraudulent, ACH credit transactions cleared and settled non-same-day, for which your institution was the ODFI

Do not include:

- ACH fraud prevented before all funds were made available to the RDFI
- Fraudulent ACH credit entries received by your institution in which another institution was the ODFI
- Fraudulent ACH credit entries originated and settled same-day

► **Example 1:** A small business accountholder at your institution originates vendor payments via ACH through your online portal. His PC was compromised by malware, and his login credentials were stolen. The perpetrator originated three payments for $3,000 each to an account he maintains under a false name. The funds were made available to the perpetrator's account two days after the transactions cleared. In this example, you would report three transactions for $9,000.

► **Example 2:** A small business accountholder at your institution originates vendor payments via ACH through your online portal. He recently acquired an expensive tool for his business and paid for it via ACH, and the funds settled two days after the file was transferred. The tool malfunctioned after five days of use, and the vendor did not offer a warranty. Your accountholder claimed the ACH payment as fraud, since he felt the vendor was unethical by not offering to send a replacement tool or a refund. Since this is an example of first-party fraud (false claim of fraud), do not include this transaction in item **9.b**).

10) Total forward ACH debit entries your institution originated (ODFI debits)

These include all network, on-us, and direct exchange ACH debit entries for which your institution was the ODFI. Exclude returns. If your answer is **No** to item **3)** above, please report "0" here.

Include:

- In-house, on-us forward debit entries for which your institution was both the ODFI and RDFI
- Network forward ACH debits originated
- Network on-us debit entries for which your institution was both the ODFI and RDFI
- All direct exchange ACH debit entries for which you are the ODFI

Do not include:

- Returns
- Network offset ACH debit entries originated
- In-house, on-us offset ACH debit entries originated
- ACH entries received from other institutions
- Credit ACH entries originated
- Addenda records
- Zero-dollar entries

► **Example:** Your corporate customer billed 10 of its suppliers $100 each electronically through the ACH using your institution as its ODFI. Five of these employees have deposit accounts at your institution. To debit those 10 employees' accounts, your institution originated in-house on-us debit entries to avoid clearing fees from the Federal Reserve or EPN. One employee has a deposit account with an institution in which you have a direct exchange relationship. For this employee, your institution originated an ACH debit entry via direct exchange. For the other four employees, your institution originated ACH debit entries through the network. In this example, you would report ten transactions for $1,000.

11) Third-party fraudulent forward ACH debit entries your institution originated (fraudulent ODFI debits)

These include only third-party, fraudulent, unauthorized ACH debit entries that cleared and settled, for which your institution was the ODFI, and that resulted in transfer of funds from the RDFI. These entries are typically fraudulent payments resulting from an account takeover by an unauthorized third party. Please report any third-party ACH transactions, regardless of whether your accountholder recovered the funds. If your answer is **No** to item **3)** above, please report "0" here.

Include:

- Only fraudulent, cleared and settled ACH debit transactions originated by your institution that were not authorized by your institution's accountholders (third-party fraud). If the fraudulent transaction was on-us, "cleared and settled" means that the funds were made available to the receiving accountholder.
- Fraudulent on-us ACH debit transactions

Do not include:

- ACH fraud attempts that were prevented before all funds were made available to the RDFI
- Returns solely for reason codes R05, R07, R10, R29, or R51 (i.e., verify with your fraud department that the unauthorized transaction was actual fraud and that the transaction settled with the RDFI)
- Fraud committed by your institution's accountholders (first-party fraud)
- Fraud committed by a valid accountholder (first-party fraud)
- Fraudulent ACH debit entries originated and authorized by a valid accountholder as part of a scam
- Fraudulent ACH debit entries that were originated by your institution and cleared and settled, but the funds were frozen and did not become available to the perpetrator at any time
- Fraudulent ACH debit entries received by your institution in which another institution was the ODFI
- Fraudulent ACH credit entries

► **Example:** Jill is a small business accountholder at your institution. Her PC was compromised by malware, and her login credentials were stolen. The perpetrator originated ten fake bills for $10,000 each to ten of Jill's suppliers. The perpetrator maintained control of your client's account while the transactions cleared and settled, so the funds were made available to him. In this example, you would report ten transactions for $100,000.

ACH Receipts and Outgoing Returns

12) Total forward ACH credit entries your institution received (RDFI credits)

These include all network, on-us, and direct exchange ACH credit entries for which your institution was the RDFI. Exclude all offset ACH credit entries received.

Include:

- In-house, on-us forward credit entries for which your institution was both the ODFI and RDFI
- Network forward ACH credits received
- Network on-us credit entries for which your institution was both the ODFI and RDFI
- All direct exchange ACH credit entries for which you are the RDFI

Do not include:

- Returns
- Network offset ACH credit entries received
- In-house, on-us offset ACH credit entries received
- ACH entries originated from other institutions
- Debit ACH entries received
- Addenda records
- Zero-dollar entries

► **Example:** Your accountholder has signed up for direct deposit with his employer that is not an accountholder at your institution. His employer pays his salary of $7,000 through ACH each month. Your institution receives the ACH credit entries on behalf of your customer. In this example, you would report twelve transactions for $84,000.

13) Third-party fraudulent forward ACH credit entries your institution received (fraudulent RDFI credits)

These include only third-party, fraudulent, unauthorized ACH credit entries that cleared and settled and resulted in a transfer of funds to your institution (the RDFI). These entries are typically fraudulent payments resulting from an account takeover by an unauthorized third party that are then sent to your accountholder.

Include:

- Only fraudulent, cleared and settled ACH credit transactions that were not authorized by that institution's accountholders (third-party fraud), and were then received by your institution
- Fraudulent ACH credit network entries received
- Fraudulent ACH credit on-us entries received
- Fraudulent ACH credit direct exchange entries received

Do not include:

- ACH fraud attempts that were prevented before all funds were made available to the RDFI (your institution)
- Returns solely for reason codes R05, R07, R10, R29, or R51 (i.e., verify with your fraud department that the unauthorized transaction was actual fraud, and that the transaction settled with the ODFI)
- Fraud committed by your institution's accountholders (first-party fraud)
- Fraud committed by a valid accountholder (first-party fraud)
- Fraudulent ACH credit entries originated and authorized by a valid accountholder as part of a scam
- Fraudulent ACH credit entries that were received by your institution and cleared and settled, but the funds were frozen and did not become available to the perpetrator at any time
- Fraudulent ACH credit entries originated by your institution, in which another institution was the RDFI
- Fraudulent ACH debit entries

► **Example:** A small business accountholder at another institution originated vendor payments via ACH through their online portal. His PC was compromised by malware, and his login credentials were stolen. The perpetrator originated 10 payments for $10,000 each to accounts he maintains under a false name, five of which were at your institution. The funds were then made available to the perpetrator's account after the transactions cleared and settled. The accountholder's institution identified the fraud and asked your institution to return the fraudulent payments. In this example, you would report five transactions that your institution received for $50,000.

14) Total forward ACH debit entries your institution received (RDFI debits) = 14.a) + 14.b) +14.c)

These include all network, on-us, and direct exchange ACH debit entries for which your institution was the ODFI.

Include:

- In-house, on-us forward debit entries for which your institution was both the ODFI and RDFI
- Network forward ACH debits received
- Network on-us debit entries for which your institution was both the ODFI and RDFI
- All direct exchange ACH debit entries for which your institution is the RDFI

Do not include:

- Returns
- Network offset ACH debit entries received
- In-house, on-us offset ACH debit entries received
- ACH entries originated from other institutions
- Credit ACH entries received
- Addenda records
- Zero-dollar entries

► **Example:** Your customer has set up direct debit of his checking account for recurring, monthly insurance bill payments of $75. His biller, the insurance company, originated debit entries through another depository institution (i.e., the ODFI), and your institution received and posted these debit entries to your customer's account. In this example, you would report twelve transactions for $900.

14.a) Network ACH debit entries received

These are debit entries for which your institution was the RDFI (but not the ODFI), and the debit entry was cleared through a network operator (i.e., the Federal Reserve or EPN). Please refer to the **General Terminology** section above for the definition of "network" entries.

Include:

- Network non-offset ACH debit entries received

Do not include:

- Returns
- ACH entries cleared directly between your institution and another (i.e., direct exchange ACH entries)
- Network offset ACH debit entries received

► **Example:** Your customer has set up direct debit of his checking account for a recurring, monthly cell phone bill payment of $50. His biller, the cell phone company, originated debit entries through another depository institution (i.e., the ODFI), and your institution received and posted these debit entries to your customer's account. In this example, you would report twelve transactions for $600.

14.b) In-house on-us ACH debit entries received

These include all ACH debit entries that were not cleared through the Federal Reserve or EPN, for which your institution was both the ODFI and RDFI, and that were originated for the purpose of moving funds from one account to another at your institution. If your answer is **No** to item **3)** above, please report "0" here.

Include:

- In-house on-us non-offset debit entries for which your institution was both the ODFI and RDFI

Do not include:

- Returns
- In-house on-us offset ACH debit entries received
- In-house on-us credits your institution originated
- Addenda records
- Zero-dollar entries

► **Example:** Your corporate customer, a cable company, collected monthly payments from its customers by originating ACH debit entries using your institution as its ODFI. Twenty of those cable company customers also have a deposit account at your institution. To debit the accounts of those customers, your institution originated in-house on-us debit entries for $45 each to avoid clearing fees from the Federal Reserve or EPN. In this example, you would report two hundred forty transactions for $1,800.

14.c) Direct exchange ACH debit entries received

These include all ACH debit entries received and not cleared through the Federal Reserve or EPN. Please refer to the **General Terminology** section above for the definition of "Direct Exchange" entries.

Include:

- All direct exchange ACH debit entries for which you are the RDFI

Do not include:

- Returns
- Debit ACH entries originated
- In-house on-us credit entries your institution originated
- Addenda records
- Zero-dollar entries

► **Example:** A cable company that is not your corporate customer collected monthly payments of $30 from its customers by originating ACH debit entries using a different institution as its ODFI. Ten of those customers bank at your institution. Your institution has established direct exchange relationships with the ODFI to avoid clearing fees from the Federal Reserve or EPN. To debit the accounts of those customers, your institution received debit entries via direct exchange. Please report one hundred twenty transactions for $3,600.

15) Total forward ACH debit entries your institution received (RDFI debits) (repeat item 14) = 15.a) + 15.b)

Repeat item **14)** above. These are all network, on-us, and direct exchange ACH debit entries for which your institution was the RDFI.

Include:

- In-house on-us forward debit entries for which your institution was both the ODFI and RDFI
- Network forward ACH debits received
- Network on-us debit entries for which your institution was both the ODFI and RDFI
- All direct exchange ACH debit entries for which you were the RDFI

Do not include:

- Returns
- Network offset ACH debit entries originated
- In-house on-us offset ACH debit entries originated
- ACH entries received from other institutions
- Credit ACH entries received
- Addenda records
- Zero-dollar entries

► **Example:** Your customer has set up direct debit of his checking account for recurring, monthly insurance bill payments of $75. His biller, the insurance company, originated debit entries through another depository institution (i.e., the ODFI). Your institution received and posted these debit entries to your customer's account. In this example, you would report twelve transactions for $900.

15.a) For consumer accounts

Please refer to the **General Terminology** section above for the definition of consumer accounts.

Include:

- All ACH debits received from consumer accounts, for which your institution was the RDFI

Do not include:

- Any ACH debits received from business/government accounts, for which your institution was the RDFI

► **Example:** Your consumer customer, Paul, received a bill payment of $500 from his landlord, which was sent electronically through the ACH. Your institution received the debit entry on behalf of Paul. In this example, you would report one transaction for $500.

15.b) For business/government accounts

Please refer to the **General Terminology** section above for the definition of business/government accounts.

Include:

- All ACH debits received from business/government accounts, for which your institution was the RDFI

Do not include:

- Any ACH debits received from consumer accounts, for which your institution was the RDFI

► **Example:** Your corporate customer, Bill's Paint Supply, received 5 bill payments of $2,000 from its suppliers, each sent electronically through the ACH. Your institution received the debit entries on behalf of your customer. In this example, you would report five transactions for $10,000.

16) Total forward ACH debit entries your institution received (RDFI debits) (repeat item 14) = 16.a) + 16.b)

Repeat item **14)** above. These are all network, on-us, and direct exchange ACH debit entries for which your institution was the RDFI.

Include:

- In-house on-us forward debit entries for which your institution was both the ODFI and RDFI
- Network forward ACH debits received
- Network on-us debit entries for which your institution was both the ODFI and RDFI
- All direct exchange ACH debit entries for which you were the RDFI

Do not include:

- Returns
- Network offset ACH debit entries originated
- In-house on-us offset ACH debit entries originated
- ACH entries received from other institutions
- Credit ACH entries received
- Addenda records
- Zero-dollar entries

► **Example:** Your customer has set up direct debit of his checking account for recurring, monthly insurance bill payments of $75. His biller, the insurance company, originated debit entries through another depository institution (i.e., the ODFI). Your institution received and posted these debit entries to your customer's account. In this example, you would report twelve transactions for $900.

16.a) Same-day settlement

These are debit entries for which your institution was the RDFI, and the payment was settled on the same day. Please refer to the **General Terminology** section above for the definition of same-day ACH entries.

Include:

- All ACH debits received and settled same-day, for which your institution was the RDFI

Do not include:

- Any ACH debits received and settled non-same-day, for which your institution was the RDFI

► **Example:** Your corporate customer, Mike's Hardware, received a one-time bill payment for $2,500 from one of its customers, Sally's Supplies, through the ACH network. Sally's Supplies does not bank with your institution. Since the payment of this bill was urgent, Sally's Supplies decided to use the same-day settlement option. In this example, you would report one entry for $2,500.

16.b) Non-same-day settlement

These are debit entries for which your institution was the RDFI, and the payment was settled on a later day after the settlement file was transmitted.

Include:

- All ACH debits received and settled non-same-day, for which your institution was the RDFI

Do not include:

- Any ACH debits received and settled same-day, for which your institution was the RDFI

► **Example:** Your customer has set up direct debit of his checking account for a recurring, monthly cell phone bill payment of $50. His biller, the cell phone company, originated debit entries through another depository institution (i.e., the ODFI). Your institution received and posted these debit entries to your customer's account. The settlement of money occurred on a different day than the transmission of the file. In this example, you would report twelve transactions for $600.

17) Third-party fraudulent forward ACH debit entries your institution received (fraudulent RDFI debits) = 17.a) + 17.b)

Third-party, fraudulent, unauthorized ACH debit entries that cleared and settled, for which your institution was the RDFI, and that resulted in a transfer of funds to the ODFI.

Include:

- Any fraudulent, third-party ACH transactions, regardless of whether or not your accountholder recovered the funds.

Do not include:

- ACH fraud attempts that were prevented before all funds were made available to the ODFI
- Returns solely for reason codes R05, R07, R10, R29, or R51 (i.e., verify with your fraud department that the unauthorized transaction was actual fraud and that the transaction settled with the ODFI)
- Fraudulent ACH debit received and authorized by a valid accountholder as part of a scam (first-party fraud)
- Fraudulent ACH debit entries received that cleared and settled, but the funds were frozen and did not become available to the perpetrator at any time
- Fraudulent ACH debit entries originated by your institution, in which another institution was the RDFI
- Fraudulent ACH credit entries

► **Example 1:** A fraudster opened a commercial bank account for a fictitious housecleaning service at another institution. He then originated unauthorized bill payments for hundreds of consumer accounts, five of which were at your institution. Each of those accounts was debited once for $200. The received debit ACH transactions cleared and settled with the ODFI. The $1,000 debited from your accountholders was made available to the fraudster's account. In this example, you would report five transactions for $1,000.

► **Example 2:** Jim is an accountholder at your institution. He lost his job and has not been able to find employment in the last six months. His cellphone provider originated an ACH debit transaction for his monthly bill of $150. The transaction cleared and settled a day later, but Jim claimed the transaction as fraudulent since he needs the $150 to pay part of his rent. Since this transaction is an example of first-party fraud (false claim of fraud), it should not be included in item **17**).

17.a) Same-day settlement

These include only third-party, fraudulent, unauthorized ACH debit entries that cleared and settled on the same day as the transmission, for which your institution was the RDFI, and that resulted in transfer of funds to the ODFI. Please report any fraudulent, third-party ACH transactions, regardless of whether or not your accountholder recovered the funds.

Include:

- All third-party, fraudulent, ACH debit transactions cleared and settled on the same-day, for which your institution was the RDFI

Do not include:

- ACH fraud attempts that were prevented before all funds were made available to the ODFI
- Returns solely for reason codes R05, R07, R10, R29, or R51 (i.e., verify with your fraud department that the unauthorized transaction was actual fraud, and that the transaction settled with the ODFI)
- Fraudulent ACH debit received and authorized by a valid accountholder as part of a scam (first-party fraud)
- Fraudulent ACH debit entries originated by your institution in which another institution was the RDFI
- Fraudulent ACH credit entries

► **Example:** A fraudster opened a commercial bank account for a fictitious gardening company at another institution and originated unauthorized bill payment for one of your accountholders for $1,000, using the same-day settlement option. The received debit cleared and settled (on the same day) for $1,000. In this example, you would report one transaction for $1,000.

17.b) Non-same-day settlement

These include only third-party, fraudulent, unauthorized ACH debit entries that settled on a later date than file transmission, for which your institution was the RDFI, and that resulted in the transfer of funds to the ODFI. Please report any fraudulent, third-party ACH transactions, regardless of whether or not your accountholder recovered the funds.

Include:

- All third-party, fraudulent, ACH debit transactions cleared and settled non-same-day, for which your institution was the RDFI

Do not include:

- ACH fraud attempts that were prevented before all funds were made available to the ODFI
- Returns solely for reason codes R05, R07, R10, R29, or R51 (i.e., verify with your fraud department that the unauthorized transaction was actual fraud, and that the transaction settled with the ODFI)
- Fraudulent ACH debit received and authorized by a valid accountholder as part of a scam (first-party fraud)
- Fraudulent ACH debit entries originated by your institution in which another institution was the RDFI
- Fraudulent ACH credit entries

► **Example 1:** A fraudster opened a commercial bank account for a fictitious house-cleaning service at another institution and originated unauthorized bill payments for hundreds of consumer accounts. Five of those accounts were at your institution, and each was debited once for $200 (not on the same day as the file transmission). The received debit ACH transactions cleared and settled with the ODFI on a different day. The $1,000 debited from your accountholders was made available to the fraudster's account. In this example, you would report five transactions for $1,000.

► **Example 2:** Jim is an accountholder at your institution. He lost his job and has not been able to find employment in the last six months. His cellphone provider originated an ACH debit transaction for his monthly bill of $150. The transaction cleared and settled non-same day, but Jim claimed the transaction as fraudulent since he needs the $150 to pay part of his rent. Since this transaction is an example of first-party fraud (false claim of fraud), you would not include it in item **17.b**).

18) ACH outgoing debit returns (i.e., debit return entries your institution originated including "on-us" debit returns)

These are ACH debit entries that your institution received and were subsequently returned by your institution, the RDFI.

Include:

- All outgoing ACH debit entries that your institution returned unpaid (whether to another institution or to your own accountholders)

Do not include:

- ACH entries returned to your institution unpaid by another institution (incoming)

► **Example:** Your customer pays his utility bill through the utility company's website. The utility company's bank (which may or may not be your institution) originates a debit ACH entry for $86. However, your customer's account has insufficient funds, and your institution returns the ACH entry unpaid. In this example, you would report one transaction for $86.

Wire Transfers Originated (Outgoing)

GENERAL TERMINOLOGY

Consumer

An account for personal use by an individual or household from which wire transfers can be originated, and by which wire transfers can be received.

Business/government

An account owned by an organization (i.e., business, government or not-for-profit organization) from which wire transfers can be originated and by which wire transfers can be received.

