The Federal Reserve Payments Study

Survey Period: Calendar Year 2017

The *Depository and Financial Institutions Payments Survey* (DFIPS) includes:

- Institution affiliates
- Institution profile
- Check payments, deposits, and returns
- ACH profile, originations, and receipts
- Wire transfers originated
- General-purpose debit and prepaid cards
- General-purpose credit cards
- Cash withdrawals
- Alternative payments

---- Glossary with Examples ----

Glossary with Examples

Institution Profile

GENERAL TERMINOLOGY

Your institution

The participating depository institution at its highest organizational level (e.g., 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 (i.e., 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.

.

SURVEY ITEMS

1) Transaction deposit accounts (including demand deposit accounts)

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
- Wholesale sweep program accounts

► 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 2017.

➲ Transaction deposit accounts (including demand deposit accounts) = Consumer deposit accounts (item **1.a**) + Business/government deposit accounts (item **1.b**).

1.a) Consumer accounts

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

1.b) Business/government accounts

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

Check Payments

GENERAL TERMINOLOGY

Check (or share draft)

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

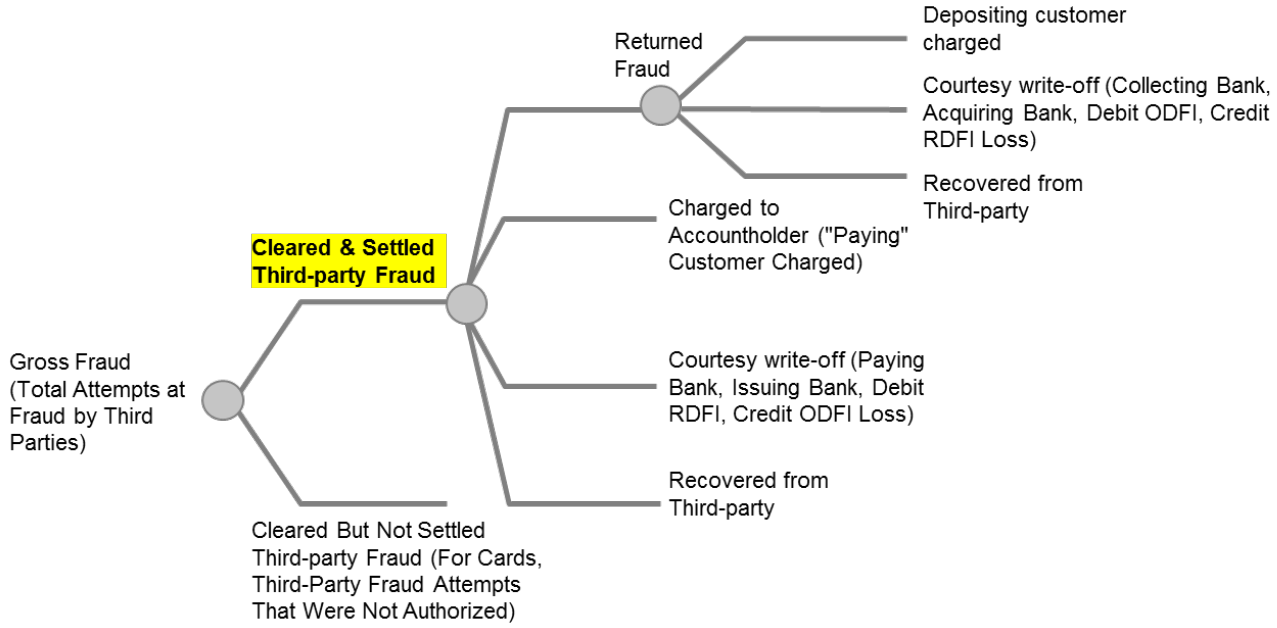
The first depository institution in which a check is deposited. The "bank of first deposit" may be a bank or credit union and may not be your institution.

"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."

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 2017?

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 2017, please answer **Yes**.

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 2017, please also request the necessary data from your institution's payments processor and combine it with check totals that were processed by your institution.

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 include these volumes in your answers below?

If possible, please report your institution's check volume processed by another organization. If your institution cannot report these volumes, please explain the reason why in the comments section of the survey instrument.

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 tickets).

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?

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 2017?

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.
If your answer is **Yes**, please report these volumes in **5.a**.

► 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 scenario, Bank B is a correspondent processor and would answer **Yes** to this question.

5) All checks drawn on your institution

These are all checks (or share drafts) for which your institution was the paying bank as defined by Reg. CC. Include items **5.a** and **5.b** below.

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

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**.

► 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 item **5** and **5.b**.

➲ All checks drawn on your institution = Checks drawn on your institution for which another institution was the "bank of first deposit" (item **5.a**) + "On-us" checks for which your institution was the "bank of first deposit" (item **5.b**).

5.a) All checks drawn on your institution for which another institution was the "bank of first deposit"

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

Include:

- Inclearings and "on-us" 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)

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

► 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.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."

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 (e.g., 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** above

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

► 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) Outgoing and "on-us" returned checks

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.

7) Third-party fraudulent checks drawn at 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.

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 ▪ On-us entries ▪ Network entries ▪ Returns (only for item 11)	▪ 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.

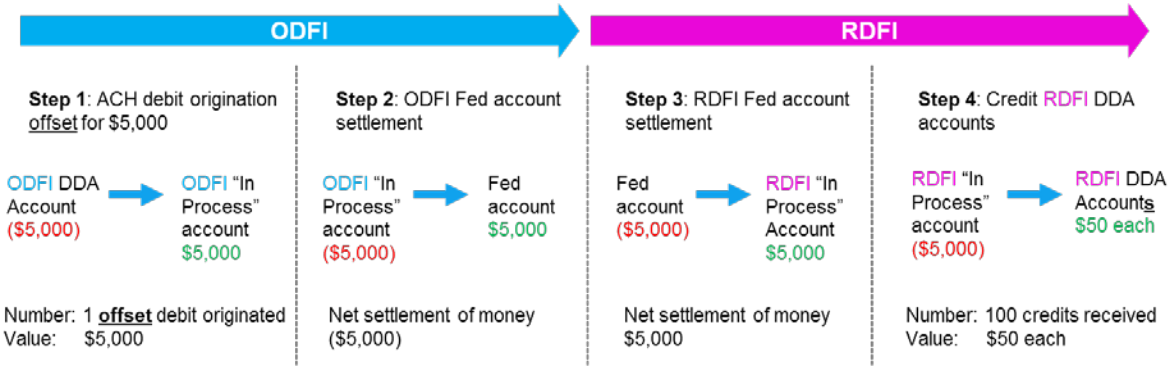
Offset ACH entry

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 can be likened 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 banks 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

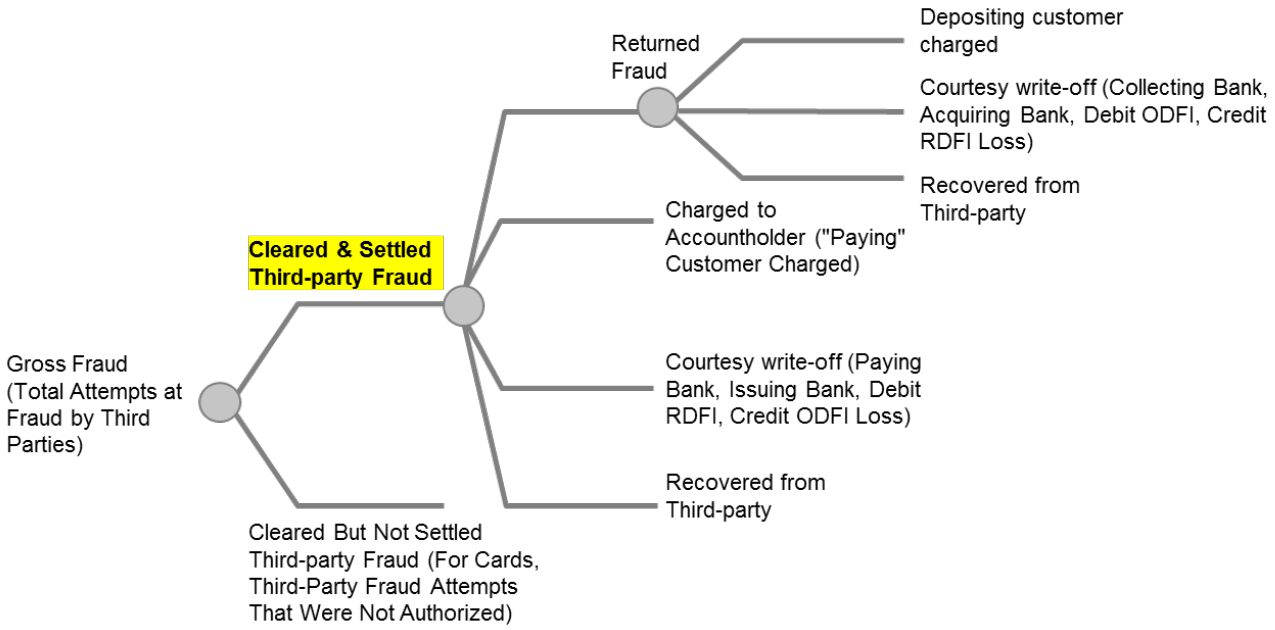
Files that do not have an offsetting entry that automatically credits or debits the customer's DDA account for the debit and/or credit originated. After receiving the file from the accountholder, the ODFI will then originate the offset entries to balance the file. Most institutions prefer to receive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

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. It 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 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 2017?

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 2017?

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 below.

3) Did your institution originate forward ACH debits (not including returns or offset entries) during calendar year 2017?

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.

Note: If your answer is **No**, please report "0" for item **9.b** below.

4) Did your institution originate offset ACH debit or credit entries during calendar year 2017?

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.

Note: If your answer is **No**, please skip items **4.a, 4.b, 4.b.1, 4.c, and 4.c.1** 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, please exclude offset volumes from your answers below. Please indicate if you are able to exclude offset ACH volumes below.