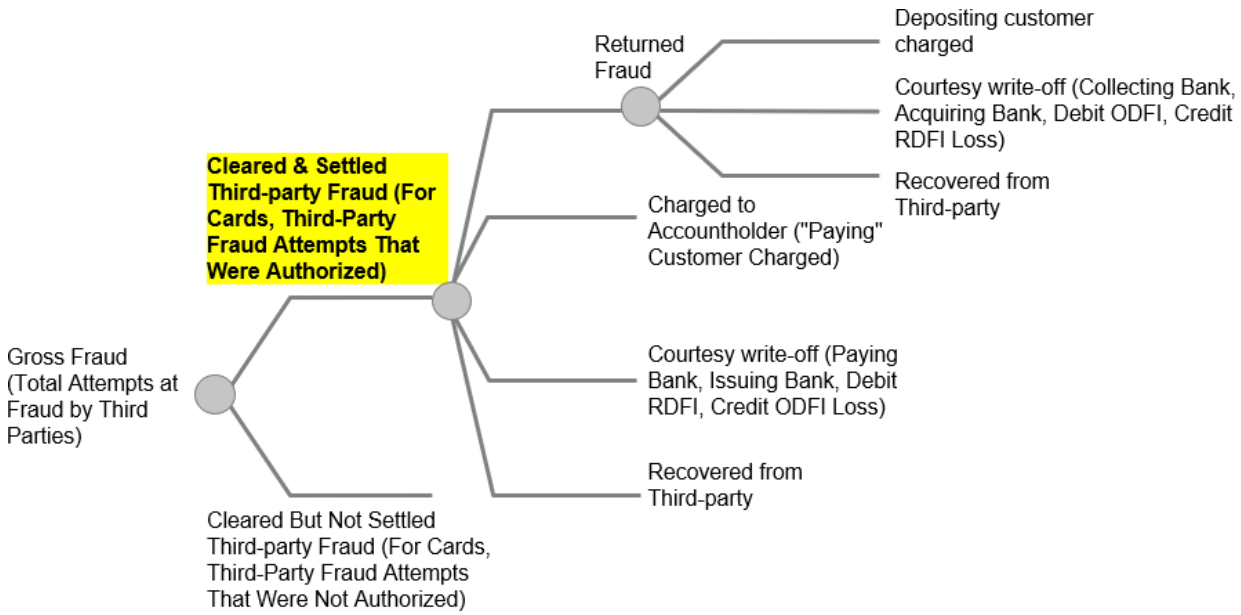
Note: Please report wire transfers originated from or received by small business accounts under business/government accounts, if possible.

U.S. domiciled account

Accounts located within the 50 U.S. states, D.C., or U.S. territories such as Guam, Puerto Rico, or U.S. Virgin Islands). Only report data associated with your institution's U.S. domiciled accounts, including transactions that are domestic and cross-border.

Third-party fraud

The Federal Reserve Payments Study has identified a measure of fraud that can be described as cleared and settled third-party fraudulent transactions. This measure is not a loss-of-funds measure, nor is it a measure of fraud attempts; rather, it is a measure of the extent to which third parties who are not authorized to conduct transactions are able to penetrate the payment system and effect settlement between banks, or create a book transfer of funds if the transaction happens within one 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 manages to create a 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.



SURVEY ITEMS

1) Did your institution originate wires on behalf of an unaffiliated depository institution during calendar year 2018 (i.e., correspondent volume)?

If your answer to this question is **No**, please skip item **1.a)** below.

1.a) If your answer is "Yes" to item 1) above, are you able to exclude these volumes from your answers below?

If your answer is **Yes, in some cases**, please explain in the comments box at the end of the Wire Transfers section.

2) Did an unaffiliated depository institution originate wires on behalf of your institution during calendar year 2018?

If your answer to this question is **No**, please skip item **2.a)** below.

2.a) If your answer is "Yes" to item 2) above, are you able to include these volumes from your answers below?

If your answer is **Yes, in some cases**, please explain in the comments box at the end of the Wire Transfers section.

3) Total wire transfer originations (outgoing) = 3.a) + 3.b)

These include all wire transfers originated by your institution's U.S. domiciled accountholders with either a domestic or foreign beneficiary.

Include:

- Funds transfers originated using the large-value systems (i.e., Fedwire and CHIPS)
- Payments that your institution's accountholders submitted and settled through these systems directly or through a correspondent (i.e., wire transfers originated on your institution's behalf by a correspondent)
- Book transfers (i.e., internal transfers using your institution's wire platform)
- All wire transfers originated for the purpose of paying one of your institution's vendors or settling your institution's position with another institution (i.e., settlement/bank business wire transfers)

Do not include:

- Wire transfers your institution originated on behalf of an unaffiliated depository institution (i.e., correspondent volume)

► **Example:** Your institution originated a $15,000 wire transfer on behalf of your corporate customer to pay its third-party vendor via Fedwire. The vendor may or may not have a depository relationship with your institution. The vendor may or may not have a U.S. domiciled account. In this example, you would report one transaction for $15,000.

3.a) Consumer originated wire transfers

All wire transfers originated from consumer accounts of any type at your institution. Please see the **General Terminology** section above for the definition of consumer accounts.

Include:

- Wire transfers originated from consumer accounts of any type

Do not include:

- Wire transfers originated from business/government accounts
- Wire transfers your institution originated on behalf of an unaffiliated depository institution (i.e., correspondent volume)

► **Example:** Your institution originated a wire transfer for $10,000 on behalf of your consumer customer to pay his daughter's college tuition. Your institution originated the wire on behalf of your customer to the school to fund his daughter's college tuition via Fedwire. The school may or may not have a depository relationship with your institution. The school may or may not have a U.S. domiciled account. In this example, you would report one transaction for $10,000.

3.b) Business/government originated wire transfers = 3.b.1) + 3.b.2)

Wire transfers originated from business/government (including non-depository financial institutions) accounts of any type at your institution. Please include small business accounts under business/government accounts. Please see the **General Terminology** section above for the definition of business/government accounts.

Include:

- Wire transfers originated from business/government accounts

Do not include:

- Wire transfers originated from consumer accounts of any type
- Wire transfers your institution originated on behalf of an unaffiliated depository institution (i.e., correspondent volume)

► **Example:** Your corporate customer made three wire transfers of $25,000 each through your institution's wire platform to pay his suppliers. The vendor may or may not have a depository relationship with your institution. And the vendor may or may not have a U.S. domiciled account. In this example, you would report three wire transactions for $75,000.

3.b.1) Settlement/bank business originated wire transfers

All wire transfers originated for the purpose of paying one of your institution's vendors or settling your institution's position with another institution.

Include:

- Settlement/bank business wire transfers

Do not include:

- Wire transfers originated from consumer or business/government accounts.
- Wire transfers your institution originated on behalf of an unaffiliated depository institution (i.e., correspondent volume)

► **Example:** Your institution originated a wire transfer of $12,000 via Fedwire to pay the bank's advertising agency. In this example, you would report one wire transaction for $12,000.

3.b.2) All other business/government originated wire transfers

All other wire transfers originated from business/government (including non-depository financial institutions) accounts at your institution.

Include:

- Wire transfers originated business/government accounts.

Do not include:

- Consumer wire transfers or settlement/bank business transfers
- Wire transfers your institution originated on behalf of an unaffiliated depository institution (i.e., correspondent volume)

► **Example:** Your institution originated a wire transfer of $5,000 on behalf of your corporate customer to pay its third-party vendor via Fedwire. The vendor may or may not have a depository relationship with your institution. The vendor may or may not have a U.S. domiciled account. In this example, you would report one wire transaction for $5,000.

4) Total wire transfer originations (outgoing) (repeat item 3) = 4.a) + 4.b)

Repeat item **3)** above. These include all wire transfers originated by your institution's U.S. domiciled accountholders with either a domestic or foreign beneficiary.

Include:

- Funds transfers originated using the large-value systems (i.e., Fedwire and CHIPS)
- Payments that your institution's accountholders submitted and settled through these systems directly or through a correspondent (i.e., wire transfers originated on your institution's behalf by a correspondent)
- Book transfers (i.e., internal transfers using your institution's wire platform)
- All wire transfers originated for the purpose of paying one of your institution's vendors or settling your institution's position with another institution (i.e., settlement/bank business wire transfers)

Do not include:

- Wire transfers your institution originated on behalf of an unaffiliated depository institution (i.e., correspondent volume)

► **Example:** Your institution originated a $15,000 wire transfer on behalf of your corporate customer to pay its third-party vendor via Fedwire. The vendor may or may not have a depository relationship with your institution. The vendor may or may not have a U.S. domiciled account. In this example, you would report one transaction for $15,000.

4.a) Domestic (U.S.) payee

These include all wire transfers originated by your institution's U.S. domiciled accountholders (i.e., those accounts located in the 50 U.S. states, D.C., or U.S. territories) to a domestic beneficiary.

Include:

- Wire transfers sent to a domestic (U.S) payee

Do not include:

- Wire transfers sent to a foreign payee

► **Example:** Your institution originated a wire transfer for $10,000 on behalf of your New York based corporate customer to pay its third-party vendor, also located in New York, via Fedwire. Your client is a U.S. domiciled accountholder. In this example, you would report one transaction for $10,000.

4.b) Foreign payee

These include all wire transfers originated by your institution's U.S. domiciled accountholders to a foreign beneficiary.

Include:

- Wire transfers sent to a foreign payee

Do not include:

- Wire transfers sent to a domestic (U.S) payee

► **Example:** Your institution originated a wire transfer for $10,000 on behalf of your New York based corporate customer to pay its third-party vendor, located in Spain, via Fedwire. Your client is a U.S. domiciled accountholder. In this example, you would report one transaction for $10,000.

5) Total wire transfer originations (outgoing) (repeat item 3) = 5.a) + 5.b)

Repeat item **3)** above. These include all wire transfers originated by your institution's U.S. domiciled accountholders with either a domestic or foreign beneficiary, sent through a network/correspondent bank or book transfers.

Include:

- Funds transfers originated using the large-value systems (i.e., Fedwire and CHIPS)
- Payments that your institution's accountholders submitted and settled through these systems directly or through a correspondent (i.e., wire transfers originated on your institution's behalf by a correspondent)
- Book transfers (i.e., internal transfers using your institution's wire platform)
- All wire transfers originated for the purpose of paying one of your institution's vendors or settling your institution's position with another institution (i.e., settlement/bank business wire transfers)

Do not include:

- Wire transfers your institution originated on behalf of an unaffiliated depository institution (i.e., correspondent volume)

► **Example:** Your institution originated a $15,000 wire transfer on behalf of your corporate customer to pay its third-party vendor via Fedwire. The vendor may or may not have a depository relationship with your institution. The vendor may or may not have a U.S. domiciled account. In this example, you would report one transaction for $15,000.

5.a) Sent through a network (i.e., Fedwire or CHIPS) or a correspondent bank

These are wire transfers sent through a network (i.e., Fedwire or CHIPS) or a correspondent bank

Include:

- All wire transfers sent through a network (i.e., Fedwire or CHIPS) or a correspondent bank

Do not include:

- Book transfers (i.e., internal transfers using your institution's wire platform)

► **Example:** Your institution originated a wire transfer for $10,000 on behalf of your corporate customer to pay its third-party vendor via Fedwire. The vendor does not have a depository relationship with your institution. In this example, you would report one transaction for $10,000.

5.b) Book transfers (i.e., internal transfers using your institution's wire platform)

These are internal wire transfers that were made using your wire platform. These are sometimes referred to as book transfers.

Include:

- All internal wire transfers that were made using your wire platform

Do not include:

- Wires that are sent through a network (i.e., Fedwire or CHIPS) or a correspondent bank

► **Example:** Your corporate customer has multiple accounts at your institution, and your institution allows this customer to transfer money among these accounts as a service. These wires are sent over your internal wire platform rather than over a network. Your customer made a wire transfer of $25,000 through your institution's wire platform for this purpose. In this example, you would report one wire transaction for $25,000.

6) Third-party fraudulent wire transfer originations = 6.a) + 6.b)

These include all third-party fraudulent unauthorized wire transfer originations that subsequently cleared and settled. Please report any third-party fraudulent wire originations, regardless of whether those funds were subsequently recovered through the wire return process or by other means.

Include:

- Fraudulent funds transfers originated using the large-value systems (i.e., Fedwire and CHIPS), including those originated on your institution's behalf by a correspondent
- Fraudulent book transfers (i.e., internal transfers using your institution's wire platform)

Do not include:

- Fraud originations that were prevented
- Fraudulent wire transfers received by your institution
- Fraud committed by a valid accountholder (first-party fraud)
- Wire transfers originated and authorized by a valid accountholder as part of a scam

► **Example 1:** A small business accountholder at your institution originated a wire payment through your online portal. His PC was compromised by malware, and his login credentials were stolen. The perpetrator originated a wire for $5,000 to an account at your institution and a wire for $10,000 to an account at another institution, both of which accounts were maintained under a false name. The transactions cleared and settled, and the funds became available to the perpetrator. In this example, you would report two transactions for $15,000.

► **Example 2:** Jennifer, a small business accountholder at your institution, originated a wire payment of $40,000 to her brother through your online portal. After a heated conversation with her brother, Jennifer decided to recover the money that had been transferred to him. She opened a fraudulent claim with your institution, stating that her brother had logged in to her account and made the wire transfer to his account without her consent. Your institution was able to verify that this was a false, fraudulent claim and that there was no wrongdoing in the transfer of funds. Since this transaction is an example of first-party fraud (false claim of fraud), it should not be included in item **6**).

6.a) Domestic (U.S) payee

These include all third-party fraudulent unauthorized wire transfers originated from your institution's U.S. domiciled accounts (i.e., those accounts located in the 50 U.S. states, D.C., or U.S. territories) to a domestic beneficiary. Please report any third-party fraudulent wire originations, regardless of whether those funds were subsequently recovered through the wire return process or by other means.

Include:

- Fraudulent wire transfers sent to a domestic (U.S) payee

Do not include:

- Fraudulent wire transfers sent to a foreign payee
- Fraud originations that were prevented
- Fraudulent wire transfers received by your institution
- Fraud committed by a valid accountholder (first-party fraud)
- Wire transfers originated and authorized by a valid accountholder as part of a scam

► **Example:** John is an accountholder at your institution. His email was hacked, and the perpetrator used his username and password to login to his bank account. The perpetrator originated a wire transfer for $5,000 to a second account in New York maintained under a false name, which subsequently cleared and settled in the perpetrator's account. A transfer of funds occurred between the originating and receiving accounts. The receiving account was with an unaffiliated institution. In this example, you would report one transaction for $5,00

6.b) Foreign payee

These include all third-party fraudulent unauthorized wire transfers originated from your institution's U.S. domiciled accounts to a foreign beneficiary. Please report any third-party fraudulent wire originations, regardless of whether those funds were subsequently recovered through the wire return process or by other means.

Include:

- Fraudulent wire transfers sent to a foreign payee

Do not include:

- Fraudulent wire transfers sent to a domestic (U.S) payee
- Fraud originations that were prevented
- Fraudulent wire transfers received by your institution
- Fraud committed by a valid accountholder (first-party fraud)
- Wire transfers originated and authorized by a valid accountholder as part of a scam

► **Example:** Carlos is an accountholder at your institution. He buys and sells antiques at an online auction website for a living. The auction website was compromised, and his username, password, and bank account information were stolen online. The perpetrator originated two wire transfers from Carlos' account for $5,000 each to two separate accounts in France, neither of which are affiliated with your institution. Both transfers cleared and settled. In this example, you would report two transactions for a total of $10,000.

Wire Transfers Received (Incoming)

7) Total wire transfer receipts (incoming)

All wire transfers received by your institution which were sent through a network or a correspondent bank, as well as internal book transfers.

Include:

- Funds transfers received using the large-value systems (i.e., Fedwire and CHIPS), including those originated on your institution's behalf by a correspondent
- Internal book transfers

Do not include:

- Wire transfers your institution received from an unaffiliated depository institution.

► **Example:** Your institution received a $3,000 wire transfer on behalf of your corporate customer, Joe's Grocery, from their client via Fedwire. Joe's Grocery's client may or may not have a depository relationship with your institution, and they may or may not have a U.S. domiciled account. In this example, you would report one wire transaction for $3,000.

8) Third-party fraudulent wire transfer receipts (incoming)

These include all third-party fraudulent wire transfers received by your institution which were sent through a network or a correspondent bank, as well as internal book transfers. These fraudulent transactions subsequently cleared and settled. Please report any third-party fraudulent wire receipts, regardless of whether those funds were subsequently recovered through the wire return process or by other means.

Include:

- Fraudulent funds transfers received using the large-value systems (i.e., Fedwire and CHIPS), including those originated on your institution's behalf by a correspondent

Do not include:

- Fraudulent wire transfers originated by your institution
- Fraud committed by a valid accountholder (first-party fraud)
- Wire transfers originated and authorized by a valid accountholder as part of a scam

► **Example:** A hacker compromised a Joe's PC by malware and stole his login credentials. The perpetrator originated a wire for $10,000 to an account at your institution, which was maintained under a false name. The transaction cleared and settled, and the funds became available to the perpetrator. Joe alerted his institution of the fraudulent transaction, and they subsequently reached out to your institution for a return of the fraudulent wire payment. In this example, you would report one transaction for $10,000.

Non-Prepaid Debit Cards

GENERAL TERMINOLOGY

Non-prepaid debit card transactions

All purchase and bill-pay transactions made with debit cards used for point-of-sale (POS) transactions. These transactions can be authenticated by either a Personal Identification Number (PIN), signature, EMV, online authorization, or any other digital method (e.g., NFC, QR code). Transactions may originate, for example, at a physical point of sale, via telephone, or via the internet. For this study, please follow these guidelines:

Non-prepaid debit card transactions include…	Non-prepaid debit card transactions do <u>not</u> include…
▪ Transactions made with Visa, MasterCard, Discover, or American Express branded cards and cleared over dual-message networks. These are typically called signature-based or offline debit card transactions. ▪ POS transactions made with debit cards and cleared over a general-purpose single-message network. These are typically called PIN-based or online debit card transactions. ▪ Transactions originated in other countries	▪ ATM withdrawals ▪ Credit card transactions ▪ Prepaid card transactions ▪ Transfers by a corporate customer to fund its employees' payroll card accounts ▪ Electronic benefits transfer (EBT) card transactions ▪ Payroll card transactions by the cardholder

Digital Wallet

All purchase and bill-pay transactions made using a digital wallet in which users can complete purchases using near-field communication (NFC) that works in conjunction with mobile payment systems, MST (magnetic secure transmission) transactions, QR code transactions, barcode transactions, in-app transactions, or browser transactions. Digital wallets can be used during in-person transactions or remote transactions. In-person transactions require the payment holder to be present to use their digital wallet, while remote transactions are used during e-commerce sales in which the authorization and transaction processes are not physically close to each other.

Digital wallet transactions include those made by using electronic devices, such as a smartphone, smart watch, or activity tracker, by "tapping" the device at the POS terminal (i.e., Apple Pay, Samsung Pay, Google Pay, Fitbit Pay, Masterpass).

They also include tokenized digital wallet transactions made by using customer's payment credentials saved in a virtual account number. These credentials can be stored either on a smartphone or in the cloud. When making a purchase, a substitute account number and a transaction specific code ("token") are used to process payments. This can include purchasing items online with a computer or using a smartphone to make a purchase with a browser or in-app (i.e., Apple Pay, Google Pay, Masterpass, Visa Checkout, Amex Express Checkout).

Contactless Card

A contactless card payment is a secure method for consumers to purchase products or services via debit smartcards (also known as chip cards) using RFID technology. To make a contactless payment, the user simply tap his or her debit card near a POS terminal (an action sometimes referred to as "tap-and-go" or "tap-and-pay").

Consumer account

A non-prepaid debit card account for personal use by an individual or household from which payments can be made or to withdraw cash from an ATM.

Business/government account

A non-prepaid debit card account owned by an organization (i.e., business, government or not-for-profit organization)from which payments can be made or to withdraw cash from an ATM.

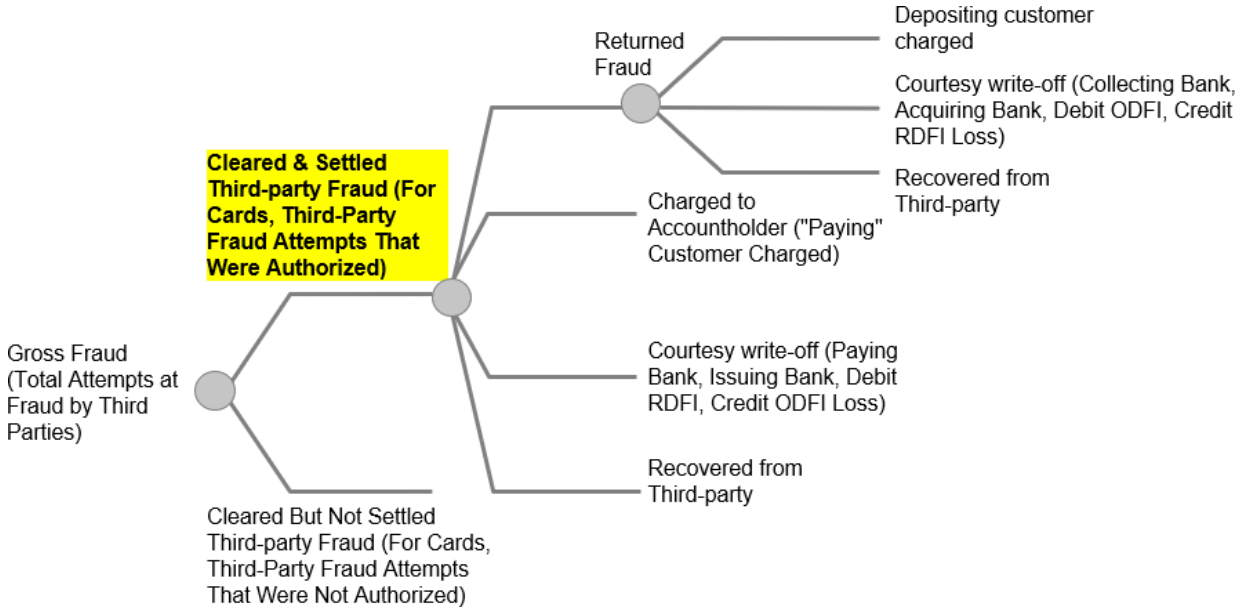
Note: Please report small business accounts under business/government accounts, if possible.