Even if you are not able to exclude all offset volumes, please report the number and value of your institution's forward ACH entries for items **6** and its subsets, **7** and its subsets, **9** and its subsets, and **10** and its subsets. Please provide instructions in the comments section to the right of the question indicating where your institution reported its offsets (e.g., network credits originated, in-house on-us credits originated).

4.b) If your answer is "Yes" to item 4 above, how many balanced files did your institution process from business/government accountholders during calendar year 2017?

Please provide the number of balanced files received from your accountholders during calendar year 2017.

Note: If you can provide a numeric answer to item **4.b**, please skip item **4.b.1** below.

4.b.1) If you are unable to answer item 4.b above, please provide an estimate of the percentage of the total settlement files that ACH balanced files constituted during calendar year 2017.

If your institution is unable to provide the number of balanced files received during calendar year 2017, please provide an estimate of the percentage of balanced files received from the total number of settlement files processed (balanced and unbalanced).

4.c) If your answer is "Yes" to item 4 above, how many unbalanced files did your institution process from business/government accountholders during calendar year 2017?

Please provide the number of unbalanced files received from your accountholders during calendar year 2017.

Note: If you can provide a numeric answer to item **4.c**, please skip item **4.c.1** below.

4.c.1) If you are unable to answer item 4.c above, please provide an estimate of the percentage of the total settlement files that ACH unbalanced files constituted (estimate) during calendar year 2017.

If your institution is unable to provide the number of unbalanced files received during calendar year 2017, please provide an estimate of the percentage of unbalanced files received from the total number of settlement files processed (balanced and unbalanced).

5) Did your institution offer same-day settlement of ACH credit originations during calendar year 2017?

The effective date for network same-day settlement of credits was September 23, 2016.

Note: If your answer is **No**, please report "0" for items **7.a** and **8.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)

These are all network 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
- 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.

➲ ACH credits your institution originated = Network ACH credit entries originated (item **6.a**) + In-house, on-us ACH credit entries originated (item **6.b**) + Direct exchange ACH credit entries originated (item **6.c**)

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.

Do not include:
- Returns
- ACH entries cleared directly between your institution and another (i.e., direct exchange ACH entries)

Note: If your answer is **No** to item **2** above, please report "0" ACH credit entries originated by your institution here.

► 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.

Note: If your answer is **No** to item **2** above, please report "0" ACH credit entries originated by your institution here.

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 10 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 you are 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 corporate customer paid 100 of its employees $750 each electronically through the ACH. Your institution originated the credit entries on behalf of your customer. Five of those employees bank at institutions with which you have established direct exchange relationships in order to avoid clearing fees from the Federal Reserve or EPN. You originated payment via direct exchange to the five employees who bank at these institutions. In this example, you would report five transactions for $3,750.

7) Total forward ACH credits your institution originated (ODFI credits)

Repeat item **6** above. These are all network 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.

➲ ACH credits your institution originated = ACH credit entries originated same-day settlement (item **7.a**) + ACH credit entries originated non-same-day settlement (item **7.b**)

7.a) ACH credit entries originated for 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.

Note: If your answer is **No** to item **5** above, please report "0" here.

► 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.

7.b) ACH credit entries originated for 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 settlement file was transmitted.

► 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 50 transactions for $120,000.

8) Third-party fraudulent forward ACH credit entries your institution originated

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.

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 entries

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
- 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 10 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 **8**.

➲ Third-party fraudulent forward ACH credit entries your institution originated = Third-party fraudulent forward ACH credit entries your institution originated for same-day settlement (item **8.a**) + Third-party fraudulent forward ACH credit entries your institution originated for non-same-day settlement (item **8.b**)

8.a) Third-party fraudulent forward ACH credit entries your institution originated for 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 settlement file was sent. Please report any third-party ACH transactions, regardless of whether or not your accountholder recovered the funds.

Note: If your answer is **No** to item **5** above, please report "0" ACH credit entries your institution originated here.

Do not include:

- ACH fraud prevented before all funds were made available to the RDFI
- Fraudulent ACH credit entries received by your institution
- Fraudulent ACH credit entries 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 **8.a**.

8.b) Third-party fraudulent forward ACH credit entries your institution originated for 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 settlement file was sent. Please report any third-party ACH transactions, regardless of whether or not your accountholder recovered the funds.

Do not include:

- ACH fraud prevented before all funds were made available to the RDFI
- Fraudulent ACH credit entries received by your institution
- Fraudulent ACH credit entries 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 **8.b**.

ACH Receipts and Outgoing Returns

9) Total forward ACH debit entries your institution received (RDFI debits)

These include all ACH debit entries for which your institution was the RDFI.

Include:

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

Do not include:

- Returns
- In-house on-us offset ACH debit entries received
- Network on-us offset ACH debit entries received
- ACH entries sent to 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 12 transactions for $900.

➲ ACH debits your institution received = Network ACH debit entries received (item **9.a**) + In-house on-us ACH debit entries received (item **9.b**) + Direct exchange ACH debit entries received (item **9.c**)

9.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 12 transactions for $600.

9.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.

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.
- ACH entries sent to or received from other institutions
- 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 240 transactions for $10,800.

9.c) Direct exchange ACH debit entries received

These include all ACH credit 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 credit 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 120 transactions for $3,600.

10) Total forward ACH debit entries your institution received

Repeat item **9** above. These are all ACH debit entries for which your institution was the RDFI.

Include:

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

Do not include:

- Returns
- In-house on-us offset ACH debit entries received
- ACH entries sent to 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 12 transactions for $900.

➲ ACH debits your institution received = ACH debit entries received same-day settlement (item **10.a**) + ACH debit entries received non-same-day settlement (item **10.b**)

10.a) ACH debit entries received for 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.

► 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.

10.b) ACH debit entries received for 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.

► 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 12 transactions for $600.

11) Total 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 that 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 (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.

12) Total third-party fraudulent forward ACH debit entries your institution received

These include only 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. Please report 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
- 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 from 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 settled as usual, 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 **12**.

12.a) Third-party fraudulent ACH debit entries your institution received for 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.

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
- Fraudulent ACH credit entries

► Example: A fraudster opened a commercial bank account for a fictitious gardening company at another institution and originated an unauthorized bill payment from 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, was debited from your accountholder, and was made available to the fraudster's account. In this example, you would report one transaction for $1,000.

12.b) Third-party fraudulent ACH debit entries your institution received for 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.

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
- 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 from 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. 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.

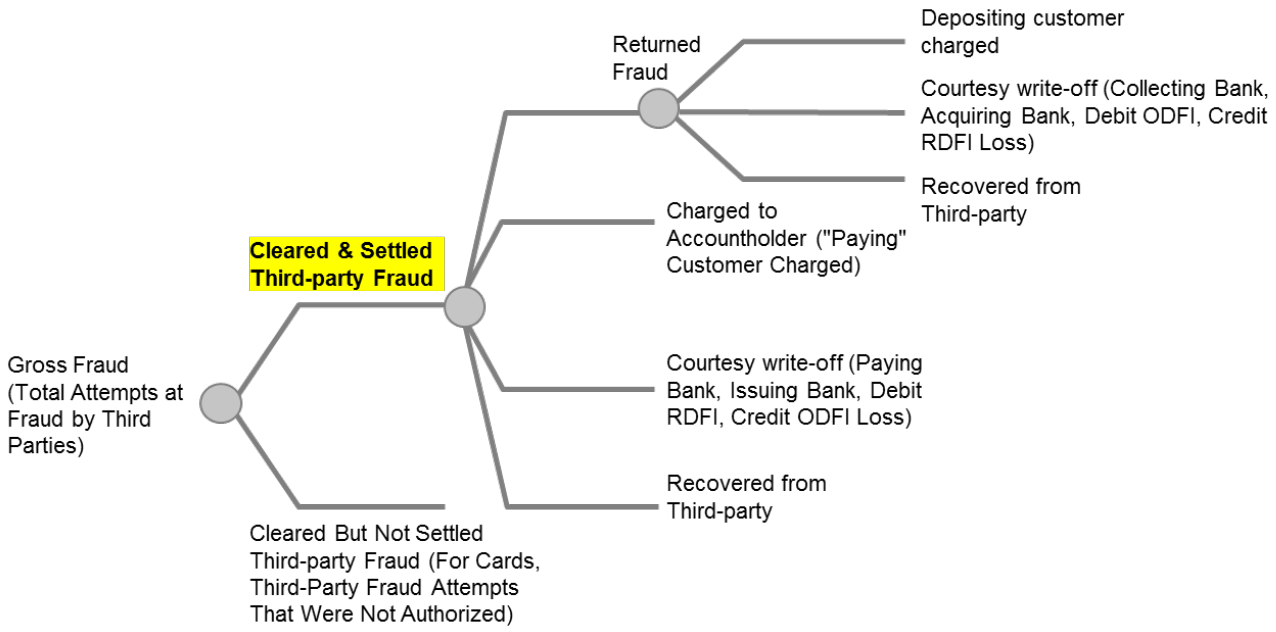
► Example 2: Jim is an accountholder at your institution. He lost his job and has not been able to find employment in the last six months. His cellphone provider originated an ACH debit transaction for his monthly bill of $150. The transaction settled a few days later as usual, but Jim claimed the transaction 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 **12.b**.

Wire Transfers Originated (Outgoing)

GENERAL TERMINOLOGY

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 2017 (i.e., correspondent volume)?

Note: 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 to the right of the question.

2) Did an unaffiliated depository institution originate wires on behalf of your institution during calendar year 2017?

Note: 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 to the right of the question.

3) Total wire transfer originations (outgoing)

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.

➲ Wire transfer originations = Wires sent through a network or a correspondent bank (item **3.a**) + Book transfers (item **3.b**).

3.a) Sent through a network (e.g., Fedwire or CHIPS) or a correspondent bank

Include:

- All wire transfers sent through a network (e.g., 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. In this example, you would report one transaction for $10,000.

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

Include:

- All internal wire transfers that were made using your wire platform (these are sometimes referred to as book transfers)

Do not include:

- Wires that are sent through a network (e.g., 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.

4) Third-party fraudulent wire transfers your institution originated

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)
- Fraudulent wire transfer originations where funds were recovered

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 a second institution, both of which accounts were maintained under a false name The transactions were 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 **4**.

➲ Third-party fraudulent wire transfers your institution originated = Fraudulent wires sent through a network or a correspondent bank (item **4.a**) + Fraudulent book transfers (item **4.b**).

4.a) Sent through a network (e.g., Fedwire or CHIPS) or a correspondent bank

Include:

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

Do not include:

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

► Example 1: Michael 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, 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 $5,000.

► Example 2: Laura, a small business accountholder at your institution, originated a wire payment for $60,000 through your online portal to her paper supplier, who banks at a different institution. Laura's paper supplier was delayed and delivered the product four weeks late. Laura lost many of her customers because of this delay. In order to recoup some of her losses, Laura opened a fraudulent claim with your institution, stating that her supplier did not deliver the product at all. 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 **4.a**.

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

Include:

- Fraudulent internal wire transfers that were made using your wire platform (these are sometimes referred to as book transfers)

Do not include:

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

► Example 1: 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 Carlos's username, password, and bank account information were stolen online. The perpetrator originated three wire transfers from Carlos's account for $7,000 each to three separate accounts. All three transfers cleared and settled. One of the receiving accounts belonged to an accountholder at your institution, and the money was transferred through your internal wire transfer platform. In this example, you would report one transaction for $7,000 in item **4.b.** (The other two transactions for $14,000 should be reported in item **4.a.**)

Debit Cards

GENERAL TERMINOLOGY

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, 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:

Debit card transactions include…	Debit card transactions do not 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 ▪ Transfers by a corporate customer to fund its employees' payroll card accounts ▪ Electronic Benefit Transfer (EBT) card transactions ▪ Payroll card transactions by the cardholder

Digital Wallet

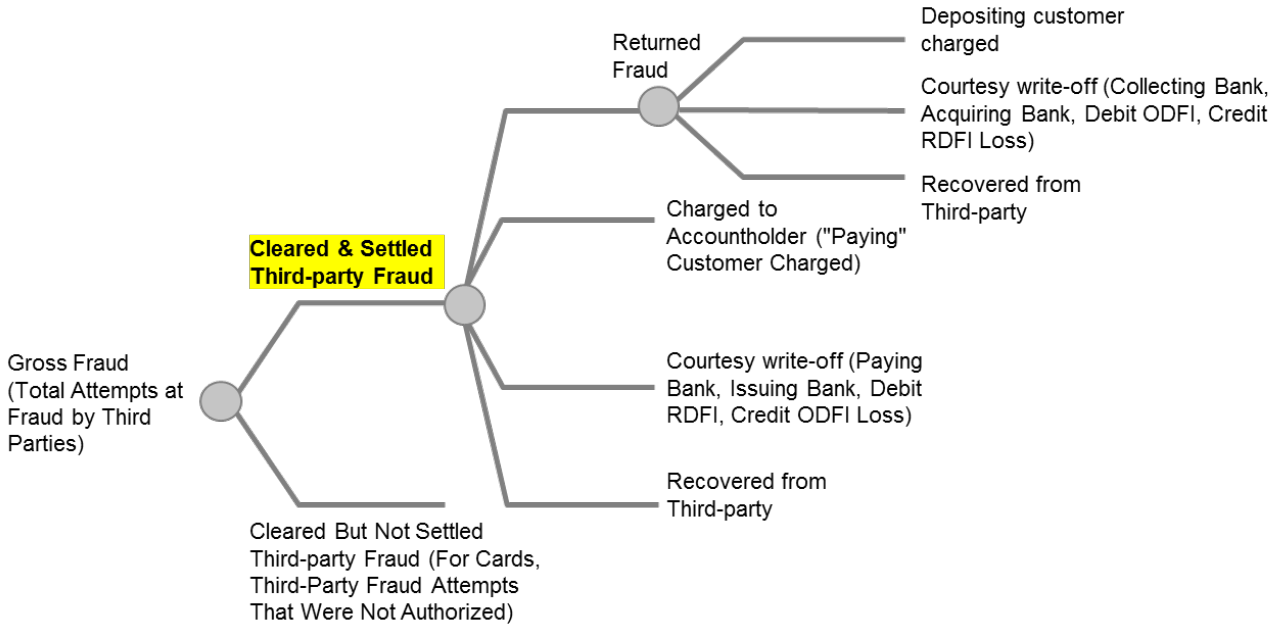
All purchase and bill-pay transactions made using a digital wallet in which users can complete purchases quickly and easily using near-field communication (NFC) that works in conjunction with mobile payment systems. Digital wallets can be used during In-person transactions or Remote transactions. In-person 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.

Contactless Card

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").

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 general-purpose debit cards in circulation in 2017 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.

Include:

- 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

Note: If your answer to this question is **No**, please report "0" for items **2** and its subsets**, 3** and its subsets, and **9.a** below.

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

Do not include general-purpose prepaid card, payroll card, or gift card transactions in this section of the questionnaire. If your answer is **No**, please report NR for any questions in which your institution can only report combined debit and prepaid transactions combined.

If your answer is **Yes, in some cases**, please explain in the comments box to the right of the question.

2) Total general-purpose debit card transactions

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.

Include:

- Both consumer and business/government card transactions
- Cash back at the point of sale

Do not include:

- 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 a Visa gift 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.

➲ Total general-purpose debit card transactions = Transactions from consumer accounts (item **2.a**) + Transactions from business/government accounts (item **2.b**).

2.a) Transactions from consumer accounts

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

Do not include:

- Debit card transactions made by business/government accountholders
- Prepaid card transactions made by business/government accountholders

► 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.

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

Do not include:

- Debit card transactions made by consumer accountholders
- Prepaid card transactions made by consumer accountholders

► 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.

3) Total general-purpose debit card transactions

Repeat item **2** 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.

Include:

- Both person-present and remote government card transactions
- Cash back at the point of sale

Do not include:

- 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 jacket at a department store. In this example, you would report two transactions for $120.

➲ Total general-purpose debit card transactions = In-person transactions (item **3.a**) + Remote transactions (item **3.b**).

3.a) In-person transactions

These include all general-purpose debit 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 for digital wallet authentication (item **3.a.1**), contactless card authentication (item **3.a.2**), EMV chip card authentication (item **3.a.3**), magnetic stripe authentication (item **3.a.4**), and all other authentication methods, including keyed-in transactions, manual imprint, etc. (item **3.a.5**).

If the transaction is authorized via PIN, please report this volume under EMV chip card authentication (item **3.a.3**) if the card has a chip, or under magnetic stripe authentication (item **3.a.4**) if the card doesn't have a chip.

Include:

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

Do not include:

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

► Example 1: 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. For this example, you would report one transaction for $15 in item **3.a** and **3.a.1**.

► Example 2: Your customer bought a new pair of jeans for $39 with his debit card by "tapping" his contactless card on the POS terminal using RFID technology. In this example, you would report one transaction for $39 in item **3.a** and **3.a.2**.

3.b) Remote transactions

These include all general-purpose 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 for digital wallet authentication (item **3.b.1**), manually entered online authentication (item **3.b.2**), and all other authentication methods, including phone orders, mail orders, etc. (item **3.b.3**).

Include:

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

Do not include:

- Person-present transactions

► 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 proceeded to buy a $65 pair of shoes in a mobile application not at the point of sale, paying with the same debit card with his digital wallet (Android Pay). In this example, you would report two transactions for $565 in item **3.b**, one transaction for $65 in item **3.b.1,** and one transaction for $500 in item **3.b.2**.

4) Total general-purpose debit card transactions

Repeat item **2** 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.

Include:

- Both digital wallet and non-digital wallet debit card transactions
- Cash back at the point of sale

Do not include:

- 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 to purchase a $70 jacket online. In this example, you would report two transactions for $120.

➲ Total general-purpose debit card transactions = Digital wallet (mobile) transactions (item **4.a**) + Non-digital wallet transactions (item **4.b**).

4.a) Digital wallet (mobile) transactions

These include all general-purpose debit card transactions made via a digital wallet (e.g., Apple Pay, Android Pay, Samsung Pay, PayPal Mobile). These can include online purchases using a computer, in-store purchases using a smartphone, and mobile in-app transactions.

Include:

- Digital wallet NFC (near-field communication) transactions, MST (magnetic secure transmission) transactions, QR code transactions, or barcode transactions
- Digital wallet in-app or browser transactions

Do not include:

- Transactions made with a debit card and not via a digital wallet
- Contactless debit card transactions (e.g., "tap and pay" with a debit card)

► 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.

4.b) Non-digital wallet transactions

These include all general-purpose debit card transactions not made via a digital wallet. Include both remote and in-person transactions not made via a digital wallet.

Include:

- Transactions made with a debit card and not via a digital wallet
- Contactless debit card transactions (e.g., "tap and pay" with a debit card)

Do not include:

- All debit card transactions made via a digital wallet (e.g., Apple Pay, Android Pay, Samsung Pay, PayPal Mobile, etc.)
- ATM withdrawals

► 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 with his digital wallet (Android Pay). In this example, you would report one transaction for $500.

5) Total general-purpose debit card transactions

Repeat item **2** 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.

Include:

- Both consumer and business/government card transactions
- Cash back at the point of sale

Do not include:

- ATM withdrawals
- Prepaid card transactions
- Credit card transactions

► Example: Your customer bought $50 worth 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 jacket at a department store. In this example, you would report two transactions for $120.

➲ Total general-purpose debit card transactions = General-purpose debit card PIN-authenticated transactions (item **5.a**) + General-purpose debit card zip-code-authenticated transactions (item **5.b**) + General-purpose debit card CID-authenticated transactions (item **5.c**) + General-purpose debit card other-authenticated transactions (item **5.d**).

5.a) PIN authentication

These include all debit card transactions for which your institution was the card issuer and in which funds were debited from a regular transaction deposit account by using PIN authentication.