U.S. domiciled account

Accounts located within the 50 U.S. states, D.C., or U.S. territories such as Guam, Puerto Rico, or U.S. Virgin Islands). Only report data associated with your institution's U.S. domiciled accounts, including transactions that are domestic and cross-border.

Third-party fraud

The Federal Reserve Payments Study has identified a measure of fraud that can be described as cleared and settled third-party fraudulent transactions. This measure is not a loss-of-funds measure, nor is it a measure of fraud attempts; rather, it is a measure of the extent to which third parties who are not authorized to conduct transactions are able to penetrate the payment system and effect settlement between banks, or create a book transfer of funds if the transaction happens within one 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 manages to create a 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.



SURVEY ITEMS

1) Did your institution have non-prepaid debit cards in circulation in 2018 for which your institution was the issuer?

These include cards issued by your institution, including those that your institution issued, that are managed by a third-party, and that route transactions over a general-use debit card network. If your answer to this question is **No**, please report "0" for all items below.

Include:

- Debit cards associated with transaction deposit accounts reported in the Institution Profile section
- Debit cards (not including prepaid cards) that can be used to make purchases at the point of sale

Do not include:

- ATM-only cards that cannot be used to make purchases at the point of sale
- Prepaid cards
- Credit cards

1.a) If your answer is "Yes" to item 1) above, are you able to exclude general-purpose prepaid card transaction volumes from your answers below?

General-purpose prepaid card (including payroll card) transactions should only be included in the volumes reported in the General-Purpose Prepaid Cards section of the questionnaire.

If your answer is **Yes, in some cases**, please explain in the comments box at the end of the Non-Prepaid Debit Cards Section.

If your answer is **No**, please enter "NR" for any questions in which your institution can only report combined debit and prepaid transactions combined.

2) Number of non-prepaid debit cards = 2.a) + 2.b)

Report non-prepaid debit cards associated with transaction deposit accounts reported in the Institution Profile section.
For cards in force report only non-prepaid debit cards that can be used at the point of sale, were issued by your institution, activated by your institution's accountholders, have not expired at the end of a month, and draw on the transaction deposit accounts reported in item **2)** in the Institution Profile section.
For cards in force with purchase activity, report only non-prepaid debit cards that had at least one point-of-sale (POS) and/or bill pay activity during the time period. Do not include cards that were only used to withdraw cash.
Average of monthly totals means the average of end-of-month totals for each of the months in 2018.
If your answer is **No** to item **1**) above, please report "0" here.

Include:

- Debit cards associated with transaction deposit accounts reported in the Institution Profile section
- Debit cards (not including prepaid cards) that can be used to make purchases at the point of sale

Do not include:

- ATM-only cards that cannot be used to make purchases at the point of sale
- Prepaid cards
- Credit cards

► **Example:** Your institution has 500 consumer and business banking accounts, with 500 debit cards issued that are related to these accounts. Of these debit cards, 450 cards have been activated and are not expired, 30 cards have not been activated yet, and 20 cards have been activated but are now expired. Of the 450 cards that are active and not expired, 350 cards have been used to make at least one purchase in 2018. In this example, you would report 450 debit cards in force and 350 debit cards with purchase activity.

2.a) Consumer cards

These include all debit cards that draw on consumer accounts. Please see the **General Terminology** section above for the definition of consumer accounts.

Include:

- Debit cards associated with consumer transaction deposit accounts reported in the Institution Profile section
- Consumer debit cards (not including prepaid cards) that can be used to make purchases at the point of sale

Do not include:

- ATM-only cards that cannot be used to make purchases at the point of sale
- Consumer debit cards that can be used to make purchases at the point of sale
- Both consumer and business/government prepaid cards that can be used to make purchases at the point of sale
- Both consumer and business/government credit cards that can be used to make purchases at the point of sale

► **Example:** Your institution has 500 personal banking accounts, with 500 debit cards issued that are related to these accounts. Of these debit cards, 450 cards have been activated and are not expired, 30 cards have not been activated yet, and 20 cards have been activated but are now expired. Of the 450 cards that are active and not expired, 350 cards have been used to make at least one purchase in 2018. In this example, you would report 450 consumer debit cards in force and 350 consumer debit cards with purchase activity.

2.b) Business/government cards

These include all debit cards that draw on business/government accounts. Please see the **General Terminology** section above for the definition of business/government accounts.

Include:

- Debit cards associated with business/government transaction deposit accounts reported in the Institution Profile section
- Business/government debit cards (not including prepaid cards) that can be used to make purchases at the point of sale

Do not include:

- ATM-only cards that cannot be used to make purchases at the point of sale
- Consumer debit cards that can be used to make purchases at the point of sale
- Both consumer and business/government prepaid cards that can be used to make purchases at the point of sale
- Both consumer and business/government credit cards that can be used to make purchases at the point of sale

► **Example:** Your institution has 1,000 business banking accounts, with 1,000 debit cards issued that are related to these accounts. Of these debit cards, 900 cards have been activated and are not expired, 70 cards have not been activated yet, and 30 cards have been activated but are now expired. Of the 900 cards that are active and not expired, 800 cards have been used to make at least one purchase in 2018. In this example, you would report 900 business debit cards in force and 800 debit cards with purchase activity.

3) Total non-prepaid debit card transactions = 3.a) + 3.b)

These include all transactions over any debit card network for which your institution was the issuer. Include all point-of-sale or bill-pay transactions made by debit cards processed over either signature payment card networks or PIN payment card networks. If your answer is **No** to item **1**) above, please report "0" here.

Include:

- Both consumer and business/government debit card transactions
- Both in-person and remote debit card transactions
- Debit card cash back at the point of sale

Do not include:

- Cash withdrawals over the counter
- ATM withdrawals
- Prepaid card transactions
- Credit card transactions

► **Example:** Your customer bought $50 of groceries with her debit card by entering her PIN at the checkout line. Later that day, she used the same debit card issued by your institution to purchase a $70 purse online. In this example, you would report two transactions for $120.

3.a) From consumer accounts

These include all transactions made by consumer accountholders over any debit card network for which your institution was the issuer.

Include:

- Consumer in-person and remote debit card transactions
- Debit card cash back at the point of sale by consumer accountholders

Do not include:

- Debit card transactions made by business/government accountholders
- Prepaid card transactions made by business/government or consumer accountholders
- Credit card transactions made by business/government or consumer accountholders
- ATM withdrawals

► **Example:** Tom used his debit card issued by your institution to buy a $40 pair of jeans. Later that day, he used his debit card at the ATM to withdraw $500. In this example, you would report one transaction for $40.

3.b) From business/government accounts

These include all transactions made by business/government accountholders over any debit card network for which your institution was the issuer.

Include:

- Business/government in-person and remote debit card transactions
- Debit card cash back at the point of sale by business/government accountholders

Do not include:

- Debit card transactions made by consumer accountholders
- Prepaid card transactions made by consumer or business/government accountholders
- Credit card transactions made by consumer or business/government accountholders
- ATM withdrawals

► **Example:** Your corporate accountholder made a purchase of $500 with a corporate debit card issued by your institution. Later that day, he withdrew $200 in cash over the counter at one of your branch locations using the same debit card. In this example, you would report one transaction for $500.

4) Total non-prepaid debit card transactions (repeat item 3) = 4.a) + 4.b)

Repeat item **3)** from above. These include all transactions over any debit card network for which your institution was the issuer. Include all point-of-sale or bill-pay transactions made by debit cards processed over either signature payment card networks or PIN payment card networks. If your answer is **No** to item **1**) above, please report "0" here.

Include:

- Both consumer and business/government debit card transactions
- Both in-person and remote debit card transactions
- Debit card cash back at the point of sale

Do not include:

- Cash withdrawals over the counter
- ATM withdrawals
- Prepaid card transactions
- Credit card transactions

► **Example:** Your customer bought $50 of groceries with her debit card by entering her PIN at the checkout line. Later that day, she used the same debit card issued by your institution to purchase a $70 purse online. In this example, you would report two transactions for $120.

4.a) In-person transactions = 4.a.1) + 4.a.2)

These include all non-prepaid debit card transactions for which the card user is physically present with the card at the point of sale. Include digital wallet (Apple Pay, Samsung Pay, etc.) transactions at the point of sale only. Please report the total transactions using a PIN (item **4.a.1)**, and without a PIN (item **4.a.2)**.

Include:

- Transactions for which the card user is present
- Mobile transactions at the point of sale (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)
- Contactless card transactions at the point of sale (i.e., "tap and pay" physical cards, fobs, or stickers)
- Intermediated transactions at the point of sale (i.e., Square, Clover, iZettle)
- Card-not-present transactions for which the card user is present at the point of sale (i.e., key-entered transactions)

Do not include:

- Remote transactions
- Digital wallet in-app or browser transactions

► **Example 1:** Your customer bought a coat for $100 with his debit card by entering his PIN at the checkout line. Later that day, he bought a $40 train ticket with his debit card by signing the receipt at the checkout. For this example, you would report two transactions for $140 in item **4.a)**, one transaction for $100 for **4.a.1)**, and one transaction for $40 for **4.a.2)**.

4.a.1) With a PIN

These are debit card transactions that are authenticated when the user enters their PIN at the point of sale.

Include:

- In-person debit card transactions authenticated via PIN

Do not include:

- In-person debit card transactions that were processed over a signature
- In-person low-value debit card transactions for which no signature or PIN was required
- Remote debit card transactions

► **Example:** Your customer bought lunch for $15 with his debit card by entering his PIN at the checkout line. Later that day, he bought a $30 sweater with his debit card by signing the receipt at the checkout. In this example, you would report one transaction for $15.

4.a.2) Without a PIN

These are debit card transactions that are not authenticated using a PIN at the point of sale (single-message over the payment card network). These transactions use dual-message authentication over the payment card network.

Include:

- In-person debit card transactions that were processed over a signature
- In-person low-value debit card transactions for which no signature or PIN was required

Do not include:

- In-person debit card transactions authenticated via PIN
- Remote debit card transactions

► **Example:** Your customer bought lunch for $15 with his debit card by entering his PIN at the checkout line. Later that day, he bought a $30 sweater with his debit card by signing the receipt at the checkout. For this example, you would report one transaction for $30.

4.b) Remote transactions = 4.b.1) + 4.b.2)

These include all non-prepaid debit card transactions for which the card user does not physically present the card to authorize the transaction, including mail-order transactions, telephone-order transactions, and internet transactions. Please report the total transactions from domestic (U.S.) payees (item **4.b.1)** and foreign payees (item **4.b.2)**.

Include:

- Remote debit card transactions (e.g., mail-order transactions, telephone-order transactions)
- Digital wallet in-app or browser debit card transactions (e.g., e-commerce transactions)

Do not include:

- Transactions for which the card user is present
- Mobile transactions at the point of sale (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)
- Contactless card transactions at the point of sale (i.e., “tap and pay” physical cards, fobs, or stickers)
- Intermediated transactions at the point of sale (i.e., Square, Clover, iZettle)
- Card-not-present transactions for which the card user is present at the point of sale (i.e., key-entered transactions)

► **Example:** Your customer purchased a $500 item on a German internet website with his debit card by entering his debit card number, name, and address. He then proceeded to buy a $65 pair of shoes from a U.S.-based store in a mobile application not at the point of sale, paying with the same debit card with his digital wallet (Google Pay). In this example, you would report two transactions for $565 in item **4.b)**, one transaction for $65 in item **4.b.1),** and one transaction for $500 in item **4.b.2**).

4.b.1) Domestic (U.S.) payee

These are remote debit card transactions in which a U.S. person or company (i.e., located in the 50 U.S. states, D.C., or U.S. territories) is the recipient of the payment.

Include:

- Domestic payee remote debit card transactions (e.g., mail-order transactions, telephone-order transactions)
- Domestic payee digital wallet in-app or browser debit card transactions (e.g., e-commerce transactions)

Do not include:

- Foreign payee remote debit card transactions
- Transactions for which the card user is present

► **Example:** Your customer purchased a $100 item on a Chinese internet website from a Chinese (foreign) merchant with his debit card by entering his debit card number, name, and address. He then proceeded to buy $70 of groceries from a New York grocery store (U.S.-based merchant) in a mobile application not at the point of sale (in-app transaction), paying with the same debit card with his digital wallet (Google Pay). In this example, you would report one transaction for $70 under **4.b.1)**. [Note that the foreign payee transaction for $100 would be reported under **4.b.2)**].

4.b.2) Foreign payee

These are remote debit card transactions in which a non-U.S. person or company is the recipient of the payment.

Include:

- Foreign payee remote debit card transactions (e.g., mail-order transactions, telephone-order transactions)
- Foreign payee digital wallet in-app or browser debit card transactions (e.g., e-commerce transactions)

Do not include:

- Domestic payee remote debit card transactions
- Transactions for which the card user is present

► **Example:** Your customer purchased a $100 item on a Chinese internet website from a Chinese (foreign) merchant with his debit card by entering his debit card number, name, and address. He then proceeded to buy $70 of groceries from a New York grocery store (U.S.-based merchant) in a mobile application not at the point of sale (in-app transaction), paying with the same debit card with his digital wallet (Google Pay). In this example, you would report one transaction for $100 under **4.b.2)**. [Note that the domestic payee transaction for $70 would be reported under **4.b.1)**].

5) Third-party fraudulent non-prepaid debit card transactions = 5.a) + 5.b)

These include all third-party unauthorized debit card transactions, before any recoveries or chargebacks, for which your institution was the card issuer. Please report any fraudulent third-party debit card transactions, regardless of whether the transaction resulted in a loss of funds. If your answer is **No** to item **1**) above, please report "0" here.

Include:

- Debit 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 credit card transactions
- Fraudulent prepaid card transactions
- Fraudulent ATM withdrawals
- Debit card transactions authorized by a valid card user as part of a scam

► **Example 1:** Your accountholder's debit card issued by your institution was stolen. The perpetrator used the card to make one purchase worth $1,000, which was authorized at the point of sale. In this example, you would report one transaction for $1,000.

► **Example 2:** Your accountholder claimed that her debit card was stolen and used to purchase a $500 TV in an electronics store. An investigation by your institution determined that in fact your accountholder made this purchase on her card. Since this transaction is an example of first-party fraud (false claim of fraud), it should not be included in item **5**).

5.a) In-person transactions = 5.a.1) + 5.a.2)

These include only third-party fraudulent non-prepaid debit card transactions for which the card user is physically present with the card at the point of sale. Include digital wallet (Apple Pay, Samsung Pay, etc.) transactions at the point of sale only. Please report the total transactions using a PIN (item **5.a.1**) and without a PIN (item **5.a.2**).

Include:

- Fraudulent transactions for which the debit card perpetrator is present
- Fraudulent contactless debit card transactions (i.e., "tap and pay" with a debit card)
- Fraudulent mobile transactions at the point of sale (i.e., 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 (i.e., Square, Clover, iZettle)
- Fraudulent card-not-present transactions for which the card user is present at the point of sale (i.e., key-entered transactions)

Do not include:

- Fraudulent remote debit card transactions (e.g., mail-order transactions, telephone-order transactions)
- Fraudulent digital wallet in-app or browser debit card transactions (e.g., e-commerce transactions)

► **Example 1:** Your accountholder's debit card was stolen. The perpetrator used the card to make two purchases totaling $1,000 online. He then bought lunch for $35 at a restaurant using the stolen card. In this example, you would report one transaction for $35.

► **Example 2:** Your accountholder claimed that her debit card was stolen and used to purchase a $500 TV in an electronics store. An investigation by your institution determined that in fact your accountholder made this purchase on her card. Since this transaction is an example of first-party fraud (false claim of fraud), it should not be included in item **5.a**).

5.a.1) With a PIN

These include only third-party fraudulent non-prepaid debit card transactions that are authenticated when the user enters their PIN at the point of sale.

Include:

- Fraudulent in-person debit card transactions authenticated via PIN

Do not include:

- Fraudulent in-person debit card transactions that were processed over a signature
- Fraudulent in-person low-value debit card transactions for which no signature or PIN was required
- Fraudulent remote debit card transactions

► **Example:** Your accountholder's debit card was stolen, and the perpetrator watched her enter her PIN at the point of sale before stealing the card. The perpetrator then used her card and PIN to buy a $200 watch at a jewelry store. He then used the card to buy dinner for $50 at a nearby restaurant by fraudulently signing the receipt. In this example, you would report one transaction of $200.

5.a.2) Without a PIN

These are fraudulent debit card transactions that are not authenticated when the user enters their PIN at checkout. These transactions use dual-message authentication over the payment card network.

Include:

- Fraudulent in-person debit card transactions that were processed over a signature
- Fraudulent in-person low-value debit card transactions for which no signature or PIN was required

Do not include:

- Fraudulent in-person debit card transactions authenticated via PIN
- Fraudulent remote debit card transactions

► **Example:** Your accountholder's debit card was stolen, and the perpetrator watched her enter her PIN at the point of sale before stealing the card. The perpetrator then used her card and PIN to buy a $200 watch at a jewelry store. He then used the card to buy dinner for $50 at a nearby restaurant by fraudulently signing the receipt. In this example, you would report one transaction of $50.

5.b) Remote transactions = 5.b.1) + 5.b.2)

These include only third-party fraudulent non-prepaid debit card transactions for which the card user does not physically present the card to authorize the transaction. Please report any fraudulent third-party debit card transactions, regardless of whether the transaction resulted in a loss of funds. Please report the total transactions from domestic (U.S.) payees (item **5.b.1)** and foreign payees (item **5.b.2)**.

Include:

- Fraudulent remote debit card transactions (e.g., mail-order transactions, telephone-order transactions)
- Fraudulent digital wallet in-app or browser debit card transactions (e.g., e-commerce transactions)

Do not include:

- Fraudulent transactions for which the debit card perpetrator is present
- Fraudulent mobile transactions at the point of sale (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)
- Fraudulent contactless card transactions at the point of sale (i.e., "tap and pay" physical cards, fobs, or stickers)
- Fraudulent intermediated transactions at the point of sale (i.e., Square, Clover, iZettle)
- Fraudulent card-not-present transactions for which the card user is present at the point of sale (i.e., key-entered transactions)

► **Example 1:** Your accountholder's debit card was stolen. The perpetrator used the card to purchase 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. Both transactions were authorized. In this example, you would report one transaction for $250.

► **Example 2:** Your accountholder claimed that his debit card was stolen and used to purchase a $20 video game online. An investigation by your institution determined that in fact your accountholder made this purchase on his card. Since this transaction is an example of first-party fraud (false claim of fraud), it should not be included in item **5.b**).

5.b.1) Domestic (U.S.) payee

These include only third-party fraudulent non-prepaid debit card transactions for which the card user does not physically present the card to authorize the transaction and a U.S. person or company (i.e., located in the 50 U.S. states, D.C., or U.S. territories) is the recipient of the payment.

Include:

- Fraudulent domestic payee remote debit card transactions (e.g., mail-order transactions, telephone-order transactions)
- Fraudulent domestic payee digital wallet in-app or browser debit card transactions (e.g., e-commerce transactions)

Do not include:

- Fraudulent foreign payee remote debit card transactions
- Fraudulent transactions for which the card perpetrator is present

► **Example:** Your accountholder's debit card was stolen. The perpetrator used the card to buy a $250 coat online from a French retailer. He then used the card online to buy a $15 book from a U.S. bookstore. In this example, you would report one transaction for $15.

5.b.2) Foreign payee

These include only third-party fraudulent non-prepaid debit card transactions for which the card user does not physically present the card to authorize the transaction and a non-U.S. person or company is the recipient of the payment.

Include:

- Fraudulent foreign payee remote debit card transactions (e.g., mail-order transactions, telephone-order transactions)
- Fraudulent foreign payee digital wallet in-app or browser debit card transactions (e.g., e-commerce transactions)

Do not include:

- Fraudulent domestic payee remote debit card transactions
- Fraudulent transactions for which the card user is present

► **Example:** Your accountholder's debit card was stolen. The perpetrator used the card to buy a $250 coat online from a French retailer. He then used the card online to buy a $15 book from a U.S. bookstore. In this example, you would report one transaction for $250.