Include:

- All general-purpose debit card transactions that were processed over a PIN (single-message) payment card network

Do not include:

- ATM withdrawals
- Credit card transactions

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

► Example: Your checking accountholder has a debit card linked to the account. She bought $50 of groceries with her debit card by entering her PIN at the checkout line. Later that day, she used her debit card with her PIN to purchase $100 of clothes at a department store. In this example, you would report two transactions for $150.

5.b) Zip-code authentication

These include all debit card transactions for which your institution was the card issuer and in which funds were debited from a regular transaction deposit account by using zip-code authentication.

Include:

- All general-purpose debit card transactions that were authorized using a zip code

Do not include:

- ATM withdrawals
- Credit card transactions

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

► Example: Your accountholder bought $65 of gas at a pump that required zip-code authentication for debit card transactions. In this example, you would report one transaction for $65.

5.c) Card Identification Number (CID) authentication

These include all debit card transactions for which your institution was the card issuer and in which funds were debited from a regular transaction deposit account by using a card identification number (CID).

Include:

- All general-purpose debit card transactions that were authorized using a CVV or CVV2 (Card Verification Value Code), CSC (Card Security Code), CVC or CVC2 (Card Verification Code), or CID (Card Identification Number).

Do not include:

- ATM withdrawals
- Credit card transactions

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

► Example: Your accountholder bought a $100 pair of shoes on a department store's website using a debit card issued by your institution. The website prompts your customer to submit their card identification number to verify the authenticity of the transaction. In this example, you would report one transaction for $100.

5.d) Other authentication

These include all debit card transactions for which your institution was the card issuer, in which funds were debited from a regular transaction deposit account and the transaction was not authorized via PIN, zip-code, or CID (**5.a, 5.b,** or **5.c**).

Include:

All general-purpose debit card transactions not authorized via PIN, zip code, or CID

Do not include:

- ATM withdrawals
- Credit card transactions

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

► Example: Your accountholder spent $5 at a convenience store using a network-branded debit card issued by your institution. The store did not require any additional identification due to the small purchase amount. In this example, you would report one transaction for $5.

6) Total general-purpose debit card cash-back 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. 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.

Do not include:

- ATM withdrawals
- Credit card transactions
- 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.

7) Third-party fraudulent general-purpose debit card transactions

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.

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

► Example: Your accountholder's debit card issued by your institution was stolen. The perpetrator used the card to make one purchase worth $1,000. 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 **7**.

➲ Third-party fraudulent general-purpose debit card transactions = Person-present transactions (item **7.a**) + Remote transactions (item **7.b**).

7.a) In-person transactions

These include only third-party fraudulent debit card transactions for which the card user was physically present with the card at the point of sale, including POS transactions, NFC transactions, MST transactions, manually entered transactions, QR code transactions, or barcode transactions. Include all third-party unauthorized debit card transactions, before any recoveries or chargebacks. 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 for digital wallet authentication (item **7.a.1**), contactless card authentication (item **7.a.2**), EMV chip card authentication (item **7.a.3**), magnetic stripe authentication (item **7.a.4),** and all other authentication methods, including keyed-in transactions, manual imprint, etc. (item **7.a.5**).

If the fraudulent transaction is authorized via PIN, please report this volume under EMV chip card authentication (item **7.a.3**) if the card has a chip, or under magnetic stripe authentication (item **7.a.4**) if the card doesn't have a chip.

Include:

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

Do not include:

- Fraudulent remote transactions
- Fraudulent digital wallet in-app or browser transactions

► Example 1: Your accountholder's debit 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 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 **7.a**.

7.b) Remote transactions

These include only third-party fraudulent debit card transactions in which the card user did not physically present the card to authorize the transaction. Include all third-party unauthorized debit card transactions, before any recoveries or chargebacks. 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 for digital wallet authentication (item **7.b.1**), manually entered online authentication (item **7.b.2**), and all other authentication methods, including phone orders, mail orders, etc. (item **7.b.3**).

Include:

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

Do not include:

- Fraudulent person-present transactions

► 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. 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 **7.b**.

8) Third-party fraudulent general-purpose debit card transactions

Repeat item **7** from above. 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.

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 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. In this example, you would report one transaction for $1000.

► **Example 2:** Your accountholder claimed 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 **8**.

➲ Third-party fraudulent general-purpose debit card transactions = Digital wallet (mobile) transactions (item **8.a**) + Non-digital wallet transactions (item **8.b**).

8.a) Digital wallet transactions

These include only third-party fraudulent debit card transactions made via a digital wallet (e.g., Apple Pay, Android Pay, Samsung Pay, PayPal Mobile). These can include online purchases using a computer, in-store purchases using a smartphone (NFC, MST, QR code, and barcode transactions), and mobile in-app purchases. Include all third-party unauthorized debit card transactions, before any recoveries or chargebacks. Please report any fraudulent third-party debit card transactions, regardless of whether the transaction resulted in a loss of funds.

Include:

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

Do not include:

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

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

► Example 2: Your accountholder claimed that his smartphone was stolen and used to make a $400 in-app purchase with the digital wallet installed in the smartphone, charging the purchase to his debit card. 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 8**.a**.

8.b) Non-digital wallet transactions

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

Include:

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

Do not include:

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

► Example 1: Your accountholder's wallet was stolen while commuting to work. Later that day, the perpetrator made an internet purchase for $325 using your accountholder's debit card. He then used the stolen card to buy lunch for $25. In this example, you would report two transactions for $350.

► 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 **8.b**.

9) Third-party fraudulent general-purpose debit card transactions

Repeat item 8 from above. 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.

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 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. In this example, you would report one transaction for $1000.

► **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 **9**.

➲ Third-party fraudulent general-purpose debit card transactions = Digital wallet (mobile) transactions (item **9.a**) + Non-digital wallet transactions (item **9.b**).

9.a) PIN authentication

These include only third-party fraudulent debit card transactions for which your institution was the card issuer and in which funds were debited from a regular transaction deposit account using PIN authentication.

Include:

- Third-party fraudulent general-purpose debit card transactions that were processed over a PIN (single-message) payment card network

Do not include:
- ATM withdrawals
- Prepaid card transactions
- Credit card transactions

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

► Example: Your accountholder's wallet was stolen while commuting to work, and the perpetrator was able to discover the PIN. Later that day, the perpetrator bought a $600 cellphone authorized via PIN using your accountholder's debit card. In this example, you would report one transaction for $600.

9.b) Zip-code authentication

These include only third-party fraudulent debit card transactions for which your institution was the card issuer and in which funds were debited from a regular transaction deposit account by using zip-code authentication.

Include:

- Third-party fraudulent general-purpose debit card transactions that were processed using zip-code authentication through a payment card network

Do not include:
- ATM withdrawals
- Debit card transactions from regular transaction deposit accounts
- Credit card transactions

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

► Example: The perpetrator of a stolen card was able to guess the zip code based on the identification in your customer's wallet. The perpetrator bought gas for $65 at a pump that required zip-code authentication for debit card transactions. In this example, you would report one fraudulent transaction for $65.

9.c) Card Identification Number (CID) authentication

These include only third-party fraudulent debit card transactions for which your institution was the card issuer and in which funds were debited from a regular transaction deposit account by using a card identification number.

Include:

- Third-party fraudulent general-purpose debit card transactions that were authorized using a CVV or CVV2 (Card Verification Value Code), CSC (Card Security Code), CVC or CVC2 (Card Verification Code), or CID (Card Identification Number).

Do not include:
- ATM withdrawals
- Debit card transactions from regular transaction deposit accounts
- Credit card transactions

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

► Example: A perpetrator bought a $100 pair of shoes on a department store's website using a stolen debit card issued by your institution. The website prompted your customer to submit his card identification number (CID) to verify the authenticity of the transaction. In this example, you would report one transaction for $100.

9.d) Other authentication

These include all debit card transactions for which your institution was the card issuer, in which funds were debited from a regular transaction deposit account, and the transaction was not authorized via PIN, zip-code, or CID (**9.a, 9.b, or 9.c**).

Include:

- All general-purpose debit card transactions not authorized via PIN, zip code, or CID

Do not include:

- ATM withdrawals
- Debit card transactions from regular transaction deposit accounts
- Credit card transactions

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

► Example: Your accountholder lost his debit card at a restaurant. A perpetrator found the debit card and spent $5 at a convenience store using your customer's debit card. The store did not require any additional identification due to the small purchase amount. In this example, you would report one transaction for $5.

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 (e.g., 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 not 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 ▪ Transactions originated in other countries	▪ ATM withdrawals ▪ Debit card transactions ▪ Credit card transactions ▪ Transfers by a corporate customer to fund its employees' payroll card accounts ▪ Electronic Benefit Transfer (EBT) card transactions

Digital Wallet

All purchase and bill-pay transactions made using a digital wallet in which users can complete purchases quickly and easily using near-field communication (NFC) that works in conjunction with mobile payment systems. 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.

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.

Gift cards

Private-label (e.g., merchant- or shopping center-branded) prepaid cards marketed as gift-giving alternatives to cash, checks, and gift certificates or as loyalty cards with payment capabilities.

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.

Note: Closed-loop applications provide access to wages via ATM or check-cashing agencies.

Electronic Benefit 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.

Closed-loop prepaid cards

Include:

- All point-of-sale or bill-pay transactions made with closed-loop (private-label) prepaid cards

Do Not Include:

- Open-loop (network-branded) prepaid card, debit card, or credit card transactions

- ATM withdrawals from transaction reporting unless specifically requested

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

Open-loop prepaid cards

Include:

- All point-of-sale or bill-pay transactions made with an open-loop (network-branded) prepaid card. (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.)

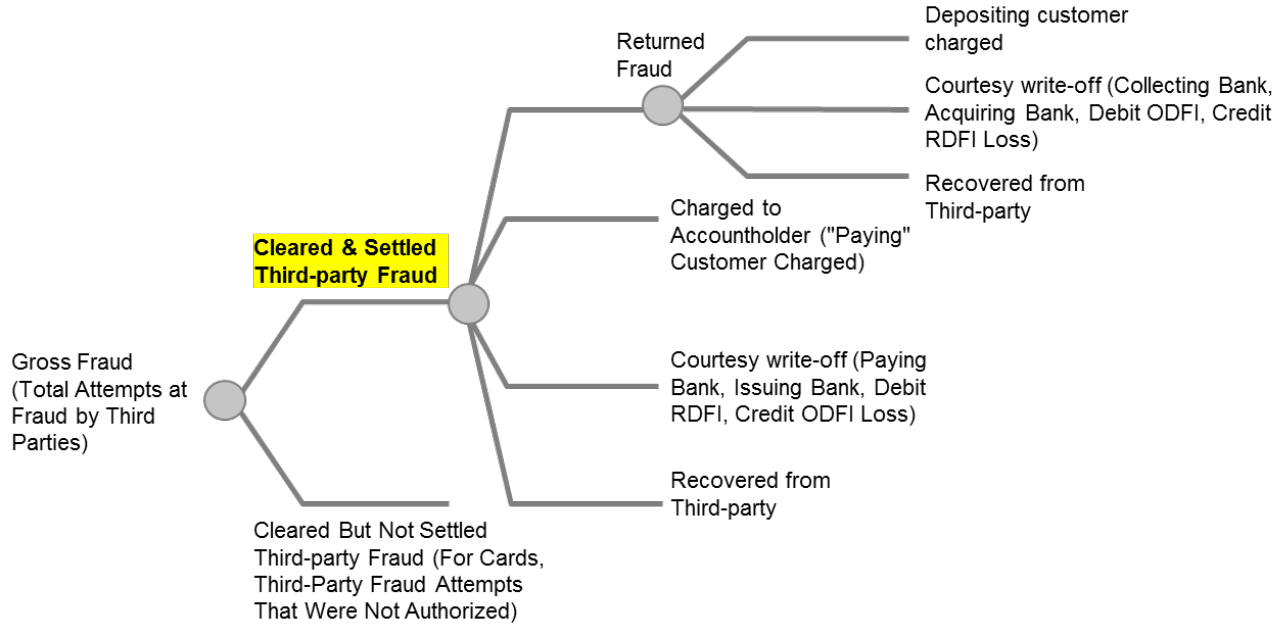
Do not include:

- Closed-loop prepaid card, debit card, or credit card transactions
- ATM withdrawals from transaction figures unless specifically requested
- Non-network-branded transactions

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

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 2017?

Note: 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 2017 for which your institution was the issuer?

These include cards issued by your institution—including those that your institution issued and that are managed by a third party—that route transactions over a general-use prepaid card network.

Include:

- General-purpose reloadable 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
- Debit cards
- Credit cards

Note: If your answer to this question is **No**, please report "0" for the remainder of the section.

3) General-purpose prepaid card program accounts

These are accounts for both reloadable and non-reloadable prepaid cards for which your institution was the issuer.

Include:
- General-purpose prepaid, gift, or payroll cards
- General-purpose prepaid card programs managed by your institution or managed by a third party
- Non-reloadable prepaid card program accounts

Do not include:
- Debit cards
- ATM-only cards
- Closed-loop prepaid cards
- Credit cards
- Electronic benefit transfer (EBT) cards

Note: These are accounts for which your institution was the issuer of a general-purpose prepaid card. Your customer can 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 2016.

4) Total general-purpose prepaid card transactions

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

Include:
- Both consumer and business/government card transactions
- Cash back at the point of sale

Do not include:
- ATM withdrawals
- Debit card transactions
- Credit card transactions

► Example: At the grocery store, your customer bought $50 of groceries with her Visa gift card issued by your institution. Later that day, she used the same Visa gift card to purchase a $70 jacket at a department store. In this example, you would report two transactions for $120.

➲ Total general-purpose prepaid card transactions = Transactions from consumer accounts (item **4.a**) + Transactions from business/government accounts (item **4.b**).

4.a) Transactions from consumer accounts

These include all transactions made by consumer accountholders over any prepaid card network for which your institution was the issuer. If your answer is **No** to item **2** above, please report "0" here.

Do not include:
- Debit card transactions made by business/government accountholders
- Prepaid card transactions made by business/government accountholders

► Example 1: Tom used his prepaid card issued by your institution to pay for a $40 meal at a local restaurant. Later that day, he used his department store, closed-loop, prepaid card issued by your institution to buy a pair of $80 jeans. In this example, you would report only one transaction for $40.

► Example 2: Tom used his prepaid card issued by your institution to buy a $40 pair of jeans. Later that day, he used his prepaid card at the ATM for a $60 cash withdrawal. In this example, you would again report only one transaction for $40.

4.b) Transactions from business/government accounts

These include all transactions made by business/government accountholders over any prepaid card network for which your institution was the issuer. If your answer is **No** to item **2** above, please report "0" here.

Do not include:
- Debit card transactions made by consumer accountholders
- Prepaid card transactions made by consumer accountholders

► Example 1: Your corporate accountholder made a purchase of $50 with a corporate reloadable prepaid card issued by your institution. In this example, you would report one transaction for $50.

► Example 2: Your corporate accountholder made a purchase of $500 with a corporate prepaid 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 prepaid card. In this example, you would report only one transaction of $500.

5) Total general-purpose prepaid card transactions

Repeat item **4** 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.

Include:

- Both in-person and remote prepaid card transactions
- Cash back at the point of sale

Do not include:

- ATM withdrawals
- Debit card transactions
- Credit card transactions

► Example: At the grocery store, your customer bought $50 of groceries with her Visa gift card issued by your institution. Later that day, she used the same Visa gift card to purchase a $70 jacket at a department store. In this example, you would report two transactions for $120.

➲ Total general-purpose prepaid card transactions = In-person transactions (item **5.a**) + Remote transactions (item **5.b**).

5.a) In-person transactions

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 for digital wallet authentication (item **5.a.1**), EMV chip card authentication (item **5.a.2**), magnetic stripe authentication (item **5.a.3**)**,** and all other authentication methods, including keyed-in transactions, manual imprint, etc. (item **5.a.4**).

If the transaction is authorized via PIN, please report this volume under EMV chip card authentication (item **5.a.2**) if the card has a chip, or under magnetic stripe authentication (item **5.a.3**) if the card does not have a chip.

Include:

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

Do not include:

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

► 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. In this example, you would report one transaction for $15 in item **5.a** and item **5.a.1**.

5.b) Remote transactions

These include all general-purpose prepaid card transactions in 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 digital wallet authentication (item **5.b.1**), manually entered online authentication (item **5.b.2**), and all other authentication methods, including phone orders, mail orders, etc. (item **5.b.3**).

Include:

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

Do not include:

- In-person transactions

► 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 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 **5.b**, one transaction for $65 in item **5.b.1**, and one transaction for $500 in item **5.b.2**.

6) Total general-purpose prepaid card transactions

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 (POS) or bill-pay transactions made by prepaid cards processed over either signature payment card networks or PIN payment card networks.

Include:
- Both digital wallet and non-digital wallet prepaid card transactions
- Cash back at the point of sale

Do not include:
- 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 a Visa gift card issued by your institution that also required a PIN to purchase a $70 jacket at a department store. In this example, you would report two transactions for $120.

➲ Total general-purpose prepaid card transactions = Digital wallet (mobile) transactions (item **6.a**) + Non-digital wallet transactions (item **6.b**).

6.a) Digital wallet (mobile) transactions

These include all general-purpose prepaid card transactions made via a digital wallet (e.g., Apple Pay, Android Pay, Samsung Pay, PayPal Mobile, etc.). These can include online purchases using a computer, in-store purchases using a smartphone, and mobile in-app transactions.

Include:
- Digital wallet NFC (near-field communication) transactions, MST (magnetic secure transmission) transactions, QR code transactions, or barcode transactions
- Digital wallet in-app or browser transactions

Do not include:
- Transactions made with a prepaid card and not via a digital wallet

► 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.

6.b) Non-digital wallet transactions

These include all general-purpose prepaid card transactions not made via a digital wallet. Include both remote and in-person transactions not made via a digital wallet.

Include:
- Transactions made with a prepaid card and not via a digital wallet

Do not include:
- Debit card transactions made via a digital wallet (e.g., Apple Pay, Android Pay, Samsung Pay, PayPal Mobile, etc.)
- ATM withdrawals

► 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 proceeded to buy a $65 pair of shoes in a mobile application, paying with the same prepaid card with his digital wallet (Android Pay). In this example, you would report one transaction for $500.

7) Total general-purpose prepaid card cash-back at the point of sale

These include all prepaid card transactions (item **4**) for which your institution was the card issuer and for 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.

Do not include:
- ATM withdrawals
- Credit card transactions
- The amount paid for goods and services

► Example 1: 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.

► Example 2: Your accountholder used her reloadable Visa-branded prepaid card at the convenience store to make a $20 purchase, entering her PIN to authorize the transaction. She also requested $50 cash back. In this example, you would report one transaction for $50.

8) Third-party fraudulent general-purpose prepaid card transactions

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

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 ATM withdrawals

► Example: Your accountholder's prepaid card issued by your institution was stolen. The perpetrator used the card to make one purchase worth $1,000. Another of your accountholder's prepaid cards was stolen, and the perpetrator made one purchase for $300. In this example, you would report two transactions for $1,300.

► Example 2: Your accountholder 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 your accountholder in fact 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 **8**.

➲ Third-party fraudulent general-purpose prepaid card transactions = In-person transactions (item **8.a**) + Remote transactions (item **8.b**).

8.a) In-person transactions

These include only third-party fraudulent prepaid card transactions for which the card user was physically present along with the card at the point of sale, including POS transactions, NFC transactions, MST transactions, manually entered transactions, QR code transactions, or barcode 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 for digital wallet authentication (item **8.a.1**), EMV chip card authentication (item **8.a.2**), magnetic stripe authentication (item **8.a.3),** and all other authentication methods, including keyed-in transactions, manual imprint, etc. (item **8.a.4**).