6) Total non-prepaid debit digital wallet transactions = 6.a) + 6.b)

These are all non-prepaid debit card transactions made via a digital wallet, including tokenized digital wallet. If your answer is **No** to item **1**) above, please report "0" here.

Include:

- Digital wallet debit card transactions made by using electronic devices, such as a smartphone, smart watch, or activity tracker, by "tapping" the device at the POS terminal (i.e., Apple Pay, Samsung Pay, Google Pay, Fitbit Pay, Masterpass)
- Tokenized digital wallet debit card transactions made by using customer's payment credentials saved in a virtual account number. These credentials can be stored either on a smartphone or in the cloud. When making a purchase, a substitute account number and a transaction specific code ("token") are used to process payments. This can include purchasing items online with a computer or using a smartphone to make a purchase with a browser or in-app (i.e., Apple Pay, Google Pay, Masterpass, Visa Checkout, Amex Express Checkout)
- Digital wallet debit card NFC (near field communication) transactions, MST (magnetic secure transmission) transactions, QR code transactions, barcode transactions, in-app transactions, or browser transactions

Do not include:

- Debit card-on-file e-commerce transactions (cardholder-initiated or merchant-initiated) (i.e., installment payment)

► **Example:** Your customer bought lunch for $10 with his debit card, which was loaded into his digital wallet (Apple Pay). He physically tapped his phone on the POS device to pay for lunch, using NFC technology. He then ordered a $30 dinner in a mobile application, paying with the same debit card via his digital wallet (Apple Pay). In this example, you would report two transactions for $40.

6.a) In-person transactions

These include debit card transactions for which an electronic device, such as a smartphone, smart watch, or activity tracker, was "tapped" to pay at the POS terminal (i.e., Apple Pay, Samsung Pay, Google Pay, Fitbit Pay)

Include:

- Mobile transactions at the point of sale (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)

Do not include:

- In-app transactions or browser transactions made with a digital wallet (e.g., Apple Pay, Google Pay, Samsung Pay)
- Tokenized digital wallet transactions made by using customer's payment credentials saved in a virtual account (e.g., Apple Pay, Google Pay, Masterpass, Visa Checkout, Amex Express Checkout)
- Card-on-file e-commerce transactions (cardholder-initiated or merchant-initiated) (e.g., installment payment)

► **Example:** Your customer bought lunch for $15 with his debit card, which was loaded into his digital wallet (Apple Pay). He physically tapped his phone on the POS device to pay for lunch, using NFC technology. He then bought groceries for $100 with his debit card by swiping the card in a magnetic reader. In this example, you would report one transaction for $15.

6.b) Remote transactions

These include debit card in-app transactions or browser transactions made with a digital wallet. Browser transactions include both digital wallets (i.e., Apple Pay, Google Pay, Samsung Pay) and third-party tokenized digital wallets (i.e., PayPal, Amazon Pay, Square Restaurants, Visa Checkout, Masterpass)

Include:

- In-app transactions or browser transactions made with a digital wallet (e.g., Apple Pay, Google Pay, Samsung Pay)
- Tokenized digital wallet transactions made by using customer's payment credentials saved in a virtual account (e.g., Apple Pay, Google Pay, Masterpass, Visa Checkout, Amex Express Checkout)

Do not include:

- Mobile transactions at the point of sale (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)
- Card-on-file e-commerce transactions (cardholder-initiated or merchant-initiated) (e.g., installment payment)

► **Example:** Your customer purchased a $500 item on an internet website with his debit card by entering his debit card number, name, and address. He then bought a $65 pair of shoes in a mobile application, paying with the same debit card via his digital wallet (Google Pay). In this example, you would report one transaction for $65.

7) Total non-prepaid debit card cash-back transactions at point of sale

These include all debit card transactions for which your institution was the card issuer and in which the accountholders received cash back at the point of sale. For cash-back value, only include the amount of cash your card users received at the point of sale. If your answer is **No** to item **1**) above, please report "0" here.

Include:

- Debit card cash-back transactions at the point of sale (i.e., amount of cash received at the point of sale)

Do not include:

- ATM withdrawals
- The amount paid for goods and services

► **Example:** Your customer used her debit card at the grocery store to purchase $50 of food. She entered her PIN to authorize the transaction and also requested $20 cash back. In this example, you would report one transaction for $20.

General-Purpose Prepaid Cards

GENERAL TERMINOLOGY

Prepaid card transactions

All purchase and bill-pay transactions made with open-loop prepaid cards used for point-of-sale (POS) transactions. These transactions can be authenticated by either a Personal Identification Number (PIN), signature, EMV, online authorization, or any other digital method (NFC, QR code, etc.). Transactions may originate, for example, at a physical point of sale, via telephone, or via the Internet. For this study, please follow these guidelines:

Prepaid card transactions include…	Prepaid card transactions do <u>not</u> include…
▪ Transactions made with Visa, MasterCard, Discover, or American Express branded prepaid cards and cleared over dual-message networks ▪ POS transactions made with prepaid cards and cleared over a general-purpose, single-message network (these are typically called PIN-based or online prepaid card transactions) ▪ Open-loop general-purpose prepaid card transactions ▪ Open-loop gift card transactions ▪ Payroll card transactions by the cardholder ▪ FSA/HAS prepaid cards ▪ Customer refund and incentive prepaid cards	▪ Closed-loop general-purpose prepaid card transactions ▪ ATM withdrawals ▪ Debit card transactions ▪ Credit card transactions ▪ Transfers by a corporate customer to fund its employees' payroll card accounts ▪ Electronic benefits transfer (EBT) card transactions

Digital Wallet

All purchase and bill-pay transactions made using a digital wallet in which users can complete purchases using near-field communication (NFC) that works in conjunction with mobile payment systems, MST (magnetic secure transmission) transactions, QR code transactions, barcode transactions, in-app transactions, or browser transactions. Digital wallets can be used during In-person transactions or Remote transactions. In-person transactions require the payment holder to be present to use their digital wallet, while remote transactions are used during e-commerce sales in which the authorization and transaction processes are not physically close to each other.

Digital wallet transactions include those made by using electronic devices, such as a smartphone, smart watch, or activity tracker, by "tapping" the device at the POS terminal (i.e., Apple Pay, Samsung Pay, Google Pay, Fitbit Pay, Masterpass).

They also include tokenized digital wallet transactions made by using customer's payment credentials saved in a virtual account number. These credentials can be stored either on a smartphone or in the cloud. When making a purchase, a substitute account number and a transaction specific code ("token") are used to process payments. This can include purchasing items online with a computer or using a smartphone to make a purchase with a browser or in-app (i.e., Apple Pay, Google Pay, Masterpass, Visa Checkout, Amex Express Checkout).

General-purpose prepaid cards

These network-branded cards are typically, but not necessarily, consumer-funded and can be used at the point of sale, for bill-pay transactions, or to withdraw cash from an ATM. These cards are often marketed to underbanked consumers as a checking account alternative.

Consumer account

A prepaid account for personal use by an individual or household from which payments can be made or to withdraw cash from an ATM.

Business/government account

A prepaid account owned by an organization (i.e., business, government or not-for-profit organization) from which payments can be made or to withdraw cash from an ATM.

Note: Please report small business accounts under business/government accounts, if possible.

U.S. domiciled account

Accounts located within the 50 U.S. states, D.C., or U.S. territories such as Guam, Puerto Rico, or U.S. Virgin Islands). Only report data associated with your institution's U.S. domiciled accounts, including transactions that are domestic and cross-border.

Open-loop prepaid cards

Network branded general-purpose prepaid cards (i.e., Visa, MasterCard, American Express, Discover) which can be used at any point of sale or for bill-pay transactions were the network is accepted. Unlike a debit card, a prepaid card is not linked to a bank account.

Note: If your institution reports on behalf of an EFT network, please include only prepaid card transactions that carry your network brand. Do not include reciprocal or gateway transactions that are not routed on your brand.

Any fees charged to the cards (i.e., monthly transaction fees) are not considered to be transactions and should be excluded.

Closed-loop prepaid cards

Prepaid cards which can only be used at certain merchant(s); these are non-network prepaid cards. Closed-loop prepaid cards are also referred as “store cards” (e.g., Old Navy gift card, Home Depot gift card) and operate between the merchant and the issuer without the use of a network.

Note: This questionnaire does not consider closed-loop prepaid cards as prepaid cards. Do not include transactions associated with these cards in this survey.

Reloadable prepaid cards

Open-loop or closed-loop prepaid card to which funds can be added at a later time after the initial purchase of the card.

Note: Any fees charged to the cards (i.e., monthly fees, dormancy fees) are not considered to be transactions and should be excluded.

Gift cards

Prepaid cards, often merchant or shopping center branded, that are marketed as gift-giving alternatives to cash, checks, and gift certificates or as loyalty cards with payment capabilities. Some network branded cards (e.g., Visa), refer to open-loop general-purpose prepaid cards as gift cards as well.

Payroll cards

Reloadable, prepaid “ATM” cards issued to disburse employee wages; typically marketed as a means to replace paper check or cash wages to unbanked employees.

Flexible Spending Account (FSA) and Health Savings Account (HSA) medical cards

Reloadable medical cards used for health care costs referred to as “qualified expenses,” including deductibles, copayments and coinsurance, and monthly prescription transactions. HSA contributions are tax-deductible but can also be taken out of pretax pay. FSA contributions are pretax, and distributions are untaxed. Both medical cards are typically used to save money on medical expenses.

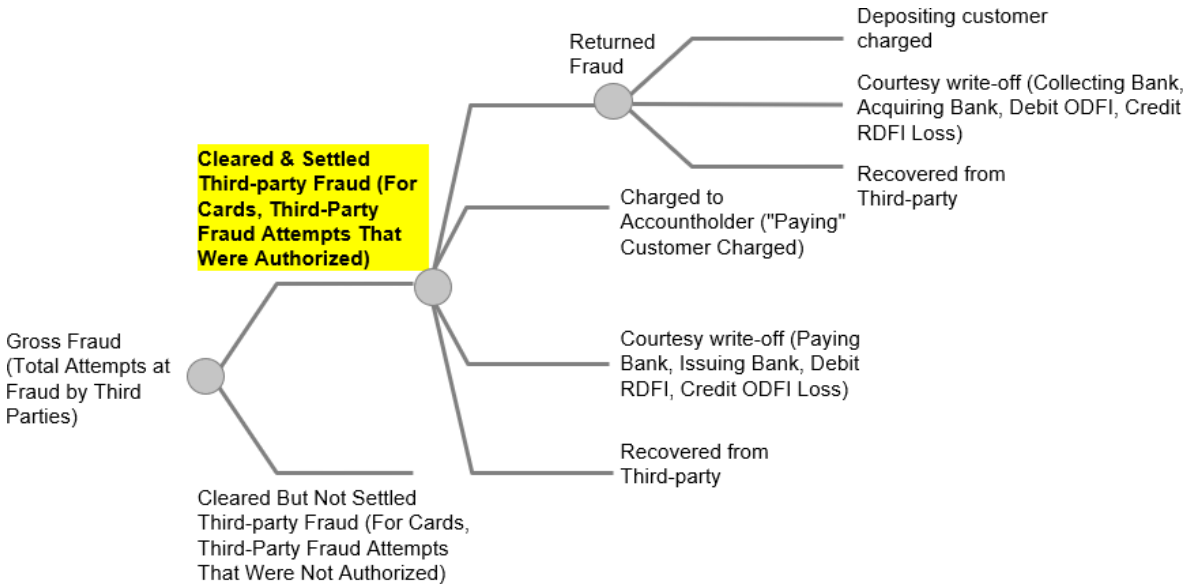
Electronic benefits transfer (EBT)

Electronic benefits transfer (EBT) is an electronic system that allows recipients to authorize transfers of their government benefits from a Federal account to a retailer account to pay for products received via a payment card.

Note: This questionnaire does not consider EBT cards as prepaid cards. Do not include transactions associated with these cards in this survey.

Third-party fraud

The Federal Reserve Payments Study has identified a measure of fraud that can be described as cleared and settled third-party fraudulent transactions. This measure is not a loss-of-funds measure, nor is it a measure of fraud attempts; rather, it is a measure of the extent to which third parties who are not authorized to conduct transactions are able to penetrate the payment system and effect settlement between banks, or create a book transfer of funds if the transaction happens within one 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 manages to create a 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.



SURVEY ITEMS

1) Did your institution offer its customers general-purpose prepaid cards issued by another financial institution during calendar year 2018?

General-purpose prepaid cards include but are not limited to: payroll prepaid cards, open-loop gift cards, government-administered open-loop prepaid cards, FSA/HSA medical cards, and open-loop customer refund and incentive cards. If your answer to this question is **Yes**, please do not include these cards (or associated transactions) in your answers below.

2) Did your institution have general-purpose prepaid cards in circulation in 2018 for which your institution was the issuer?

Cards issued for prepaid card programs managed by your institution or managed by a third-party for which your institution was the issuer and that route transactions over a debit card network. If your answer to this question is **No**, please report "0" for the remainder of the General-Purpose Prepaid Cards section and skip question **2.a)**.

Include:

- Consumer and business/government general-purpose open-loop reloadable prepaid cards
- Consumer and business/government general-purpose open-loop non-reloadable prepaid cards
- Open-loop gift cards
- Payroll prepaid cards
- FSA/HSA medical cards
- Government-administered general-purpose open-loop prepaid cards
- Open-loop customer refund and incentive cards

Do not include:

- Closed-loop prepaid cards (i.e., prepaid cards that do not route transactions over a debit card network)
- Non-prepaid debit cards
- ATM or ATM-only cards
- Electronic benefits transfer (EBT) cards
- Credit cards

2.a) If your answer is "Yes" to item 2) above, are you able to include business/government prepaid card volumes in your answers below?

If your answer is "**Yes, in some cases**," please explain in the comments box at the end of the General-Purpose Prepaid Cards section.

3) Total general-purpose prepaid card program accounts = 3.a) + 3.b)

These are accounts for both reloadable and non-reloadable open-loop prepaid cards for which your institution was the issuer. Your customer may or may not be able to add additional funds to this card after it has been issued and use these funds to shop, transfer money, or pay bills. If your answer is **No** to item **2)** above, please report "0" here.

Average of monthly totals means the average of end-of-month totals for each of the months in 2018.

Include:

- General-purpose prepaid card programs managed by both your institution and a third-party
- Consumer and business/government general-purpose open-loop reloadable prepaid card accounts
- Consumer and business/government general-purpose open-loop non-reloadable prepaid card accounts
- Open-loop gift card accounts
- Payroll prepaid card accounts
- FSA/HSA medical card accounts
- Government-administered general-purpose open-loop prepaid card accounts
- Customer refund and incentive card accounts

Do not include:

- Closed-loop prepaid cards (i.e., prepaid cards that don't route transactions over a debit card network)
- Non-prepaid debit card accounts
- ATM or ATM-only card accounts
- Electronic benefits transfer (EBT) card accounts
- Credit card accounts

► **Example:** John has an open-loop prepaid card issued by your institution that he reloads every month for his grocery shopping. His prepaid card account contains an additional prepaid card used by his spouse. In this example, you would report one general-purpose prepaid card account with its respective average end-of-month balance.

3.a) Reloadable accounts

These are accounts for reloadable open-loop prepaid cards which may be loaded with money multiple times.

► **Example:** Mary, owner or Mary's Boutique, has a business prepaid card account with your institution. She issued five business prepaid cards from her account to each one of her employees. Mary reloads her account each month to cover her employees' expenses. Mary also owns a Visa gift card, issued by your institution, that she received as a gift and can be reloaded with more funds at any time. In this example, you would report two reloadable prepaid card accounts with their respective average end-of-month balances.

3.b) Non-reloadable accounts

These are account for non-reloadable open-loop prepaid cards, which may be used multiple times but funds cannot be replenished.

► **Example:** Jane owns a Visa gift card issued by your institution that she received as a gift and can only use for the $100 loaded onto the card. In this example, you would report only one card account with its respective average end-of-month balance.

4) Number of general-purpose prepaid cards = 4.a) + 4.b)

These are all general-purpose open-loop prepaid cards that can be used at the point of sale that were issued by your institution, drawn on prepaid card program accounts listed in item **3)** above, and in force at the end of the month. Please report average monthly totals for both reloadable and non-reloadable prepaid cards for which your institution was the issuer. If your answer is **No** to item **2)** above, please report "0" here.

For cards in force, report only general-purpose open-loop prepaid cards that had been issued by your institution, activated by your institution's accountholders, and had not expired at the end of a month.

For cards in force with purchase activity, report only general-purpose open-loop prepaid cards that had at least one point-of-sale (POS) and/or bill pay activity during the time period.

If your answer is **No** to item **2)** above, please report "0" here.

Average of monthly totals means the average of end-of-month totals for each of the months in 2018.

Include:

- Consumer and business/government general-purpose open-loop reloadable prepaid cards
- Consumer and business/government general-purpose open-loop non-reloadable prepaid cards
- Payroll prepaid cards
- Government-administered general-purpose open-loop prepaid cards
- Open-loop gift cards
- FSA/HSA medical cards
- Customer refund and incentive cards

Do not include:

- Closed-loop prepaid cards (i.e., prepaid cards that don't route transactions over a debit card network)
- Non-prepaid debit cards
- ATM or ATM-only cards
- Electronic benefits transfer (EBT) cards
- Credit cards

► **Example:** Your institution has 500 consumer and business general-purpose open-loop prepaid accounts, with 600 prepaid cards issued that are related to these accounts. Of these prepaid cards, 450 cards have been activated and are not expired, 130 cards have not been activated yet, and 20 cards have been activated but are now expired. Of the 450 cards that are active and not expired, 350 cards have been used to make at least one purchase in 2018. In this example, you would report 450 prepaid cards in force and 350 prepaid cards with purchase activity.

4.a) Reloadable cards

These are all reloadable general-purpose open-loop prepaid cards that can be used at the point of sale that were issued by your institution, drawn on prepaid card program accounts listed in item **3)** above, and in force at the end of the month. Please report average monthly totals for reloadable prepaid cards only for which your institution was the issuer.

Include:

- Consumer and business/government general-purpose open-loop reloadable prepaid cards

Do not include:

- Consumer and business/government general-purpose open-loop non-reloadable prepaid cards
- Closed-loop prepaid cards (i.e., prepaid cards that don't route transactions over a debit card network)
- Electronic benefits transfer (EBT) cards

► **Example:** Jill, your customer, has three prepaid cards linked to one business prepaid card account that she reloads every month for her small business. All three cards were activated, but only two cards were used in 2018 to make purchases. In this example, you would report three prepaid cards in force and two prepaid cards with purchase activity.

4.b) Non-reloadable cards

These are all non-reloadable general-purpose open-loop prepaid cards that can be used at the point of sale that were issued by your institution, drawn on prepaid card program accounts listed in item **3)** above, and in force at the end of the month. Please report average monthly totals for non-reloadable prepaid cards only for which your institution was the issuer.

Include:

- Consumer and business/government general-purpose open-loop non-reloadable prepaid cards

Do not include:

- Consumer and business/government general-purpose open-loop reloadable prepaid cards
- Closed-loop prepaid cards (i.e., prepaid cards that don't route transactions over a debit card network)
- Electronic benefits transfer (EBT) cards

► **Example:** Joe owns a MasterCard gift card issued by your institution that he received as a gift and can only use for the $100 loaded onto the card. Joe activated the card and used the $100 balance to purchase a video game console. In this example, you would report one prepaid card in force and one prepaid card with purchase activity.

5) Total general-purpose prepaid card transactions = 5.a) + 5.b)

These include all transactions over any prepaid card network for which your institution was the issuer. Include all point-of-sale or bill-pay transactions made by prepaid cards processed over either signature payment card networks or PIN payment card networks. If your answer is **No** to item **2)** above, please report "0" here.

Include:

- Both consumer and business/government general-purpose open-loop prepaid card transactions
- Payroll prepaid card transactions
- Government-administered general-purpose open-loop prepaid card transactions
- Open-loop gift card transactions
- FSA/HSA medical card transactions
- Customer refund and incentive card transactions
- Cash-back transactions at the point of sale (i.e., amount of cash received at the point of sale)

Do not include:

- Closed-loop prepaid card transactions (i.e., prepaid cards that don't route transactions over a debit card network)
- ATM withdrawals
- Debit card transactions
- Credit card transactions

► **Example:** Jenny bought $50 of groceries with her prepaid card, issued by your institution, by entering her PIN at the checkout line. Later that day, she used a debit card issued by your institution to purchase a $70 jacket at a department store. In this example, you would report only one transaction for $50.

5.a) From reloadable accounts

These include all transactions over any prepaid card network for which your institution was the issuer. Include all point-of-sale or bill-pay transactions made by open-loop reloadable prepaid cards processed over either signature payment card networks or PIN payment card networks.