If the fraudulent transaction is authorized via PIN, please report this volume under EMV chip card authentication (item **8.a.2**) if the card has a chip, or under magnetic stripe authentication (item **8.a.3**) if the card does not have a chip.

Include:

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

Do not include:

- Fraudulent remote transactions
- Fraudulent digital wallet in-app or browser transactions

► Example 1: Your accountholder's prepaid 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 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 **8.a**.

8.b) Remote transactions

These include only third-party fraudulent prepaid card transactions for which the card user did not physically present the card to authorize the transaction. 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 for digital wallet authentication (item **8.b.1**), manually entered online authentication (item **8.b.2**), and all other authentication methods including phone orders, mail orders, etc. (item **8.b.3**).

Include:

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

Do not include:

- Fraudulent in-person 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 used 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 **8.b**.

9) Third-party fraudulent general-purpose prepaid card transactions

Repeat item **8** from above. 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.

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 ATM withdrawals
- Debit 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 $1,000. Another of your accountholder's prepaid cards was stolen, and the perpetrator made one purchase for $300. In this example, you would report two transactions for $1,300.

► **Example 2:** Your accountholder 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 **9**.

➲ Third-party fraudulent general-purpose prepaid card transactions = Digital wallet (mobile) transactions (item **9.a**) + Non-digital wallet transactions (item **9.b**)

9.a) Digital wallet transactions

These include only third-party fraudulent prepaid card transactions made via a digital wallet (e.g., Apple Pay, Android Pay, Samsung Pay, PayPal Mobile, etc.)/ These can include online purchases using a computer, in-store purchases using a smartphone (NFC, MST, QR code, and barcode transactions), or mobile in-app 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.

Include:

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

Do not include:

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

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

► Example 2: Your accountholder claimed that his smartphone was stolen and used to make a $400 in-app purchase with the digital wallet installed in the smartphone, charging the purchase to his prepaid card. 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.a**.

9.b) Non-digital wallet transactions

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

Include:

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

Do not include:

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

► Example 1: Your accountholder's wallet was stolen while commuting to work. Later that day, the perpetrator made an internet purchase for $325 using your accountholder's prepaid card, name, and address. He then used the stolen card to buy lunch for $25. In this example, you would report two transactions for $350.

► Example 2: Your accountholder 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 **9.b**.

Credit Card Transactions

GENERAL TERMINOLOGY

Credit card transactions

All transactions made with credit or charge cards issued by your institution, meaning that your institution owns the receivable. 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 (e.g., 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 not include...
▪ Transactions made with Visa, MasterCard, Discover, or American Express branded credit cards. These include secured and unsecured credit cards. ▪ Transactions originated in other countries ▪ Cash advances	▪ Debit card transactions ▪ Prepaid card transactions ▪ Transfers by a corporate customer to fund its employees' payroll card accounts ▪ Convenience checks ▪ Balance transfers ▪

Digital Wallet

All purchase and bill-pay transactions made using a digital wallet in which users can complete purchases quickly and easily using near-field communication (NFC) that works in conjunction with mobile payment systems. 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.

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 tap 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 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.

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.

Convenience checks

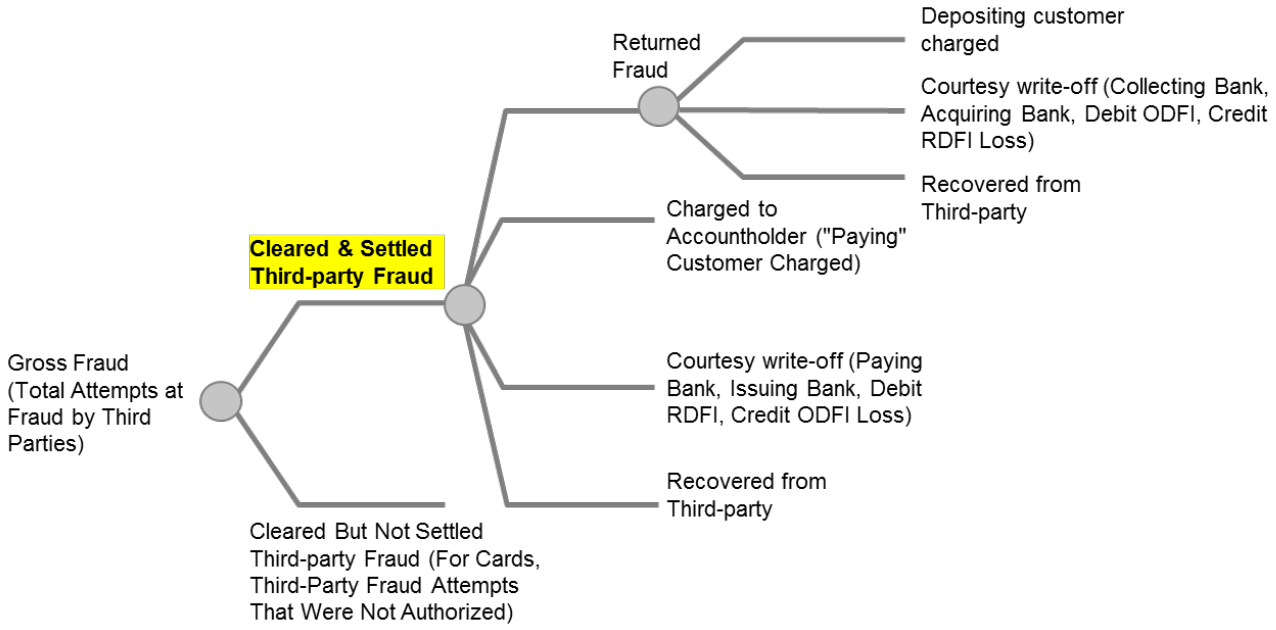
A check linked to a cardholder's credit line that can be used to make purchases, pay bills or transfer balances from one credit account to another. Convenience checks can be written up to the amount of the cardholder's credit limit (or some percentage thereof) and are considered cash advances.

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 2017 for which your institution was the issuer?

These include credit cards, charge cards, or co-branded cards for which your institution owned the receivables and that used any one of the four major credit card networks (i.e., Visa, MasterCard, American Express, and Discover).

Do not include:

- Private-label credit or charge cards that 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 cards for which your institution was not the issuing institution

Note: If your institution had cards that were branded with your institution's name, but another institution owned the receivables, do not report this volume. If your answer to this question is **No**, please report "0" for all items below in this section.

2) Did your institution have co-branded credit cards in circulation in 2017 for which your institution was the issuer?

These are credit cards that are jointly sponsored by both your institution and a retail merchant and that used any one of the four major credit card networks (i.e., Visa, MasterCard, American Express, and Discover).

Note: If your answer to this question is **Yes**, please include both "internal" (closed-loop transactions) and "external" (network transactions) volumes in your answers below.

3) Total general-purpose credit card accounts

These are unsecured or secured credit and charge card accounts for which your institution owns the receivables. Please report average monthly totals for consumer accounts (item **3.a**) and business/government accounts (item **3.b**). Average of monthly totals means the average of end-of-month totals for each of the months in 2017. If your answer is **No** to item **1** above, please report "0" here.

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

4) Consumer general-purpose credit card accounts

Please repeat item **3.a** from above. These are unsecured or secured credit and charge card accounts for which your institution owns the receivables. Please report average monthly totals for consumer accounts with current balances only (item **4.a**) and

consumer accounts with revolving balances (item **4.b**). Average of monthly totals means the average of end-of-month totals for each of the months in 2017. If your answer is **No** to item **1** above, please report "0" here.

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

Note: If your answer is **No** to item **1** above, please report "0" here. Average of monthly total means the average of end-of-month totals for each of the months in 2017.

► Definition of current balances (item 4.a): Total amount owed on the credit card up to the end of your most recent billing cycle. This is the balance that you need to pay by a certain due date so that no interest is applied.

► Definition of revolving balances (item 4.b): 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.

5) Total general-purpose credit card network transactions

These include all transactions made with credit cards, charge cards, or co-branded cards issued by your institution over a credit card network. Please report all transactions from consumer accounts (item **5.a**) and all transactions from business/government accounts (item **5.b**).

Include:

- Transactions from both consumer accounts and business/government accounts
- Both in-person transactions and remote transactions
- Cash advances

Do not include:

- Debit card transactions
- Prepaid card transactions
- Credit card non-network transactions (e.g., balance transfers or convenience checks)

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

► Example: Your customer bought $40 worth of groceries with her consumer credit card and signed a sales receipt to authorize the transaction. Later that day, she used the same card to purchase a $100 dress online but did not sign anything. In this example, you would report two transactions for $140 in items **5** and **5.a.**

6) Total general-purpose credit card network transactions

Repeat item **5** from above. These include all transactions made with credit cards, charge cards, or co-branded cards issued by your institution over a credit card network.

Include:

- Transactions from both consumer accounts and business/government accounts
- Both in-person transactions and remote transactions
- Cash advances

Do not include:

- Debit card transactions
- Prepaid card transactions
- Credit card non-network transactions (e.g., balance transfers or convenience checks)

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

► Example: Your customer bought $40 worth of groceries with her credit card and signed a sales receipt to authorize the transaction. Later that day, she used the same card to purchase a $100 dress online but did not sign anything. In this example, you would report two transactions for $140.

➲ Total general-purpose credit card network transactions = In-person transactions (item **5.a**) + Remote transactions (item **5.b**).

6.a) In-person transactions

These are all credit card transactions for which the card user is physically present with the card at the point of sale (POS). Include digital wallet (Apple Pay, Android Pay, Samsung Pay, etc.) transactions at the point of sale. Please report the total transactions for digital wallet authentication (item **6.a.1**), contactless card authentication (item **6.a.2**), EMV chip card authentication (item **6.a.3**), magnetic stripe authentication (item **6.a.4),** and all other authentication methods including keyed-in transactions, manual imprint, etc. (item **6.a.5**). If the transaction is authorized via PIN, please report this volume under EMV chip card authentication (item **6.a.3**) if the card has a chip, or under magnetic stripe authentication (item **6.a.4**) if the card does not have a chip.