Include:

- Consumer and business/government general-purpose open-loop reloadable prepaid card transactions

Do not include:

- Consumer and business/government general-purpose open-loop non-reloadable prepaid card transactions
- Closed-loop prepaid card (i.e., prepaid cards that don't route transactions over a debit card network) transactions
- Electronic benefits transfer (EBT) card transactions

► **Example:** Before going to the mall, Joe reloaded his prepaid card issued by your institution with $500. At the mall, Joe used his prepaid card to buy a $100 jacket. Later in the week, he used his prepaid card at the ATM to withdraw $200. In this example, you would report one transaction for $100.

5.b) From non-reloadable accounts

These include all transactions over any prepaid card network for which your institution was the issuer. Include all point-of-sale or bill-pay transactions made by open-loop non-reloadable prepaid cards processed over either signature payment card networks or PIN payment card networks.

Include:

- Consumer and business/government general-purpose open-loop non-reloadable prepaid card transactions

Do not include:

- Consumer and business/government general-purpose open-loop reloadable prepaid card transactions
- Closed-loop prepaid card (i.e., prepaid cards that don't route transactions over a debit card network) transactions
- Electronic benefits transfer (EBT) card transactions

► **Example:** Bill went to the grocery store and bought $90 of groceries using his prepaid card issued by your institution. On the way home, he realized he still had $10 left on the same non-reloadable prepaid card, so he bought a $10 DVD. In this example, you would report two transactions for $100.

6) Total general-purpose prepaid card transactions (repeat item 5) = 6.a) + 6.b)

Repeat item **5**) from above. These include all transactions over any prepaid card network for which your institution was the issuer. Include all point-of-sale or bill-pay transactions made by prepaid cards processed over either signature payment card networks or PIN payment card networks. If your answer is **No** to item **2)** above, please report "0" here.

Include:

- Both consumer and business/government general-purpose open-loop prepaid card transactions
- Payroll prepaid card transactions
- Government-administered general-purpose open-loop prepaid card transactions
- Open-loop gift card transactions
- FSA/HSA medical card transactions
- Customer refund and incentive card transactions
- Cash-back transactions at the point of sale (i.e., amount of cash received at the point of sale)

Do not include:

- Closed-loop prepaid card transactions (i.e., prepaid cards that don't route transactions over a debit card network)
- ATM withdrawals
- Debit card transactions
- Credit card transactions

► **Example:** Your customer bought $50 of groceries with her prepaid card by entering her PIN at the checkout line. Later that day, she used the same prepaid card issued by your institution to purchase a $70 jacket at a department store. In this example, you would report two transactions for $120.

6.a) In-person transactions = 6.a.1) + 6.a.2)

These include all general-purpose prepaid card transactions for which the card user is physically present with the card at the point of sale. Include digital wallet (Apple Pay, Android Pay, Samsung Pay, etc.) transactions at the point of sale only. Please report the total transactions using PIN authentication (item **6.a.1**) and without PIN (item **6.a.2**).

Include:

- Transactions for which the card user is present
- Mobile transactions at the point of sale (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)
- Contactless card transactions at the point of sale (i.e., "tap and pay" physical cards, fobs, or stickers)
- Intermediated transactions at the point of sale (i.e., Square, Clover, iZettle)
- Card-not-present transactions for which the card user is present at the point of sale (i.e., key-entered transactions)

Do not include:

- Remote transactions
- Digital wallet in-app or browser transactions

► **Example:** Your customer bought a coat for $100 with his prepaid card by entering his PIN at the checkout line. Later that day, he bought a $40 train ticket with his prepaid card by signing the receipt at the checkout. For this example, you would report two transactions for $140 in item **6.a)**, one transaction for $100 for **6.a.1)**, and one transaction for $40 for **6.a.2)**.

6.a.1) With a PIN

These are prepaid card transactions that are authenticated when the user enters their PIN at the point of sale.

Include:

- In-person prepaid card transactions authenticated via PIN

Do not include:

- In-person prepaid card transactions that were processed over a signature
- In-person low-value prepaid card transactions for which no signature or PIN was required
- Remote prepaid card transactions

► **Example:** Your customer bought groceries for $20 with his prepaid card, which he authenticated by entering his PIN at the checkout. He also used his prepaid card to buy dinner for $50 that night, which he authenticated by signing the receipt. In this example, you would report one transaction for $20.

6.a.2) Without a PIN

These are prepaid card transactions that are not authenticated using a PIN at the point of sale (single-message over the payment card network). These transactions use dual-message authentication over the payment card network.

Include:

- In-person prepaid card transactions that were processed over a signature
- In-person low-value prepaid card transactions for which no signature or PIN was required

Do not include:

- In-person prepaid card transactions authenticated via PIN
- Remote prepaid card transactions

► **Example:** Your customer bought groceries for $20 with his prepaid card, which he authenticated by entering is PIN at the checkout. He also used his prepaid card to buy dinner for $50 that night, which he authenticated by signing the receipt. In this example, you would report one transaction for $50.

6.b) Remote transactions = 6.b.1) + 6.b.2)

These include all general-purpose prepaid card transactions for which the card user does not physically present the card to authorize the transaction, including mail-order transactions, telephone-order transactions, and internet transactions. Please report the total transactions involving domestic (U.S.) payees (item **6.b.1**) and foreign payees (item **6.b.2**).

Include:

- Remote prepaid card transactions (e.g., mail-order transactions, telephone-order transactions)
- Digital wallet in-app or browser prepaid card transactions (e.g., e-commerce transactions)

Do not include:

- Transactions for which the card user is present
- Mobile transactions at the point of sale (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)
- Contactless card transactions at the point of sale (i.e., "tap and pay" physical cards, fobs, or stickers)
- Intermediated transactions at the point of sale (i.e., Square, Clover, iZettle)
- Card-not-present transactions for which the card user is present at the point of sale (i.e., key-entered transactions)

► **Example:** Your prepaid cardholder purchased a $500 item on a German internet website with his prepaid card by entering his prepaid card number, name, and address. He then proceeded to buy a $65 pair of shoes from a U.S.-based store in a mobile application not at the point of sale, paying with the same prepaid card with his digital wallet (Android Pay). In this example, you would report two transactions for $565 in item **6.b)**, one transaction for $65 in item **6.b.1),** and one transaction for $500 in item **6.b.2)**.

6.b.1) Domestic (U.S.) payee

These are remote prepaid card transactions in which a U.S. person or company (i.e., located in the 50 U.S. states, D.C., or U.S. territories) is the recipient of the payment.

Include:

- Domestic payee remote prepaid card transactions (e.g., mail-order transactions, telephone-order transactions)
- Domestic payee digital wallet in-app or browser prepaid card transactions (e.g., e-commerce transactions)

Do not include:

- Foreign payee remote prepaid card transactions
- Transactions for which the card user is present

► **Example:** Your prepaid cardholder purchased a $100 item on a Chinese internet website from a Chinese (foreign) merchant with his prepaid card by entering his prepaid card number, name, and address. He then proceeded to buy a $70 of groceries from a New York grocery store in a mobile application not at the point of sale, paying with the same prepaid card with his digital wallet (Google Pay). In this example, you would report one transaction for $70 under **6.b.1)**. [Note that the foreign payee transaction for $100 would be reported under **6.b.2)**].

6.b.2) Foreign payee

These are remote prepaid card transactions in which a non-U.S. person or company is the recipient of the payment.

Include:

- Foreign payee remote prepaid card transactions (e.g., mail-order transactions, telephone-order transactions)
- Foreign payee digital wallet in-app or browser prepaid card transactions (e.g., e-commerce transactions)

Do not include:

- Domestic payee remote prepaid card transactions
- Transactions for which the card user is present

► **Example:** Your prepaid cardholder purchased a $100 item on a Chinese internet website from a Chinese (foreign) merchant with his prepaid card by entering his prepaid card number, name, and address. He then proceeded to buy $70 of groceries from a New York (U.S.-based merchant) grocery store in a mobile application not at the point of sale (in-app transaction), paying with the same prepaid card with his digital wallet (Google Pay). In this example, you would report one transaction for $100 under **6.b.2)**. [Note that the domestic payee transaction for $70 would be reported under **6.b.1)**]

7) Third-party fraudulent general-purpose prepaid card transactions = 7.a) + 7.b)

These include all third-party unauthorized prepaid card transactions, before any recoveries or chargebacks, for which your institution was the card issuer. Please report any fraudulent third-party prepaid card transactions, regardless of whether the transaction resulted in a loss of funds. If your answer is **No** to item **2)** above, please report "0" here.

Include:

- Prepaid 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 credit card transactions
- Fraudulent debit card transactions
- Fraudulent ATM withdrawals
- Prepaid card transactions authorized by a valid card user as part of a scam

► **Example 1:** Your accountholder's prepaid card issued by your institution was stolen. The perpetrator used the card to make one purchase worth $50. In this example, you would report one transaction for $50.

► **Example 2:** Your accountholder claimed that her prepaid card was stolen and used to purchase a $200 TV in an electronics store. An investigation by your institution determined that in fact your accountholder made this purchase on her card. Since this transaction is an example of first-party fraud (false claim of fraud), it should not be included in item **7)**.

7.a) In-person transactions = 7.a.1) + 7.a.2)

These include only third-party fraudulent general-purpose prepaid card transactions for which the card user is physically present with the card at the point of sale. Include digital wallet (Apple Pay, Android Pay, Samsung Pay, etc.) transactions at the point of sale only. Include all third-party unauthorized prepaid card transactions, before any recoveries or chargebacks. Please report any fraudulent third-party prepaid card transactions, regardless of whether the transaction resulted in a loss of funds. Please report the total transactions with PIN authentication (item **7.a.1**), and without PIN authentication (item **7.a.2**).

Include:

- Fraudulent transactions for which the prepaid card perpetrator is present
- Fraudulent contactless prepaid card transactions (i.e., "tap and pay" with a prepaid card)
- Fraudulent mobile transactions at the point of sale (i.e., 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 (i.e., Square, Clover, iZettle)
- Fraudulent card-not-present transactions for which the card user is present at the point of sale (i.e., key-entered transactions)

Do not include:

- Fraudulent remote prepaid card transactions (e.g., mail-order transactions, telephone-order transactions)
- Fraudulent digital wallet in-app or browser prepaid card transactions (e.g., e-commerce transactions)

► **Example 1:** Your accountholder's prepaid card was stolen. The perpetrator used the card to make two online purchases totaling $100 over the internet. He then bought lunch for $35 at a restaurant using the stolen card. In this example, you would report one transaction for $35.

► **Example 2:** Your accountholder registered her prepaid card online and later claimed that her prepaid card was stolen and used to purchase a $500 TV in an electronics store. An investigation by your institution determined that in fact your accountholder made this purchase on her card. Since this transaction is an example of first-party fraud (false claim of fraud), it should not be included in item **7.a**).

7.a.1) With a PIN

These are fraudulent prepaid card transactions that are authenticated when the user enters their PIN at checkout.

Include:

- Fraudulent in-person prepaid card transactions authenticated via PIN

Do not include:

- Fraudulent in-person prepaid card transactions that were processed over a signature
- Fraudulent in-person low-value prepaid card transactions for which no signature or PIN was required
- Fraudulent remote prepaid card transactions

► **Example:** Your accountholder's prepaid card was stolen, and the perpetrator watched her enter her PIN at the point of sale before stealing the card. The perpetrator then used her card and PIN to buy a $200 watch at a jewelry store. He then used the card to buy dinner for $50 at a nearby restaurant by fraudulently signing the receipt. In this example, you would report one transaction of $200.

7.a.2) Without a PIN

These are fraudulent prepaid card transactions that are not authenticated when the user enters their PIN at checkout. These transactions use dual-message authentication over the payment card network.

Include:

- Fraudulent in-person prepaid card transactions that were processed over a signature
- Fraudulent in-person low-value prepaid card transactions for which no signature or PIN was required

Do not include:

- Fraudulent in-person prepaid card transactions authenticated via PIN
- Fraudulent remote prepaid card transactions

► **Example:** Your accountholder's prepaid card was stolen, and the perpetrator watched her enter her PIN at the point of sale before stealing the card. The perpetrator then used her card and PIN to buy a $200 watch at a jewelry store. He then used the card to buy dinner for $50 at a nearby restaurant by fraudulently signing the receipt. In this example, you would report one transaction of $50.

7.b) Remote transactions = 7.b.1) + 7.b.2)

These include only third-party fraudulent general-purpose prepaid card transactions for which the card user does not physically present the card to authorize the transaction, including mail-order transactions, telephone-order transactions, and internet transactions. Include all third-party unauthorized prepaid card transactions, before any recoveries or chargebacks. Please report any fraudulent third-party prepaid card transactions, regardless of whether the transaction resulted in a loss of funds. Please report the total transactions to domestic (U.S.) payees (item **7.b.1**) and foreign payees (item **7.b.2**).

Include:

- Fraudulent remote prepaid card transactions (e.g., mail-order transactions, telephone-order transactions)
- Fraudulent digital wallet in-app or browser prepaid card transactions (e.g., e-commerce transactions)

Do not include:

- Fraudulent transactions for which the prepaid card perpetrator is present
- Fraudulent mobile transactions at the point of sale (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)
- Fraudulent contactless card transactions at the point of sale (i.e., "tap and pay" physical cards, fobs, or stickers)
- Fraudulent intermediated transactions at the point of sale (i.e., Square, Clover, iZettle)
- Fraudulent card-not-present transactions for which the card user is present at the point of sale (i.e., key-entered transactions)

► **Example 1:** Your accountholder's prepaid card was stolen. The perpetrator used the card to purchase 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. In this example, you would report one transaction for $250.

► **Example 2:** Your accountholder claimed that his prepaid card was stolen and used to purchase a $20 video game online. An investigation by your institution determined that in fact your accountholder made this purchase on his card. Since this transaction is an example of first-party fraud (false claim of fraud), it should not be included in item **7.b**).

7.b.1) Domestic (U.S.) payee

These are fraudulent remote prepaid card transactions in which a U.S. person or company (i.e., located in the 50 U.S. states, D.C., or U.S. territories) is the recipient of the payment.

Include:

- Fraudulent domestic payee remote prepaid card transactions (e.g., mail-order transactions, telephone-order transactions)
- Fraudulent domestic payee digital wallet in-app or browser prepaid card transactions (e.g., e-commerce transactions)

Do not include:

- Fraudulent foreign payee remote prepaid card transactions
- Fraudulent transactions for which the card perpetrator present

► **Example:** Your accountholder's prepaid card was stolen. The perpetrator used the card to buy a $250 coat online from a French retailer. He then used the card online to buy a $15 book from a U.S. bookstore. In this example, you would report one transaction for $15.

7.b.2) Foreign payee

These are fraudulent remote debit card transactions in which a non-U.S. person or company is the recipient of the payment.

Include:

- Fraudulent foreign payee remote prepaid card transactions (e.g., mail-order transactions, telephone-order transactions)
- Fraudulent foreign payee digital wallet in-app or browser prepaid card transactions (e.g., e-commerce transactions)

Do not include:

- Fraudulent domestic payee remote prepaid card transactions
- Fraudulent transactions for which the card user is present

► **Example:** Your accountholder's prepaid card was stolen. The perpetrator used the card to buy a $250 coat online from a French retailer. He then used the card online to buy a $15 book from a U.S. bookstore. In this example, you would report one transaction for $250.

8) General-purpose prepaid digital wallet transactions = 8.a) + 8.b)

Report all general-purpose prepaid card transactions made via a digital wallet, including tokenized digital wallet. If your answer is **No** to item **2)** above, please report "0" here.

Include:

- Digital wallet transactions made by using electronic devices, such as a smartphone, smart watch, or activity tracker, by "tapping" the device at the POS terminal (i.e., Apple Pay, Samsung Pay, Google Pay, Fitbit Pay, Masterpass)
- Tokenized digital wallet transactions made by using customer's payment credentials saved in a virtual account number. These credentials can be stored either on a smartphone or in the cloud. When making a purchase, a substitute account number and a transaction specific code ("token") are used to process payments. This can include purchasing items online with a computer or using a smartphone to make a purchase with a browser or in-app (i.e., Apple Pay, Google Pay, Masterpass, Visa Checkout, Amex Express Checkout)
- Digital wallet NFC (near field communication) transactions, MST (magnetic secure transmission) transactions, QR code transactions, barcode transactions, in-app transactions, or browser transactions.

Do not include:

- Card-on-file e-commerce transactions (cardholder-initiated or merchant-initiated) (i.e., installment payment).

► **Example:** Your customer bought a movie ticket for $10 with his prepaid card, which was loaded into his digital wallet (Apple Pay). He physically tapped his phone on the POS device to pay for the movie ticket, using NFC technology. He then ordered a $30 dinner in a mobile application, paying with the same prepaid card via his digital wallet (Apple Pay). In this example, you would report two transactions for $40.

8.a) In-person transactions

Include transactions for which an electronic device, such as a smartphone, smart watch, or activity tracker, was "tapped" to pay at the POS terminal (i.e., Apple Pay, Samsung Pay, Google Pay, Fitbit Pay)

Include:

- Mobile transactions at the point of sale (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)

Do not include:

- In-app transactions or browser transactions made with a digital wallet (e.g., Apple Pay, Google Pay, Samsung Pay)
- Tokenized digital wallet transactions made by using customer's payment credentials saved in a virtual account (e.g., Apple Pay, Google Pay, Masterpass, Visa Checkout, Amex Express Checkout)
- Card-on-file e-commerce transactions (cardholder-initiated or merchant-initiated) (e.g., installment payment)

► **Example:** Your customer bought lunch for $15 with his prepaid card, which was loaded into his digital wallet (Apple Pay). He physically tapped his phone on the POS device to pay for lunch, using NFC technology. He then bought groceries for $100 with his prepaid card by swiping the card in a magnetic reader. In this example, you would report one transaction for $15.

8.b) Remote transactions

Include in-app transactions or browser transactions made with a digital wallet. Browser transactions include both digital wallets (i.e., Apple Pay, Google Pay, Samsung Pay) and third-party tokenized digital wallets (i.e., PayPal, Amazon Pay, Square Restaurants, Visa Checkout, Masterpass)

Include:

- In-app transactions or browser transactions made with a digital wallet (e.g., Apple Pay, Google Pay, Samsung Pay)
- Tokenized digital wallet transactions made by using customer's payment credentials saved in avirtual account (e.g., Apple Pay, Google Pay, Masterpass, Visa Checkout, Amex Express Checkout)

Do not include:

- Mobile transactions at the point of sale (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)
- Card-on-file e-commerce transactions (cardholder-initiated or merchant-initiated) (e.g., installment payment)

► **Example:** Your customer purchased a $500 item on an internet website with his prepaid card by entering his prepaid card number, name, and address. He then bought a $65 pair of shoes in a mobile application, paying with the same prepaid card with his digital wallet (Google Pay). In this example, you would report one transaction for $65.

9) General-purpose prepaid card cash-back transactions

These include all prepaid card transactions for which your institution was the card issuer and in which the accountholders received cash back at the point of sale. These include both signature-based cash-back and PIN-based cash-back transactions. For cash-back value, only include the amount of cash your card users received at the point of sale. If your answer is **No** to item **2)** above, please report "0" here.

Include:

- Prepaid card cash-back transactions at the point of sale (i.e., amount of cash received at the point of sale)

Do not include:

- ATM withdrawals
- Credit card transactions
- Debit card transactions
- The amount paid for goods and services

► **Example:** Your customer used her prepaid card at the grocery store to purchase $50 of food. She entered her PIN to authorize the transaction and also requested $20 cash back. In this example, you would report one transaction for $20.

General-Purpose Credit Cards

GENERAL TERMINOLOGY

Credit card transactions

All transactions made with credit or charge cards issued by your institution, meaning that your institution owns the receivables. All purchase and bill-pay transactions made with credit cards used for point-of-sale (POS) transactions. These transactions can be authenticated by either a Personal Identification Number (PIN), signature, EMV, online authorization, or any other digital method (NFC, QR code, etc.). Transactions may originate, for example, at a physical point of sale, via telephone, or via the internet. For this study, please follow these guidelines:

Credit card transactions include…	Credit card transactions do <u>not</u> include…
▪ Network transactions made with Visa, MasterCard, Discover, or American Express branded credit cards. These include secured and unsecured credit cards. ▪ Network transactions originated in other countries	▪ Debit card transactions ▪ Prepaid card transactions ▪ Convenience checks ▪ Balance transfers

Digital Wallet

All purchase and bill-pay transactions made using a digital wallet in which users can complete purchases using near-field communication (NFC) that works in conjunction with mobile payment systems, MST (magnetic secure transmission) transactions, QR code transactions, barcode transactions, in-app transactions, or browser transactions. Digital wallets can be used during in-person transactions or remote transactions. In-person transactions require the payment holder to be present to use their digital wallet, while remote transactions are used during e-commerce sales in which the authorization and transaction processes are not physically close to each other.

Digital wallet transactions include those made by using electronic devices, such as a smartphone, smart watch, or activity tracker, by "tapping" the device at the POS terminal (i.e., Apple Pay, Samsung Pay, Google Pay, Fitbit Pay, Masterpass).

They also include tokenized digital wallet transactions made by using customer's payment credentials saved in a virtual account number. These credentials can be stored either on a smartphone or in the cloud. When making a purchase, a substitute account number and a transaction specific code ("token") are used to process payments. This can include purchasing items online with a computer or using a smartphone to make a purchase with a browser or in-app (i.e., Apple Pay, Google Pay, Masterpass, Visa Checkout, Amex Express Checkout).

Contactless Card

Contactless card payment is a secure method for consumers to purchase products or services via credit smartcards (also known as chip cards) using RFID technology. To make a contactless payment, the user simply taps his or her credit card near a POS terminal (an action sometimes referred to as "tap-and-go" or "tap-and-pay").

Consumer account

A credit card account for personal use by an individual or household from which payments can be made.

Business/government account

A credit account owned by an organization (i.e., business, government or not-for-profit organization) from which payments can be made.

Note: Please report small business accounts under business/government accounts, if possible.

U.S. domiciled account

Accounts located within the 50 U.S. states, D.C., or U.S. territories such as Guam, Puerto Rico, or U.S. Virgin Islands). Only report data associated with your institution's U.S. domiciled accounts, including transactions that are domestic and cross-border.

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 item is the credit limit (or some percentage thereof). Also included are convenience checks drawn on a credit card account and balance transfers.

Note: This questionnaire does not consider credit card cash advances as credit card transactions. Do not include cash advances transactions in this section of the survey.

Convenience checks

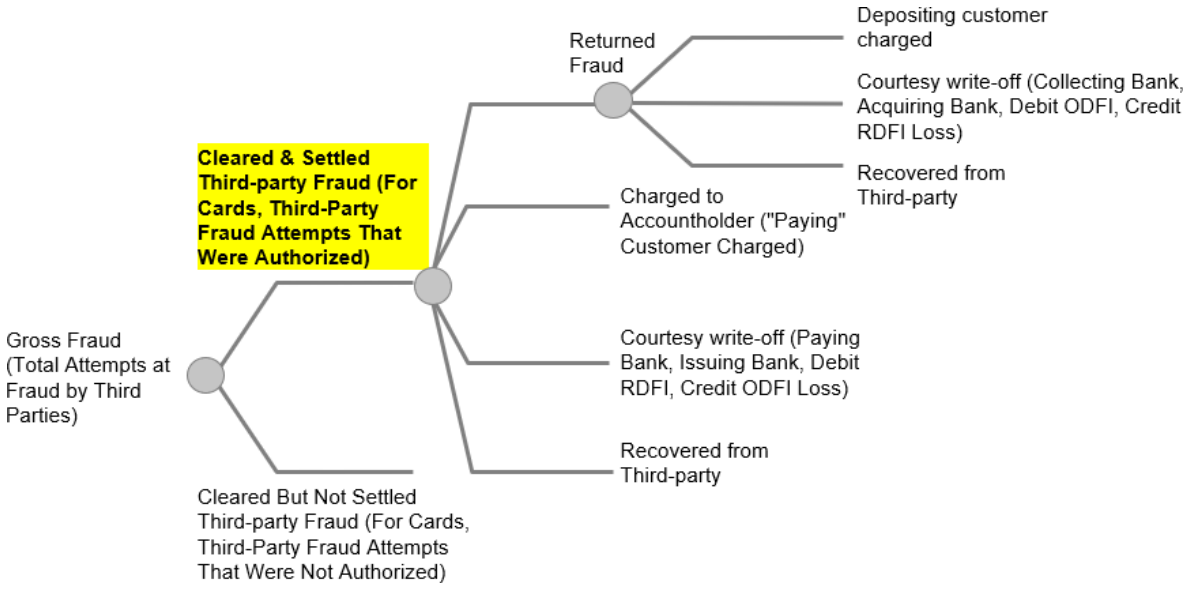
A check linked to a cardholder's credit line that can be used to make purchases, pay bills or transfer balances from one credit account to another. Convenience checks can be written up to the amount of the cardholder's credit limit (or some percentage thereof) and are considered cash advances.

Balance transfers

The transfer by a credit card accountholder of an outstanding debt balance from one credit card account to another. These are considered cash advances.

Third-party fraud

The Federal Reserve Payments Study has identified a measure of fraud that can be described as cleared and settled third-party fraudulent transactions. The measure is not a loss-of-funds measure, nor is it a measure of fraud attempts; rather, it is a measure of the extent to which third parties who are not authorized to conduct transactions are able to penetrate the payment system and effect settlement between banks, or create a book transfer of funds if the transaction happens within one 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 manages to create a 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.



SURVEY ITEMS

1) Did your institution have general-purpose credit cards in circulation in 2018 for which your institution was the issuer?

These include general-purpose credit cards, charge cards, and co-branded cards for which your institution owns the receivables and that use any one of the four major credit card networks (i.e., Visa, MasterCard, American Express, and Discover). If your answer to this question is **No**, please report "0" for all items below.

2) Did your institution have co-branded credit cards (using one of the above four major credit card networks) in circulation in 2018 for which your institution was the issuer?

These are retail merchant credit cards that are issued in partnership with a specific network processor (i.e., Visa, MasterCard, American Express, and Discover). Co-branded cards are branded with the logo of the retailer and network processor. Users can earn discounts or rewards points when they make purchases with sponsoring merchants.

If your answer is **Yes**, please exclude "internal" (closed-loop, not using one of the above four major credit card networks) and include "external" (open-loop, using one of the above four major credit card networks) volumes in your answers below.

2.a) If your answer is "Yes" to item 2) above, are you able to exclude "internal" (closed loop, not using one of the four major credit card networks) volumes from your answers below?

If your answer is **Yes, in some cases**, please explain in the comments box at the end of the General-Purpose Credit Cards section.

3) Total general-purpose credit card accounts = 3.a) + 3.b)

These include general-purpose credit card accounts for which your institution was the issuer. Please report account totals, not cards (i.e., if a customer and their spouse both have a card under the same account, please report as one account). If your answer is **No** to item **1)** above, please report "0" here.
Average of monthly totals means the average of end-of-month totals for each of the months in 2018.

Include:

- All general-purpose credit card accounts, including zero-balance active accounts, with a credit line and the ability to transact

Do not include:

- Private-label credit or charge card accounts whose cards can only be used at a limited set of merchants and that do not use one of the four major credit card networks
- White-label card accounts for which your institution was not the issuing institution
- Transaction deposit accounts
- Closed accounts

► **Example:** Tom, your consumer customer, has one credit card issued by your institution. Joe's Diner, your corporate customer, has a corporate credit card account with separate cards for each of their ten employees. In this example, you would report two credit card accounts.

3.a) Consumer accounts

These include all credit card accounts that are for consumer accountholders. Please see the **General Terminology** section above for the definition of consumer accounts.

Include:

- All credit card accounts for consumer accountholders with credit card accounts for which your institution was the issuer

Do not include:

- Business/government credit card accounts
- Private-label credit or charge card accounts whose cards can only be used at a limited set of merchants and that do not use one of the four major credit card networks
- White-label card accounts for which your institution was not the issuing institution
- Transaction deposit accounts
- Closed accounts

► **Example:** Tom used his credit card issued by your institution to buy a $40 pair of jeans. His wife then used another card linked to the same account to buy $15 worth of candy. In this example, you would report one consumer credit card account.

3.b) Business/government accounts

These include all debit cards accounts that are for business/government accountholders. Please see the **General Terminology** section above for the definition of business/government accounts.

Include:

- All credit card accounts for business/government accountholders with credit card accounts for which your institution was the issuer

Do not include:

- Consumer credit card accounts
- Private-label credit or charge card accounts whose cards can only be used at a limited set of merchants and that do not use one of the four major credit card networks
- White-label card accounts for which your institution was not the issuing institution
- Transaction deposit accounts
- Closed accounts

► **Example:** Your corporate accountholder made a purchase of $500 with a corporate credit card issued by your institution. An employee of the same institution then used her own credit card linked to the same account to make a purchase of $100. In this example, you would report one business/government credit card account.

4) Consumer general-purpose credit card accounts (repeat item 3.a) = 4.a) + 4.b) + 4.c) + 4.d)

Please repeat item **3.a)** from above. These include general-purpose credit cards for which your institution was the issuer. If your answer is **No** to item **1)** above, please report "0" here. If you are unable to report items **4.a)**, **4.d)**, **4.d.1)**, and **4.d.2)**, please explain in the comments field. In this case, report "NR" for those items and report balances for **4.b)** and **4.c)**.

Report interest-free balance transfers and interest-free spend (e.g., on introductory card offers) under current balances for the duration of the interest-free period.

Average of monthly totals means the average of end-of-month totals for each of the months in 2018.

4.a) With zero balance (no current balance, no revolving balance)

These are accounts with zero balance at the end of the billing cycle and have no purchase activity.

► **Example:** Joe has a credit card issued by your institution. He has never made a purchase on this card, although the card account has been activated. In this example, you would report one credit card account with a balance of $0.

4.b) With current balance only (nonzero current balance, no revolving balance)

These include the total number of accounts in which there is an amount owed on the credit card up to the end of the most recent billing cycle. This is the balance that needs to be paid by a certain due date so that no interest is applied.

► **Example:** Jay has a credit card issued by your institution, and he is a transactor (i.e., he pays the balance in full each cycle). He uses this card to make purchases occasionally and had $300 outstanding at the end of last cycle. Jay has until the end of the next billing cycle to pay the balance before interest is applied. In this example, you would report one credit card account with a balance of $300.

4.c) With revolving balance only (no current activity)

These include the total number of accounts in which there is an amount owed on the credit card for which interest was applied already. This is the balance which was not paid by its due date.

► **Example:** Rachael has a credit card issued by your institution, and she is a revolver (i.e., she carries a balance from one cycle to the next). She frequently uses this card to make purchases, and she had a balance of $500 that was outstanding at the end of the prior month, of which interest was applied to her bill this month. In this example, you would report one credit card account with a balance of $500. Do not include interest.

4.d) With current and revolving balances = 4.d.1) + 4.d.2)

These include the total number of accounts in which there is an amount owed on the credit card which includes interest that was applied already, as well as a current balance owed on the most recent billing cycle. This includes both the balance that was not paid by its due date, as well as the balance that needs to be paid by a certain due date to avoid incurring an interest expense.

► **Example:** Sarah has a credit card issued by your institution. She frequently uses this card to make purchases, and she had a balance of $500 that was outstanding at the end of the prior month, of which interest was applied to her bill this month. She then spent an additional $200 on the same card this month, of which interest has not yet been applied. In this example, you would report one credit card account with a balance of $700.

4.d.1) Current balance

Total amount owed on the credit card up to the end of your most recent billing cycle. Thisis the balance that you need to pay by a certain due date so that no interest is applied.

► **Example:** Sarah has a credit card issued by your institution. She frequently uses this card to make purchases, and she had a balance of $500 that was outstanding at the end of the prior month, of which interest was applied to her bill this month. She then spent an additional $200 on the same card this month, of which interest has not yet been applied. In this example, the current balance would be $200.

4.d.2) Revolving balance

Total amount owed on the credit card on which interest was applied already. This is the balance which was not paid by its due date.

► **Example:** Sarah has a credit card issued by your institution. She frequently uses this card to make purchases, and she had a balance of $500 that was outstanding at the end of the prior month, of which interest was applied to her bill this month. She then spent an additional $200 on the same card this month, of which interest has not yet been applied. In this example, the revolving balance would be $500. Do not include interest.

5) Number of general-purpose credit cards = 5.a) + 5.b)

For cards in force, report only cards that had been issued by your institution, activated by your institution's accountholders, and had not expired at the end of a month.

For cards in force with purchase activity, report only cards in force that were used to make at least one point-of-sale (POS) and/or bill payment in a month.

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

Average of monthly totals means the average of end-of-month totals for each of the months in 2018.

Do not include:

- Private-label credit or charge card accounts whose cards can only be used at a limited set of merchants and that do not use one of the four major credit card networks
- White-label card accounts for which your institution was not the issuing institution
- Transaction deposit accounts
- Closed accounts

► **Example:** Your institution has 500 credit cards issued to your consumer and business accountholders. Of these credit cards, 450 cards have been activated and are not expired, 30 cards have not been activated yet, and 20 cards have been activated but are now expired. Of the 450 cards that are active and not expired, 350 cards have been used to make at least one purchase in 2018. In this example, you would report 450 credit cards in force and 350 credit cards with purchase activity.

5.a) Consumer cards

These include all credit cards associated with consumer accounts. Please see the **General Terminology** section above for the definition of consumer accounts.

Include:

- All credit cards for consumer accountholders over any credit card network for which your institution was the issuer

Do not include:

- Business/government credit cards
- Consumer and business/government debit cards
- Consumer and business/government prepaid cards

► **Example:** Your institution has 500 credit cards issued to your consumer accounts. Of these credit cards, 450 cards have been activated and are not expired, 30 cards have not been activated yet, and 20 cards have been activated but are now expired. Of the 450 cards that are active and not expired, 350 cards have been used to make at least one purchase in 2018. In this example, you would report 450 consumer credit cards in force and 350 consumer credit cards with purchase activity.

5.b) Business/government cards

These include all credit cards associated with business/government accounts. Please see the **General Terminology** section above for the definition of business/government accounts.

Include:

- All credit cards for business/government accountholders over any credit card network for which your institution was the issuer

Do not include:

- Consumer credit card accounts
- Consumer and business/government debit card accounts
- Consumer and business/government prepaid card accounts

► **Example:** Your institution has 1,000 credit cards issued to business/government accountholders. Of these credit cards, 900 cards have been activated and are not expired, 70 cards have not been activated yet, and 30 cards have been activated but are now expired. Of the 900 cards that are active and not expired, 800 cards have been used to make at least one purchase in 2018. In this example, you would report 900 business credit cards in force and 800 credit cards with purchase activity.

6) Total general-purpose co-branded credit card non-network transactions ("internal" closed-loop transactions)

These are retail merchant credit cards that are issued in partnership with a specific network processor (i.e., Visa, MasterCard, American Express, and Discover). Co-branded cards are branded with the logo of the retailer and network processor. Users can earn discounts or rewards points when they make purchases with sponsoring merchants. If your answer is **No** to item **1)** above, please report "0" here.

Include:

- "Internal" (closed-loop, not using one of the above four major credit card networks) co-branded credit card network transactions

Do not include:

- "External" (open-loop, using one of the above four major credit card networks) co-branded credit card network transactions

► **Example:** Your customer paid for her $200 hotel room with her credit card that was issued by your institution and co-branded with a hotel company. Later that day, she used another credit card issued by your institution to buy lunch for $20. In this example, you would report only one transaction for $200.

7) Total general-purpose credit card network transactions = 7.a) + 7.b)

These include all network transactions over any credit card network for which your institution was the issuer. If your answer is **No** to item **1)** above, please report "0" here.

Include:

- All transactions made with general-purpose credit cards, charge cards, or co-branded cards (network volume) issued by your institution
- Both consumer and business/government credit card transactions
- Both in-person and remote credit card transactions

Do not include:

- General-purpose credit card non-network transactions (i.e., balance transfers, convenience checks)
- Co-branded credit card "internal" closed-loop transactions
- Debit card transactions
- Prepaid card transactions
- Credit card cash advances (e.g., ATM withdrawals, over-the-counter withdrawals)

► **Example:** Your customer bought $50 of groceries with her credit card. Later that day, she used the same credit card issued by your institution to purchase a $70 purse online. In this example, you would report two transactions for $120.

7.a) From consumer accounts

Include:

- All transactions made by consumer accountholders with general-purpose credit cards, charge cards, or co-branded cards (network volume) issued by your institution
- Both in-person and remote credit card transactions

Do not include:

- Credit card transactions made by business/government accountholders
- Debit card transactions made by consumer or business/government accountholders
- Prepaid card transactions made by consumer or business/government accountholders
- General-purpose credit card non-network transactions (i.e., balance transfers, convenience checks)
- Co-branded credit card "internal" (closed-loop transactions) volume
- Credit card cash advances (e.g., ATM withdrawals, over-the-counter withdrawals)

► **Example:** Tom used his credit card issued by your institution to buy a $40 pair of jeans. Later that day, he used his credit card at the ATM to make a $500 cash advance. In this example, you would report one transaction for $40.

7.b) From business/government accounts

Include:

- All transactions made by business/government accountholders over any credit card network for which your institution was the issuer

Do not include:

- Credit card transactions made by consumer accountholders
- Debit card transactions made by consumer or business/government accountholders
- Prepaid card transactions made by consumer or business/government accountholders
- General-purpose credit card non-network transactions (i.e., balance transfers, convenience checks)
- Co-branded credit card "internal" (closed-loop transactions) volume
- Credit card cash advances (e.g., ATM withdrawals, over-the-counter withdrawals)

► **Example:** Your corporate accountholder made a purchase of $500 with a corporate credit card issued by your institution. Later that day, he made a cash advance using the same credit card and withdrew $200 in cash over the counter at one of your branch locations. In this example, you would report one transaction for $500.

8) Total general-purpose credit card network transactions (repeat item 7) = 8.a) + 8.b)

Repeat item **7)** from above. These include all transactions over any credit card network for which your institution was the issuer. If your answer is **No** to item **1)** above, please report "0" here.

Include:

- All transactions made with general-purpose credit cards, charge cards, or co-branded cards (network volume) issued by your institution
- Both consumer and business/government credit card transactions
- Both in-person and remote credit card transactions

Do not include:

- General-purpose credit card non-network transactions (i.e., balance transfers, convenience checks)
- Co-branded credit card "internal" closed-loop transactions
- Debit card transactions
- Prepaid card transactions
- Credit card cash advances (e.g., ATM withdrawals, over-the-counter withdrawals)

► **Example:** Your customer bought $50 of groceries with her credit card. Later that day, she used the same credit card issued by your institution to purchase a $70 purse online. In this example, you would report two transactions for $120.

8.a) In-person transactions = 8.a.1) + 8.a.2)

These include all general-purpose credit card transactions for which the card user is physically present with the card at the point of sale. Include digital wallet (Apple Pay, Samsung Pay, etc.) transactions at the point of sale only. Please report the total transactions using a PIN (item **8.a.1**), and without a PIN (item **8.a.2**).

Include:

- Transactions for which the card user is present
- Mobile transactions at the point of sale (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)
- Contactless card transactions at the point of sale (i.e., "tap and pay" physical cards, fobs, or stickers)
- Intermediated transactions at the point of sale (i.e., Square, Clover, iZettle)
- Card-not-present transactions for which the card user is present at the point of sale (i.e., key-entered transactions)

Do not include:

- Remote transactions
- Digital wallet in-app or browser transactions

► **Example:** Your customer bought a coat for $100 with his credit card by entering his PIN at the checkout line. Later that day, he bought a $40 train ticket with his credit card by signing the receipt at the checkout. For this example, you would report two transactions for $140 in item **8.a)**, one transaction for $100 for **8.a.1)**, and one transaction for $40 for **8.a.2)**.

8.a.1) With a PIN

These are credit card transactions that are authenticated when the user enters their PIN at point of sale.

Include:

- In-person credit card transactions authenticated via PIN

Do not include:

- In-person credit card transactions that were processed over a signature
- In-person low-value credit card transactions for which no signature or PIN was required
- Remote credit card transactions

► **Example:** Your customer bought lunch for $15 with his credit card by entering his PIN at the checkout line. Later that day, he bought a $30 sweater with his credit card by signing the receipt at the checkout. In this example, you would report one transaction for $15.

8.a.2) Without a PIN

These are credit card transactions that are not authenticated using a PIN at the point ofsale (single-message over the payment card network). These transactions use dual- message authentication over the payment card network.

Include:

- In-person credit card transactions that were processed over a signature
- In-person low-value credit card transactions for which no signature or PIN was required.

Do not include:

- In-person credit card transactions authenticated via PIN
- Remote credit card transactions

► **Example:** Your customer bought lunch for $15 with his credit card by entering his PIN at the checkout line. Later that day, he bought a $30 sweater with his credit card by signing the receipt at the checkout. For this example, you would report one transaction for $30.

8.b) Remote transactions = 8.b.1) + 8.b.2)

These include all general-purpose credit card transactions for which the card user does not physically present the card to authorize the transaction, including mail-order transactions, telephone-order transactions, and internet transactions. Please report the total transactions for domestic (U.S.) payees (item **8.b.1**) and foreign payees (item **8.b.2**).