Include:

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

Do not include:

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

► Example 1: Your customer bought lunch for $15 with his credit card, which is loaded into his digital wallet (Samsung Pay). He physically tapped his phone on the POS device to pay for lunch using NFC technology. In this example, you would report one transaction for $15 in item **6.a** and **6.a.1**.

► Example 2: Your customer used an ATM to withdraw $300 as a credit card cash advance. The credit cards has an EMV chip. In this example, you would report one transaction for $300 in item **6.a** and **6.a.3**.

► Example 3: Your customer pays for an Uber ride with Apple Pay in the Uber app. The total amount for the ride was $8.50. Do not report this transaction as in-person in item **6.a**. Digital wallet in-app transactions are considered remote transactions (item **6.b**). Please report this 1 transaction for $8.50 in item **6.b.**

6.b) Remote transactions

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 digital wallet authentication (item **6.b.1**), manually entered online authentication (item **6.b.2**), and all other authentication methods including phone orders, mail orders, etc. (item **6.b.3**).

Include:

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

Do not include:

- In-person transactions

► 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 used the same credit card in a digital wallet (Android Pay) to buy a $75 pair of shoes through a mobile application using his with his digital wallet. Please report two transactions for $575.

7) Total general-purpose credit card network transactions

Repeat item **5** from above. These include all transactions made with credit cards, charge cards, or co-branded cards issued by your institution over a credit card network.

Include:

- Transactions from both consumer accounts and business/government accounts
- Both card-present transactions as well as card-not-present transactions

Do not include:

- Debit card transactions
- Prepaid card transactions
- Credit card non-network transactions (e.g., balance transfers or convenience checks)

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

► Example: Your customer paid $40 for groceries with her credit card and signed a sales receipt to authorize the transaction. Later that day, she used the same card to purchase a $100 dress online but did not sign anything. In this example, you would report two transactions for $140.

➲ Total general-purpose credit card network transactions = Digital wallet (mobile) transactions (item **7.a**) + Non-digital wallet transactions (item **7.b**).

7.a) Digital wallet (mobile) transactions

These include all credit card transactions made via a digital wallet (e.g., Apple Pay, Android Pay, Samsung Pay, PayPal Mobile, etc.). These can include purchases made online with a computer, in-store purchases using a smartphone, and mobile in-app transactions.

Include:

- Digital wallet NFC (near-field communication) transactions, MST (magnetic secure transmission) transactions, QR code transactions, or barcode transactions

- Digital wallet in-app or browser transactions

Do not include:

- Transactions made with a credit card but not made via a digital wallet

► Example: Your customer bought lunch for $15 with his credit card, which is loaded into his digital wallet (Apple Pay). He physically tapped his phone on the POS device to pay for lunch. 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.

7.b) Non-digital wallet transactions

These include all general-purpose credit card transactions that are not made via a digital wallet. Include both remote and in-person transactions not made via a digital wallet.

Include:

- Transactions made with a credit card and not made via a digital wallet

Do not include:

- All credit card transactions made via a digital wallet (e.g., Apple Pay, Android Pay, Samsung Pay, PayPal Mobile, etc.)

► 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 using the same credit card in his digital wallet (Android Pay) on a mobile app. In this example, you would report one transaction for $500.

8) Total general-purpose credit card transactions

Repeat item **5** from above. These include all transactions made with credit cards, charge cards, or co-branded cards issued by your institution over a credit card network.

Include:

- Transactions from both consumer accounts and business/government accounts
- Both in-person transactions as well as remote transactions
- Cash advances

Do not include:

- Debit card transactions
- Prepaid card transactions
- Credit card non-network transactions (e.g., balance transfers or convenience checks)

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

► Example: Your customer bought $40 of groceries with her consumer credit card and signed a sales receipt to authorize the transaction. Later that day, she used the same card to purchase a $100 dress online but did not sign anything. In this example, you would report two transactions for $140 in item **8.**

➲ Total general-purpose credit card transactions = General-purpose credit card PIN-authenticated transactions (item **8.a**) + General-purpose credit card zip-code-authenticated transactions (item **8.b**) + General-purpose credit card CID authenticated transactions (item **8.c**) + General-purpose credit card other-authenticated transactions (item **8.d**).

8.a) PIN authentication

These are all general-purpose credit card transactions that were processed over a PIN payment card network.

Include:

- All general-purpose credit card transactions that were processed over a PIN (single-message) payment card network

Do not include:

- ATM withdrawals
- Prepaid card transactions
- Debit card transactions

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

► Example: Your accountholder bought $50 of groceries with her credit card by entering her PIN at the POS. In this example, you would report one transactions for $50.

8.b) Zip-code authentication

These include all credit card transactions for which your institution was the card issuer and for which the funds were authorized with a zip code over the payment card network.

Include:

- All general-purpose credit card transactions that were processed using zip-code authentication through a payment card network

Do not include:
- ATM withdrawals
- Debit card transactions

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

► Example: Your accountholder bought $65 of gas at a pump that requires zip-code authentication for credit card transactions. In this example, you would report one transaction for $65.

8.c) Card Identification Number (CID) authentication

These include all credit card transactions for which your institution was the card issuer and where the transaction was authorized using a card identification number.

Include:

All general-purpose credit card transactions that were authorized using a CVV or CVV2 (Card Verification Value Code), CSC (Card Security Code), CVC or CVC2 (Card Verification Code), or CID (Card Identification Number).

Do not include:
- ATM withdrawals
- Debit card transactions

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

► Example: Your accountholder bought a $100 pair of shoes on a department store's website using a credit card issued by your institution. The website prompted your customer to submit her card identification number (CID) to verify the authenticity of the transaction. In this example, you would report one transaction for $100.

8.d) Other authentication

These are all credit card transactions for which your institution was the card issuer and the transaction was not authorized via PIN, zip-code, or CID (**8.a, 8.b,** or **8.c**).

Include:

All general-purpose credit card transactions not authorized via PIN, zip code, or CID

Do not include:
- ATM withdrawals
- Debit card transactions

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

► Example: Your accountholder spent $5 at a convenience store using a credit card issued by your institution. The store did not require any additional identification due to the small purchase amount. In this example, you would report one transaction for $5.

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

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.

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
- Fraudulent ATM withdrawals
- Credit card transactions authorized by a valid card user as part of a scam

► Example 1: Your credit card accountholder's credit card was stolen. The perpetrator used the card and made a $500 one-time purchase. In this example, you would report one transaction for $500.

► 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 is an example of first-party fraud (false claim of fraud), you would not include this transaction in item **9**.

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

9.a) In-person transactions

These include only third-party fraudulent credit card transactions for which the card user was physically present with the card at the point of sale, including POS transactions, NFC transactions, MST transactions, manually entered transactions, RFID transactions, QR code transactions, and barcode transactions. Include all third-party unauthorized credit card transactions, before any recoveries or chargebacks. Please report any fraudulent third-party credit card transactions, regardless of whether the transaction resulted in a loss of funds. Please report the total transactions for digital wallet authentication (item **9.a.1**), contactless card authentication (item **9.a.2**), EMV chip card authentication (item **9.a.3**), magnetic stripe authentication (item **9.a.4),** and all other authentication methods, including keyed-in transactions, RFID, manual imprint, etc. (item **9.a.5**).

If the fraudulent transaction is authorized via PIN, please report this volume under EMV chip card authentication (item **9.a.3**) if the card has a chip, or under magnetic stripe authentication (item **9.a.4**) if the card does not have a chip.

Include:

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

Do not include:

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

► Example 1: Your accountholder's credit card was stolen. The perpetrator used the card and made two purchases totaling $1,000 over the internet. He then proceeded to buy lunch for $35 at a restaurant using the stolen card by swiping the magnetic stripe at the POS. In this example, you would report one transaction for $35 in item **9.a** and **9.a.4**. The internet transactions should be reported in item **9.b.**

► Example 2: Jane was a credit card accountholder at your institution. She was an active customer in good standing. She consistently paid her credit card balance on time and never maxed out her credit limit. Over time, her credit limit had increased to $10,000. One day, Jane maxed out her limit and decided not to pay off any part of her outstanding balance. Since this is an example of first-party fraud (no intention to pay balance), these transactions should not be included in item **9.a**.

9.b) Remote transactions

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

Include:

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

Do not include:

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

► Example: Your accountholder's credit card was stolen. The perpetrator used the card to purchase a TV for $500 at a store by fraudulently signing the receipt. He then used the stolen card to buy an item online for $250. In this example, you would report one transaction for $250 in item **9.b** and **9.b.2**. The in-store transaction for $500 should be reported in item **9.a.**

► 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 your accountholder in fact made this purchase on his card. Since this transaction is an example of first-party fraud (false claim of fraud), it would not be included in item **9.b**.

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

Repeat item **9** from above. 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.

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
- Fraudulent ATM withdrawals
- Credit card transactions authorized by a valid card user as part of a scam

► Example 1: Your credit card accountholder's credit card was stolen. The perpetrator used the card to make a one-time $500 purchase. In this example, you would report one transaction for $500.

► 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 your accountholder in fact made this purchase on her card. Since this transaction is an example of first-party fraud (false claim of fraud), it would not be included in item **10**.

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

10.a) Digital wallet transactions

These include only third-party fraudulent credit card transactions made via a digital wallet (e.g., Apple Pay, Android Pay, Samsung Pay, PayPal Mobile). These can include purchases made online using a computer, in-store purchases using a smartphone (NFC, MST, QR code, and barcode transactions), and mobile in-app purchases. Include all third-party unauthorized credit card transactions, before any recoveries or chargebacks. Please report any fraudulent third-party credit card transactions, regardless of whether the transaction resulted in a loss of funds.