Include:

- Remote credit card transactions (e.g., mail-order transactions, telephone-order transactions)
- Digital wallet in-app or browser credit card transactions (e.g., e-commerce transactions)

Do not include:

- Transactions for which the card user is present
- Mobile transactions at the point of sale (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)
- Contactless card transactions at the point of sale (i.e., "tap and pay" physical cards, fobs, or stickers)
- Intermediated transactions at the point of sale (i.e., Square, Clover, iZettle)
- Card-not-present transactions for which the card user is present at the point of sale (i.e., key-entered transactions)

► **Example:** Your customer purchased a $500 item on a German internet website with his credit card by entering his credit card number, name, and address. He then proceeded to buy a $65 pair of shoes from a U.S.-based store in a mobile application not at the point of sale, paying with the same credit card with his digital wallet (Google Pay). In this example, you would report two transactions for $565 in item **8.b)**, one transaction for $65 in item **8.b.1),** and one transaction for $500 in item **8.b.2)**.

8.b.1) Domestic (U.S.) payee

These are remote credit card transactions in which a U.S. person or company (i.e., located in the 50 U.S. states, D.C., or U.S. territories) is the recipient of the payment.

Include:

- Domestic payee remote credit card transactions (e.g., mail-order transactions, telephone-order transactions)
- Domestic payee digital wallet in-app or browser credit card transactions (e.g., e-commerce transactions)

Do not include:

- Foreign payee remote credit card transactions
- Transactions for which the card user is present

► **Example:** Your customer purchased a $100 item on a Chinese internet website from a Chinese (foreign) merchant with his credit card by entering his credit card number, name, and address. He then proceeded to buy $70 of groceries from a New York grocerystore in a mobile application not at the point of sale (in-app transaction), paying with the same credit card with his digital wallet (Google Pay). In this example, you would report one transaction for $70 under **8.b.1)**. [Note that the foreign payee transaction for $100 would be reported under **8.b.2)**].

8.b.2) Foreign payee

These are remote credit card transactions in which a non-U.S. person or company is the recipient of the payment.

Include:

- Foreign payee remote credit card transactions (e.g., mail-order transactions, telephone-order transactions)
- Foreign payee digital wallet in-app or browser credit card transactions (e.g., e-commerce transactions)

Do not include:

- Domestic payee remote credit card transactions
- Transactions for which the card user is present

► **Example:** Your customer purchased a $100 item on a Chinese internet website from a Chinese (foreign) merchant with his credit card by entering his credit card number, name, and address. He then proceeded to buy $70 of groceries from a New York (U.S.- based merchant) grocery store in a mobile application not at the point of sale (in-app transaction), paying with the same credit card with his digital wallet (Google Pay). In thisexample, you would report one transaction for $100 under **8.b.2)**. [Note that the domesticpayee transaction for $70 would be reported under **8.b.1)**].

9) Third-party fraudulent general-purpose credit card network transactions = 9.a) + 9.b)

These include 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 the transaction resulted in a loss of funds. If your answer is **No** to item **1)** above, please report "0" here.

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 transactions
- Fraudulent prepaid card transactions
- Credit card transactions authorized by a valid card user as part of a scam
- Fraudulent credit card cash advances (e.g., ATM withdrawals, over-the-counter withdrawals)

► **Example 1:** Your accountholder's credit card issued by your institution was stolen. The perpetrator used the card to make one purchase worth $1,000, which was authorized at the point of sale. In this example, you would report one transaction for $1,000.

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

9.a) In-person transactions = 9.a.1) + 9.a.2)

These include only third-party fraudulent general-purpose credit card transactions for which the card user is physically present with the card at the point of sale. Include digital wallet (Apple Pay, Samsung Pay, etc.) transactions at the point of sale only. Please report the total transactions using PIN (item **9.a.1**), and without PIN (item **9.a.2**).

Include:

- Fraudulent transactions for which the credit card perpetrator is present
- Fraudulent contactless credit card transactions (i.e., "tap and pay" with a credit card)
- Fraudulent mobile transactions at the point of sale (i.e., 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 (i.e., Square, Clover, iZettle)
- Fraudulent card-not-present transactions for which the card user is present at the point of sale (i.e., key-entered transactions)

Do not include:

- Fraudulent remote transactions
- Fraudulent digital wallet in-app or browser transactions

► **Example 1:** Your accountholder's credit card was stolen. The perpetrator used the card to make two purchases totaling $1,000 over the internet. He then bought lunch for $35 at a restaurant using the stolen card. In this example, you would report one transaction for $35.

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

9.a.1) With a PIN

These are fraudulent general-purpose credit card transactions that are authenticated when the user enters their PIN at the point of sale.

Include:

- Fraudulent in-person credit card transactions that were authenticated via PIN

Do not include:

- Fraudulent in-person credit card transactions that were processed over a signature
- Fraudulent in-person low-value credit card transactions for which no signature or PIN was required
- Fraudulent remote credit card transactions

► **Example:** Your accountholder's credit card was stolen, and the perpetrator watchedher enter her PIN at the point of sale before stealing the card. The perpetrator then usedher card and PIN to buy a $200 watch at a jewelry store. He then used the card to buy dinner for $50 at a nearby restaurant by fraudulently signing the receipt. In this example,you would report one transaction of $200.

9.a.2) Without a PIN

These include only third-party fraudulent general-purpose credit card transactions that arenot authenticated using a PIN at the point of sale (single-message over the payment card network). These fraudulent transactions use zip code authentication, card identification number authentication, or other authentication method.

Include:

- Fraudulent in-person credit card transactions that were processed over a signature
- Fraudulent in-person low-value credit card transactions for which no signature or PINwas required

Do not include:

- Fraudulent in-person credit card transactions authenticated via PIN
- Fraudulent remote credit card transactions

► **Example:** Your accountholder's credit card was stolen, and the perpetrator watchedher enter her PIN at the point of sale before stealing the card. The perpetrator then usedher card and PIN to buy a $200 watch at a jewelry store. He then used the card to buy dinner for $50 at a nearby restaurant by fraudulently signing the receipt. In this example,you would report one transaction of $50.

9.b) Remote transactions = 9.b.1) + 9.b.2)

These include only third-party fraudulent general-purpose credit card transactions for which the card user does not physically present the card to authorize the transaction. Please report any fraudulent third-party credit card transactions, regardless of whether the transaction resulted in a loss of funds. Please report the total transactions to domestic (U.S.) payees, (item **9.b.1)** and foreign payees (item **9.b.2)**.

Include:

- Fraudulent remote credit card transactions (e.g., mail-order transactions, telephone-order transactions)
- Fraudulent digital wallet in-app or browser credit card transactions (e.g., e-commerce transactions)

Do not include:

- Fraudulent transactions for which the credit card perpetrator is present
- Fraudulent mobile transactions at the point of sale (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)
- Fraudulent contactless card transactions at the point of sale (i.e., "tap and pay" physical cards, fobs, or stickers)
- Fraudulent intermediated transactions at the point of sale (i.e., Square, Clover, iZettle)
- Fraudulent card-not-present transactions for which the card user is present at the point of sale (i.e., key-entered transactions)

► **Example 1:** Your accountholder's credit card was stolen. The perpetrator used the card to purchase 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. Both transactions were authorized. In this example, you would report one transaction for $250.

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

9.b.1) Domestic (U.S.) payee

These include only third-party fraudulent general-purpose credit card transactions for which the card user does not physically present the card to authorize the transaction anda U.S. person or company (i.e., located in the 50 U.S. states, D.C., or U.S. territories) is the recipient of the payment.

Include:

- Fraudulent domestic payee remote credit card transactions (e.g., mail-order transactions, telephone-order transactions)
- Fraudulent domestic payee digital wallet in-app or browser credit card transactions (e.g., e-commerce transactions)

Do not include:

- Fraudulent foreign payee remote credit card transactions
- Fraudulent transactions for which the card user is present

► **Example:** Your accountholder's credit card was stolen. The perpetrator used the card to buy a $250 coat online from a French retailer. He then used the card online to buya $15 book from a U.S. bookstore. In this example, you would report one transaction for $15.

9.b.2) Foreign payee

These include only third-party fraudulent general-purpose credit card transactions for which the card user does not physically present the card to authorize the transaction anda non-U.S. person or company is the recipient of the payment.

Include:

- Fraudulent foreign payee remote credit card transactions (e.g., mail-order transactions, telephone-order transactions)
- Fraudulent foreign payee digital wallet in-app or browser credit card transactions (e.g., e-commerce transactions)

Do not include:

- Fraudulent domestic payee remote credit card transactions
- Fraudulent transactions for which the card user is present

► **Example:** Your accountholder's credit card was stolen. The perpetrator used the card to buy a $250 coat online from a French retailer. He then used the card online to buya $15 book from a U.S. bookstore. In this example, you would report one transaction for $15.

10) Total general-purpose credit digital wallet transactions = 10.a) + 10.b)

These are all general-purpose credit card transactions made via a digital wallet, including tokenized digital wallet.

Include:

- Digital wallet credit card transactions made by using electronic devices, such as a smartphone, smart watch, or activity tracker, by "tapping" the device at the POS terminal (i.e., Apple Pay, Samsung Pay, Google Pay, Fitbit Pay, Masterpass)
- Tokenized digital wallet credit card transactions made by using customer's payment credentials saved in a virtual account number. These credentials can be stored either on a smartphone or in the cloud. When making a purchase, a substitute account number and a transaction specific code ("token") are used to process payments. This can include purchasing items online with a computer or using a smartphone to make a purchase with a browser or in-app (i.e., Apple Pay, Google Pay, Masterpass, Visa Checkout, Amex Express Checkout.)
- Digital wallet credit card NFC (near field communication) transactions, MST (magnetic secure transmission) transactions, QR code transactions, barcode transactions, in-app transactions, or browser transactions.

Do not include:

- Credit card-on-file e-commerce transactions (cardholder-initiated or merchant-initiated) (i.e., installment payment).

  ► **Example:** Your customer bought a movie for $10 with his credit card, which was loaded into his digital wallet (Apple Pay). He physically tapped his phone on the POS device to pay for lunch, using NFC technology. He then ordered a $30 dinner in a mobile application, paying with the same credit card via his digital wallet (Apple Pay). In this example, you would report two transactions for $40.

10.a) In-person transactions

These include credit card transactions for which an electronic device, such as a smartphone, smart watch, or activity tracker, was “tapped” to pay at the POS terminal (i.e., Apple Pay, Samsung Pay, Google Pay, Fitbit Pay)

Include:

- Mobile transactions at the point of sale (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)

Do not include:

- In-app transactions or browser transactions made with a digital wallet (e.g., Apple Pay, Google Pay, Samsung Pay)
- Tokenized digital wallet transactions made by using customer's payment credentials saved in a virtual account (e.g., Apple Pay, Google Pay, Masterpass, Visa Checkout, Amex Express Checkout)
- Card-on-file e-commerce transactions (cardholder-initiated or merchant-initiated) (e.g., installment payment)

► **Example:** Your customer bought lunch for $15 with his credit card, which was loaded into his digital wallet (Apple Pay). He physically tapped his phone on the POS device to pay for lunch, using NFC technology. He then bought groceries for $100 with his credit card by swiping the card in a magnetic reader. In this example, you would report one transaction for $15.

10.b) Remote transactions

These include in-app credit card transactions or browser transactions made with a digital wallet. Browser transactions include both digital wallets (i.e., Apple Pay, Google Pay, Samsung Pay) and third-party tokenized digital wallets (i.e., PayPal, Amazon Pay, Square Restaurants, Visa Checkout, Masterpass)

Include:

- In-app transactions or browser transactions made with a digital wallet (e.g., Apple Pay, Google Pay, Samsung Pay)
- Tokenized digital wallet transactions made by using customer's payment credentials saved in a virtual account (e.g., Apple Pay, Google Pay, Masterpass, Visa Checkout, Amex Express Checkout)

Do not include:

- Mobile transactions at the point of sale (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)
- Card-on-file e-commerce transactions (cardholder-initiated or merchant-initiated) (e.g., installment payment)

► **Example:** Your customer purchased a $500 item on an internet website with his credit card by entering his credit card number, name, and address. He then bought a $65 pair of shoes in a mobile application, paying with the same credit card with his digital wallet (Google Pay). In this example, you would report one transaction for $65.

Cash

GENERAL TERMINOLOGY

Cash withdrawals

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

Cash withdrawals include…	Cash Withdrawals do <u>not</u> include…
▪ All cash withdrawals by your accountholders (including, as appropriate for the particular survey question, withdrawals made in other countries) ▪ Credit card cash advances ▪ Prepaid card cash withdrawals	▪ 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

Cash deposits

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

Cash deposits include…	Cash deposits do <u>not</u> include…
▪ All cash deposits by your accountholders regardless of channel ▪ Prepaid card deposits	▪ Cash deposits or other transactions by individuals or businesses other than your accountholders ▪ Withdrawal transactions ▪ Inquiries ▪ Funds transfers

Cash advances

A service provided by credit card and charge card issuers that allows cardholders to withdraw a prescribed limit of cash, either in-person through an ATM or over the counter at a bank or other financial agency. For a credit card, this limit is the credit limit or some percentage thereof. Credit card cash advances using ATM withdrawals **excludes** convenience checks drawn on credit card account and balance transfers.

ATM cash withdrawals

Cash withdrawals made by your accountholders at your ATMs or at "foreign" ATMs. For this study, please follow these guidelines:

ATM cash withdrawals include…	ATM cash withdrawals do <u>not</u> include…
▪ All ATM cash withdrawals by your accountholders (including, as appropriate for the particular survey question, withdrawals made in other countries) ▪ Credit card cash advances ▪ Prepaid card cash withdrawals	▪ Cash withdrawals or other transactions by individuals or businesses other than your accountholders ▪ Over-the-counter withdrawals ▪ Withdrawals from remote currency management terminals (RCMTs) ▪ Deposit transactions ▪ Convenience checks ▪ Inquiries ▪ Funds transfers ▪ Statement print-outs ▪ Purchases (i.e., stamps, tickets) ▪ Any other non-withdrawal transactions

Consumer account

An account for personal use by an individual or household from which ATM withdrawals can be made and cash can be deposited.

Business/government account

An account owned by an organization (i.e., business, government or not-for-profit organization) from which ATM withdrawals can be made and cash can be deposited

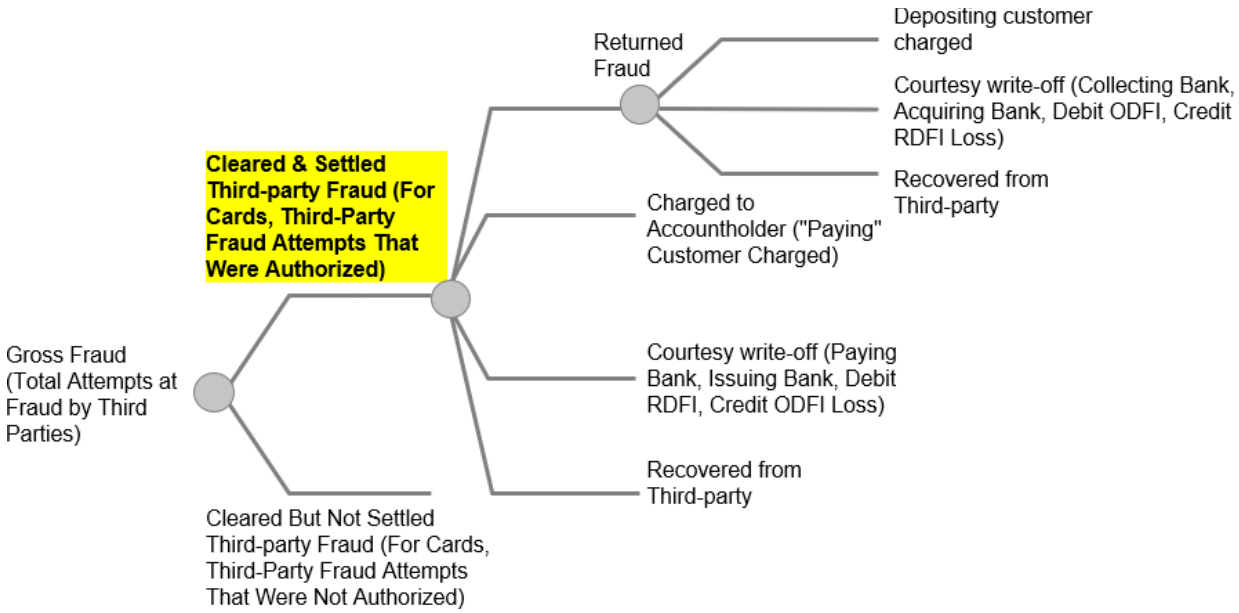
Note: Please report small business accounts under business/government accounts, if possible.

U.S. domiciled account

Accounts located within the 50 U.S. states, D.C., or U.S. territories such as Guam, Puerto Rico, or U.S. Virgin Islands). Only report data associated with your institution's U.S. domiciled accounts, including transactions that are domestic and cross-border.

Third-party fraud

The Federal Reserve Payments Study has identified a measure of fraud that can be described as cleared and settled third-party fraudulent transactions. This measure is not a loss-of-funds measure, nor is it a measure of fraud attempts; rather, it is a measure of the extent to which third parties who are not authorized to conduct transactions are able to penetrate the payment system and effect settlement between banks, or create a book transfer of funds if the transaction happens within one 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 manages to create a 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) Total cash withdrawals from your institution by your accountholders = 1.a) + 1.b) + 1.c) +1.d)

These include all cash withdrawals made from accounts at your institution.

Include:

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

Do not include:

- Noncash withdrawal transactions made from accounts at your institution
- Withdrawals made from accounts at another institution
- Deposit transactions
- Teller vault activity
- Convenience checks
- Balance transfers
- Other non-withdrawal transactions (i.e., inquiries, statement print-outs, purchases of stamps, tickets)

1.a) Over the counter cash withdrawals

These include all cash withdrawals made by your institution's accountholders at bank lobby teller window or drive-through teller.

Note: Please count only over-the-counter cash withdrawals made at your institution's branch locations from accounts at your institution.

Include:

- Withdrawal transactions initiated via a withdrawal slip or via the deposit of any negotiable or nonnegotiable instrument
- Over-the-counter cash withdrawals made using your accountholder's debit, prepaid or credit card linked to the account

Do not include:

- Cash withdrawals at ATM terminals
- Cash withdrawals at ATM terminals located at your institution's branch locations
- Noncash withdrawal transactions made from accounts at your institution
- Withdrawals made from accounts at another institution
- Deposit transactions
- Teller vault activity
- Convenience checks
- Balance transfers
- Other non-withdrawal transactions (i.e., inquiries, statement print-outs, purchases of stamps, tickets)

► **Example:** Your accountholder withdrew $100 in cash over the counter from a teller at one of your institution's branch locations. In this example, you would report one transaction of $100.

1.b) Cash orders at wholesale vaults

These include all cash withdrawals handled through armored couriers including vaults operated by your institution or outsourced to armored couriers or other third-party vault operators. Also include all cash (notes and coin) withdrawals made at wholesale vaults from accounts at your institution.

Note: Please count only cash withdrawals made from accounts at your institution at wholesale vaults.

Include:

- Cash withdrawals at outsourced wholesale vaults made from accounts at your institution

Do not include:

- Cash withdrawals at ATM terminals
- Noncash withdrawal transactions made from accounts at your institution
- Withdrawals made from accounts at another institution
- Deposit transactions
- Teller vault activity
- Convenience checks
- Balance transfers
- Other non-withdrawal transactions (i.e., inquiries, statement print-outs, purchases of stamps, tickets)

► **Example:** 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 and to order $1,500 in various denominations of cash straps and coin rolls to make change available in its store(s). In this example, you would include one cash order for $1,500.

1.c) Cash withdrawals made at remote currency management terminals (RCMTs)

These include 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 (i.e., gas station, restaurant).

Include:

- All cash withdrawals at RCMTs

Do not include:

- Cash deposits made at remote currency management terminals
- Transactions that involved armored couriers withdrawing cash from these terminals or replenishing cash in cash recyclers

► **Example:** 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. In this example, you would report one withdrawal for $1,000.

1.d) Total ATM cash withdrawals (your institution's accountholder, any ATM) = 1.d.1) + 1.d.2)

These include all cash withdrawals made from accounts at your institution from any ATM, including those at your institution's ATM terminals (item **1.d.1)** below) or "foreign" ATMs (item **1.d.2)** below). A "foreign" ATM is an ATM operated by an unaffiliated depository institution or ATM operator that is not sponsored by your institution.

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

Include:

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

Do not include:

- Withdrawals made from accounts at another institution
- Deposit transactions
- Convenience checks
- Balance transfers
- Noncash withdrawal transactions made from accounts at your institution teller vault activity
- Other non-withdrawal transactions (i.e., inquiries, statement print-outs, purchases of stamps, tickets)

► **Example:** Glen is a checking accountholder at your institution. 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. In this example, you would report two ATM withdrawals for a total of $300.

1.d.1) "On-us" ATM withdrawals (your institution's accountholder, your institution's ATM)

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

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

Include:

- Your institution's prepaid, debit, and credit card accountholders' ATM cash withdrawals at your institution's ATMs (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

► **Example:** Your customer used her Visa debit card to withdraw $200 from an ATM located in a grocery store. The ATM is owned and operated by your institution. In this example, you would report one transaction for $200.

1.d.2) "Foreign" ATM withdrawals (your institution's accountholder, "foreign" ATM)

A "foreign" ATM is any ATM not owned or operated by your institution. These are all cash withdrawals made at other institutions' ATMs from accounts at your institution.

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

Include:

- Your institution's prepaid, debit, and credit card accountholders' ATM cash withdrawals at "foreign" ATMs (include cash advances from credit card accountholders)
- Both domestic and cross-border transactions at ATM terminals operated by other depository institutions or by ATM operators that are not sponsored by your institution

Do not include:

- Any transactions at your institution's ATM terminals, regardless of who made them (whether they hold an account at your institution)
- Over-the-counter cash withdrawals
- Non-withdrawal transactions

► **Example:** Your customer used her Visa debit card to withdraw $50 from an ATM located in a grocery store. The ATM is owned and operated by another institution. In this example, you would report one transaction for $50.

2) Total cash withdrawals from your institution (repeat item 1) = 2.a) + 2.b)

Repeat item **1)** above. These include all cash withdrawals made from accounts at your institution.

Include:

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

Do not include:

- Noncash withdrawal transactions made from accounts at your institution
- Withdrawals made from accounts at another institution
- Deposit transactions
- Teller vault activity
- Convenience checks
- Balance transfers
- Other non-withdrawal transactions (i.e., inquiries, statement print-outs, purchases of stamps, tickets)

2.a) From consumer accounts

These include all consumer deposit account cash withdrawals. Please refer to the **General Terminology** section above for the definition of consumer accounts.

Include:

- Consumer or prepaid account withdrawals
- Consumer credit card cash advances

Do not include:

- Business/government account withdrawals

► **Example:** Your consumer accountholder withdrew $250 in cash at an ATM. In this example, you would report one withdrawal of $250.

2.b) From business/government accounts

These include all Business/government account cash withdrawals. Please include small business accounts under business/government accounts. Please refer to the **General Terminology** section above for the definition of business/government accounts.

Include:

- Cash withdrawals made on a debit or prepaid card linked to a business/government account
- Business/government credit card cash advances

Do not include:

- Consumer account withdrawals

► **Example:** Your small business accountholder, a restaurant owner, withdrew $500 in cash over the counter at one of your institution's branches. In this example, you would report one withdrawal of $500.

3) Total ATM cash withdrawals (your institution's accountholder, any ATM) (repeat item 1.d) = 3.a) + 3.b)

These are 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.

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

Include:

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

Do not include:

- Withdrawals by another institution's accountholders at your institution's ATMs
- Deposit transactions
- RCMT withdrawals
- Teller vault activity
- Over-the-counter cash withdrawals
- Other non-withdrawal transactions (i.e., inquiries, statement print-outs, purchases of stamps, tickets)

► **Example:** Glen is a checking accountholder at your institution, and Jennifer is not. Glen withdrew $100cash 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. In this example, you would report two withdrawals for a total of $300.

3.a) Domestic ATM withdrawals (your institution's accountholder, any ATM in the U.S.)

These are cash withdrawals made from accounts at your institution from any ATM located in the U.S. (i.e., ATMs located in the 50 U.S. states, D.C., or U.S. territories).

Include:

- All cash withdrawals on your institution's accounts from any ATM located in the U.S.

Do not include:

- Cash withdrawals on your institution's accounts from any ATM located outside the U.S

► **Example:** Sam, John, and Jenny are checking accountholders at your institution. Sam withdrew $100 in cash at one of your institution's ATMs located in New York. John withdrew $150 in cash at another institution's ATM located in Chicago. Jenny withdrew $200 in cash at another institution's ATM located in Canada. In this example, you would report two withdrawals for a total of $250.

3.b) Cross-border ATM withdrawals (your institution's accountholder, any ATM outside the U.S.)

These are cash withdrawals made from accounts at your institution from any ATM located outside the U.S.

Include:

- All cash withdrawals on your institution's accounts from any ATM located outside the U.S.

Do not include:

- Cash withdrawals on your institution's accounts from any ATM located in the U.S

► **Example:** Sam, John, and Jenny are checking accountholders at your institution. Sam withdrew $100 in cash at one of your institution's ATMs located in New York. John withdrew $150 in cash at another institution's ATM located in Chicago. Jenny withdrew $200 in cash at another institution's ATM located in Canada. In this example, you would report one withdrawal for $200.

4) Third-party fraudulent ATM cash withdrawals (your institution's accountholder, any ATM) = 4.a) + 4.b)

These are all ATM cash withdrawals that were not authorized by your institution's accountholders (third-party fraud).

Include:

- Any third-party, fraudulent ATM cash withdrawals, regardless of whether those funds were subsequently recovered (Debit, prepaid ATM cash withdrawals and credit card cash advances)

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 to make a one-time $200 ATM withdrawal. In this example, you would report one transaction for $200.

► **Example 2:** Your accountholder claimed that a perpetrator stole her debit card and used it to withdraw $100 from an ATM. However, an investigation by your institution determined the claim to be false, as the money was actually withdrawn by your accountholder. Since this transaction is an example of first-party fraud (false claim fraud), you would not include it in item **4)**.

4.a) Domestic ATM withdrawals (your institution's accountholder, any ATM in the U.S.)

These include all cash withdrawals from ATMs located in the U.S. (i.e., ATMs located in the 50 U.S. states, D.C., or U.S. territories), that were not authorized by your institution's accountholders (third-party fraud)

Include:

- Any third-party, fraudulent cash withdrawals from ATMs located in the U.S., regardless of whether those funds were subsequently recovered

Do not include:

- Any third-party, fraudulent cash from any ATM located outside the U.S.

► **Example:** Jen and Kate are accountholders at your institution. Both of their debit cards were stolen by perpetrators who watched them enter their PINs at the point-of-sale. Jen's perpetrator used her card and PIN to make a one-time $300 ATM withdrawal in Atlanta. Kate's perpetrator used her card and PIN to make a one-time $400 ATM withdrawal in Italy. In this example, you would report one transaction for $300.

4.b) Cross-border ATM withdrawals (your institution's accountholder, any ATM outside the U.S.)

These include all cash withdrawals from ATMs located outside the U.S., that were not authorized by your institution's accountholders (third-party fraud)

Include:

- Any third-party, fraudulent cash withdrawals from ATMs located outside the U.S., regardless of whether those funds were subsequently recovered

Do not include:

- Any third-party, fraudulent cash from any ATM located in the U.S.

► **Example:** Jen and Kate are accountholders at your institution. Both of their debit cards were stolen by perpetrators who watched them enter their PINs at the point-of-sale. Jen's perpetrator used her card and PIN to make a one-time $300 ATM withdrawal in Atlanta. Kate's perpetrator used her card and PIN to make a one-time $400 ATM withdrawal in Italy. In this example, you would report one transaction for $400.

5) Total cash deposited at your institution = 5.a) + 5.b) + 5.c) + 5.d)

These are the total cash deposits made into accounts at your institution. Include cash deposits that were made over the counter at your institution's bank branches, cash deposits at ATMs, cash deposits at wholesale vaults and RCMTs.

Include:

- Cash deposits into both deposit accounts as well as into prepaid card program accounts

Do not include:

- Noncash deposit transactions made to accounts at your institution
- Teller vault activity
- Withdrawal transactions
- Other non-deposit transactions (i.e., inquiries, statement print-outs, purchases of stamps, tickets)

5.a) Over-the-counter cash deposits

These are the cash deposits made at bank lobby teller window or drive-through teller.

Include:

- Over-the-counter cash deposits made at your institution's branch locations to accounts at your institution

Do not include:

- Cash deposits at ATM terminals located in your institution's branch locations
- Noncash deposit transactions made to accounts at your institution

► **Example:** Your accountholder deposited $600 in cash into his account over the counter through a teller at one of your institution's branch locations. In this example, you would report one deposit of $600.

5.b) Cash deposits at wholesale vaults

These are the cash deposits handled through armored couriers including vaults operated by your institution or outsourced to an armored courier or other third-party vault operator.

Include:

- Cash deposits made to accounts at your institution at wholesale vaults

Do not include:

- Noncash deposit transactions made to accounts at your institution
- Teller vault activity

► **Example:** 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 and to order $1,500 in various denominations of cash straps and coin rolls to make change available in its store(s). In this example, you would report one cash deposit for $5,000.

5.c) Cash deposits made at remote currency management terminals (RCMTs)

These are the cash deposits made at RCMTs at merchant customer locations (i.e., "smart safes" and "cash recyclers") that were deployed by your institution and resided at a client site (i.e., gas station, restaurant).

Include:

- All cash deposits made at RMCTs

Do not include:

- Cash withdrawals made at remote currency management terminals
- Transactions that involved armored couriers depositing cash from these terminals or replenishing cash in cash recyclers

► **Example:** 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 $700 from the same recycler. In this example, you would report one deposit for $500.

5.d) ATM cash deposits (your institution's accountholder, any ATM) = 5.d.1) + 5.d.2)

These are all cash deposits made to accounts at your institution at any ATM, including those at your institution's ATM terminals (item **5.d.1)** below) or "foreign" ATMs (item **5.d.2)** below). A "foreign" ATM is an ATM operated by an unaffiliated depository institution or ATM operator.

Include:

- Cash deposits made to your institution on any ATM

Do not include:

- Deposits made to accounts at another institution
- Withdrawal transactions
- Other non-deposit transactions (i.e., inquiries, statement print-outs, purchases of stamps, tickets)

► **Example:** On Monday your accountholder deposited $250 cash into his checking account via an ATM. On Tuesday he deposited $500 in checks at the same ATM. In this example, you would report one cash deposit for $250.

5.d.1) "On-us" ATM deposits (your institution's accountholder, your institution's ATM)

These are all cash deposits made to accounts at your institution at your institution's ATM terminals.

Include:

- Deposits made to accounts at your institution at fee-free ATM networks in which it participates

Do not include:

- Deposits by cardholders other than your institution's accountholders, deposits made to accounts at your institution at "foreign" ATMs, or non-deposit transactions made to accounts at your institution

► **Example:** On Monday your accountholder deposited $250 cash into his checking account via an ATM owned by your institution. On Tuesday he deposited $500 in checks at the same ATM. In this example, you would report one cash deposit for $250.

5.d.2) "Foreign" ATM deposits (your institution's accountholder, "foreign" ATM)

These are all cash deposits made to accounts at your institution at "foreign" ATMs.

Do not include:

- Any transactions at your institution's ATM terminals, regardless of who made them (whether they hold an account at your institution)
- Any non-deposit transactions made to accounts at your institution

► **Example:** Your institution has a reciprocal arrangement with a local bank to allow one another's accountholders to make deposits at any ATMs either institution owns. While the arrangement adds convenience for accountholders, it is not necessarily free, and any "foreign" ATM fees still apply. Your checking accountholder deposited $100 cash into an ATM owned by your institution on Monday and then deposited $250 into an ATM terminal owned by the other institution on Wednesday. In this example, you would report one deposit for $250.

Alternative Payment Initiation Methods

GENERAL TERMINOLOGY

Consumer account

An account for personal use by an individual or household from which payments can be made. For person-to-person transactions, these transactions would take place between two consumer accounts.

Business/government account

An account owned by an organization (i.e., business, government or not-for-profit organization) from which payments can be made. For person-to-person transactions, these transactions would take place between two business/government accounts.

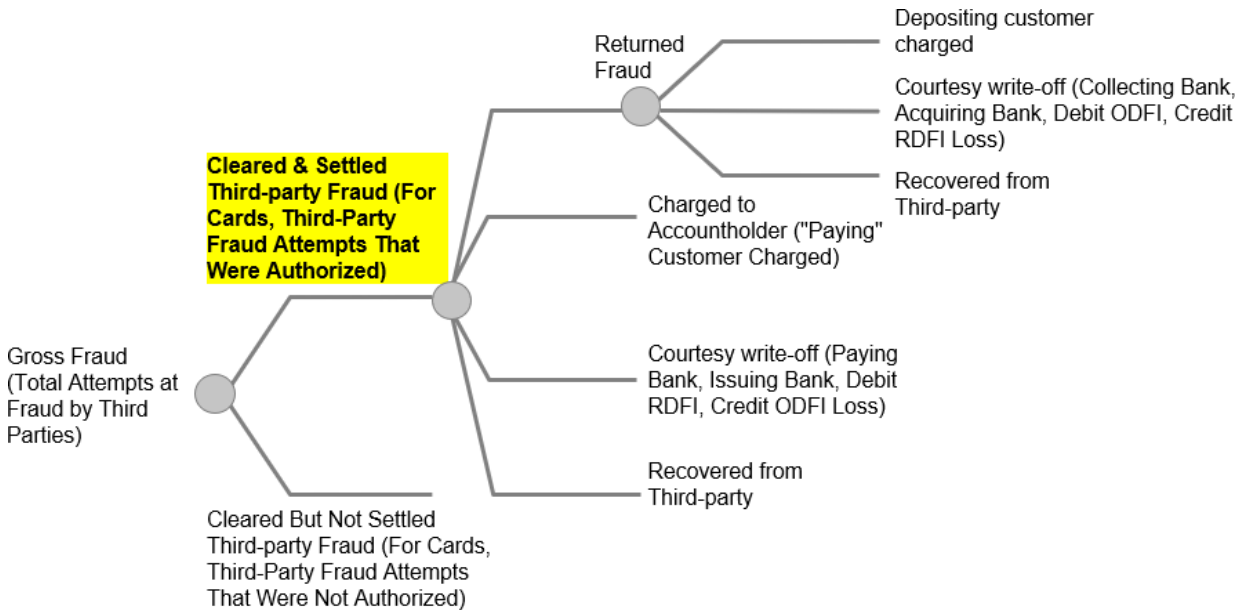
Note: Please report small business accounts under business/government accounts, if possible.

U.S. domiciled account

Accounts located within the 50 U.S. states, D.C., or U.S. territories such as Guam, Puerto Rico, or U.S. Virgin Islands). Only report data associated with your institution's U.S. domiciled accounts, including transactions that are domestic and cross-border.

Third-party fraud

The Federal Reserve Payments Study has identified a measure of fraud that can be described as cleared and settled third-party fraudulent transactions. This measure is not a loss-of-funds measure, nor is it a measure of fraud attempts; rather, it is a measure of the extent to which third parties who are not authorized to conduct transactions are able to penetrate the payment system and effect settlement between banks, or create a book transfer of funds if the transaction happens within one 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 manages to create a 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.



SURVEY ITEMS

1) Did your institution offer online or mobile consumer bill payments during calendar year 2018?

These include online and mobile bill payment transactions initiated through your institution's bill payment platform. If your answer to this question is **No**, please report "0" for item **2)** below.

Include:

- All online and mobile bill payment transactions paid from consumer accounts at your institution and initiated through a web browser (including a mobile browser), a mobile application, or an SMS/text message

Do not include:

- Payments made through a biller's website
- Person-to-person transfers (i.e., Zelle) reported in item **4)** below
- All online and mobile bill payment transactions paid from business/government accounts at your institution and initiated through a web browser (including a mobile browser), a mobile application, or an SMS/text message

► **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 initiating 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

These include online and mobile bill payment transactions initiated through your institution's bill payment platform. If your answer is **No** to item **1)** above, please report "0" here.

Include:

- All online and mobile bill payment transactions paid from consumer accounts at your institution and initiated through a web browser (including a mobile browser), a mobile application, or an SMS/text message

Do not include:

- Payments made through a biller's website
- Person-to-person transfers (i.e., Zelle) reported in item **4**) below
- All online and mobile bill payment transactions paid from business/government accounts at your institution and initiated through a web browser (including a mobile browser), a mobile application, or an SMS/text message

► **Example:** Your accountholder paid her $50 utility bill through her PC by initiating a payment from her account via your institution's website. In this example you would report one transaction for $50.

3) Did your institution offer an online or mobile person-to-person (P2P) funds transfer system during calendar year 2018?

These include all online, mobile, and SMS/text message funds transfer transactions from person to person (P2P). If your answer is **No**, please report "0" for item **4)** below.

Include:

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

Do not include:

- Business/government-to-person
- Transfers made from an external party's website such as Venmo or Popmoney
- Transfers from small business accounts to consumer accounts
- Online and mobile bill payment transactions initiated through your institution's bill payment platform
- Received P2P transfers from an accountholder at another institution

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

4) Total online or mobile person-to-person (P2P) transfer originations = 4.a) + 4.b)

These include all person-to-person transfers originated by your institution's consumer accountholders and initiated via your institution's website, mobile application, or an SMS/text message to another consumer account. If your answer is **No** to item **3)** above, please report "0" here.

Include:

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

Do not include:

- Business/government-to-person
- Transfers made from an external party's website such as Venmo or Popmoney
- Transfers from small business accounts to consumer accounts
- Online and mobile bill payment transactions initiated through your institution's bill payment platform
- Received P2P transfers from an accountholder at another institution

► **Example:** Your accountholder, Jenny, initiated a $200 payment from her account to another person's account at another institution through your institution's mobile application on her tablet by entering the recipient's phone number or e-mail address. Jenny then initiated another payment for $50 from her account to another person's account at your institution through your institution's mobile application. In this example, you would report two transactions for $250.

4.a) "On-us" transfer originations

These include all P2P transactions between two accountholders at your institution.

Include:

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

Do not include:

- P2P transfers where the recipient is an accountholder at another institution
- Business/government-to-person
- Transfers from small business accounts to consumer accounts
- Online and mobile bill payment transactions initiated through your institution's bill payment platform

► **Example:** Your accountholder paid his friend, also an accountholder at your institution, $50 using Zelle on your institution's mobile application. In this example, you would report one transaction for $50.

4.b) "Off-us" transfer originations

These include all P2P transfers originated by your institution's consumer accountholders for which the receiver is an accountholder at another institution.

Include:

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

Do not include:

- P2P transfers where the recipient is an accountholder at your institution
- Received P2P transfers from an accountholder at another institution
- Business/government-to-person
- Transfers from small business accounts to consumer accounts
- Online and mobile bill payment transactions initiated through your institution's bill payment platform

► **Example 1:** Your customer paid $100 using Popmoney offered through your institution's website to her brother, an accountholder at another institution. In this example, you would report one transaction for $100.

► **Example 2:** Your customer received a P2P transfer for $55 via Zelle from her father, an accountholder at another institution. Since this P2P transfer was not initiated by your customer, you would not include this transaction in item **4)** or **4.b)**.

5) Third-party fraudulent online or mobile person-to-person (P2P) transfer originations = 5.a) + 5.b)

These include all fraudulent person-to-person transfers originated from your institution's consumer account and initiated via your institution's website, mobile application, or an SMS/text message to another consumer account. If your answer is **No** to item **3)** above, please report "0" here.

Include:

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

Do not include:

- Fraudulent business/government-to-person
- Fraudulent transfers made from an external party's website such as Venmo or Popmoney
- Fraudulent transfers from small business accounts to consumer accounts
- Any fraudulent bill payment transactions initiated through your institution's bill payment platform
- Fraudulent received P2P transfers from an accountholder at another institution

► **Example:** John is an accountholder at your institution. His account was hacked. The perpetrator used Zelle through your institution's mobile application and paid his own account, also at your institution $100. He then initiated a second payment of $200 from John's account to pay another person's account at another institution using Zelle as before. In this example you would report two transactions for $300.

5.a) "On-us" transfer originations

These include all fraudulent P2P transactions between two accountholders at your institution.

Include:

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

Do not include:

- Fraudulent P2P transfers where the recipient is an accountholder at another institution
- Fraudulent business/government-to-person
- Fraudulent transfers from small business accounts to consumer accounts

► **Example:** Your customer's account at your institution was hacked. The fraudster paid his own account, also at your institution, $100 using your institution's mobile application. In this example, you would report one transaction for $100.

5.b) "Off-us" transfer originations

These include all fraudulent P2P transfers originated by your institution's consumer accounts for which the receiver is an accountholder at another institution.

Include:

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

Do not include:

- Fraudulent P2P transfers where the recipient is an accountholder at your institution
- Fraudulent business/government-to-person
- Fraudulent transfers from small business accounts to consumer accounts
- Fraudulent received P2P transfers from an accountholder at another institution

► **Example:** Your customer's account at your institution was hacked. The fraudster paid $100 using Popmoney from your institution's website to his account at another institution. In this example, you would report one transaction for $100.