Include:

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

Do not include:

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

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

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

10.b) Non-digital wallet transactions

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

Include:

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

Do not include:

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

► Example 1: Your accountholder's wallet was stolen while commuting to work. The perpetrator made an internet purchase for $325 using your accountholder's credit card, name, and address. He then used the stolen card to buy lunch for $25. In this example, you would report two transactions for $350.

► Example 2: Mark was a credit card accountholder at your institution. He was an active customer in good standing. He consistently paid off his credit card balance on time and had never maxed out his credit limit. One year after opening his account, however, he maxed out his credit limit and began missing payments. When your institution tried to collect payments from Mark, his identity was discovered to be falsified (synthetic ID). Since this is an example of first-party fraud (bust-out fraud with synthetic ID), these transactions should not be included in item **10.b**.

11) Third-party fraudulent general-purpose credit card transactions

Repeat item 9 from above. 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.

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

► Example 1: Your accountholder's credit card, which was issued by your institution, was stolen. The perpetrator used the card to make one purchase worth $1,000. In this example, you would report one transaction for $1000.

► **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 your accountholder in fact 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, 10,** or **11**.

➲ Third-party fraudulent general-purpose debit card transactions = PIN authentication transactions (item **11.a**) + Zip-code authentication (item **11.b**) + Card Identification Number (**11.c**) + Other authentication (**11.d**).

11.a) PIN authentication

These include only third-party fraudulent credit card transactions for which your institution was the card issuer and which were authorized using PIN authentication.

Include:

- Third-party fraudulent general-purpose credit card transactions that were processed over a PIN (single-message) payment card network

Do not include:

- ATM withdrawals
- Prepaid card transactions
- Debit card transactions

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

► Example: Your accountholder's wallet was stolen while commuting to work, and the perpetrator was able to discover the PIN. The perpetrator then made a PIN authorized credit card transaction of $200. In this example, you would report one transaction for $200.

11.b) Zip-code authentication

These include only third-party fraudulent credit card transactions for which your institution was the card issuer and for which the transactions were approved using zip-code authentication

Include:

- Third-party fraudulent general-purpose credit card transactions that were processed using zip-code authentication through a payment card network

Do not include:

- ATM withdrawals
- Prepaid card transactions
- Debit card transactions

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

► Example: A perpetrator stole your customer's wallet and was able to guess the credit card account's zip code based on the identification in your customer's wallet. The perpetrator bought gas for $65 at a pump and entered the required zip-code to authorize the credit card transactions. In this example, you would report one fraudulent transaction for $65.

11.c) Card Identification Number (CID) authentication

These include only third-party fraudulent credit card transactions for which your institution was the card issuer and for which transactions were approved using a card identification number.

Include:

- Third-party fraudulent general-purpose credit card transactions that were authorized using a CVV or CVV2 (Card Verification Value Code), CSC (Card Security Code), CVC or CVC2 (Card Verification Code), or CID (Card Identification Number).

Do not include:

- ATM withdrawals
- Debit card transactions
- Prepaid card transactions

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

► Example: A perpetrator stole your customer's credit card, which was issued by your institution. He used the card to buy a $100 pair of shoes on a department store's website. The website prompted your customer to submit his card identification number to verify the authenticity of the transaction. In this example, you would report one transaction for $100.

11.d) Other authentication

These include all fraudulent credit card transactions for which your institution was the card issuer and the transaction was not authorized via PIN, zip-code, or CID (**11.a, 11.b,** or **11.c**).

Include:

- All general-purpose credit card transactions not authorized via PIN, zip code, or CID

Do not include:

- ATM withdrawals
- Debit card transactions from regular transaction deposit accounts
- Prepaid card transactions

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

► Example: Your accountholder lost his credit card at a restaurant. A perpetrator found the credit card and spent $5 at a convenience store using your customer's credit card. The store did not require any additional identification due to the small purchase amount. In this example, you would report one transaction for $5.

Cash

GENERAL TERMINOLOGY

ATM cash withdrawals

Cash withdrawals made by your accountholders at your ATMs or at "foreign" ATMs. For this study, please follow these guidelines:

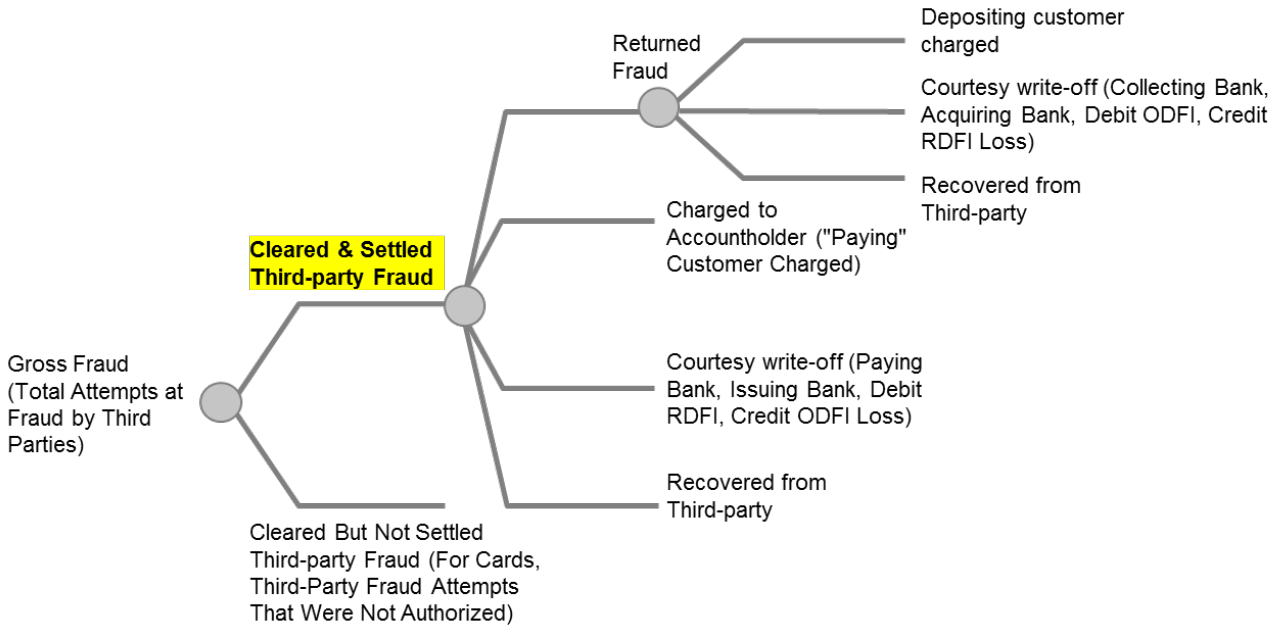
ATM cash withdrawals include...	ATM cash withdrawals do not include...
▪ All ATM cash withdrawals by your accountholders (including, as appropriate for the particular survey question, withdrawals made in other countries) ▪ Credit card cash advances	▪ Cash withdrawals or other transactions by individuals or businesses other than your accountholders ▪ Over-the-counter withdrawals ▪ Withdrawals from remote currency management terminals (RCMTs) ▪ Deposit transactions ▪ Inquiries ▪ Funds transfers ▪ Statement print-outs ▪ Purchases (e.g., stamps, tickets) ▪ Any other non-withdrawal transactions

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 limit is the credit limit or some percentage thereof. Cash advances also include convenience checks drawn on a credit card account and balance transfers.

Third-party fraud

The Federal Reserve Payments Study has identified a measure of fraud that can be described as cleared and settled third-party 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.



Cash Withdrawals

SURVEY ITEMS

1) Total ATM cash withdrawals (your institution's accountholder, any ATM)

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.

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, or other non-withdrawal transactions (e.g., inquiries, statement print-outs, purchases of stamps, tickets)

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

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

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

1.a) 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.

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

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

► Example: Your customer used her Visa Check card to withdraw $200 from an ATM that is located in a grocery store but is owned and operated by your institution. In this example, you would report one transaction for $200.

1.b) "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.

Include:

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

Do not include:

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

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

► Example: Your customer used her Visa Check card to withdraw $50 from an ATM located in a grocery store and owned and operated by another institution. In this example, you would report one transaction for $50.

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

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.

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 of fraud), you would not include it in item **2.**

Alternative Payment Initiation Methods

SURVEY ITEMS

1) Did your institution offer online or mobile consumer bill payments during calendar year 2017?

Include:

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

Do not include:

- Payments made through the biller's website

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

► Example: Your accountholder paid his utility bill through his PC by initiating a payment from his account via your institution's website. Another accountholder paid his rent by initiating a payment from his account via your institution's website using his smartphone. A third accountholder paid his rent by 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.

1.a) If your answer is "Yes" to item 1 above, are you able to exclude small business volume from your answer below?

If your answer is "No," please explain in the comments box to the right of the question and include the small business volume in your response.

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

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

Include:

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

Do not include:

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

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

► Example: Your accountholder paid his $50 utility bill through his PC by initiating a payment from his account via your institution's website. 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 2017?

Include:

- All online, mobile, and SMS/text message funds transfer transactions from person to person (P2P)

Note: If your answer to this question is **No**, please skip item **3.a** and report "0" for items **4**, **4.a**, and **4.b** below.

► Example: Your accountholder initiated payment from his account to another person's account at another institution via Zelle on the mobile version of your institution's website. Another accountholder at your institution initiated 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.

3.a) If your answer is "Yes" to item 3 above, are you able to exclude small business volume from your answer below?

If your answer is "No," please explain in the comments box to the right of the question and include the small business volume in your response.

4) Total online or mobile person-to-person (P2P) transfer originations

These include all person-to-person transfers originated by your institution's consumer accountholders and initiated through your institution's website, mobile application, or via SMS/text message to another consumer account.

Include:

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

Do not include:
- Any bill payment transactions

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

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

4.a) Total online or mobile person-to-person (P2P) "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 SMS/text message

Do not include:
- Business/government-to-person
- Transfers from small business accounts to consumer accounts

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

► Example: Your accountholder paid his friend, also an accountholder at your institution, $50 using Zelle on your institution's mobile app. In this example you would report one transaction for $50.

4.b) Total online or mobile person-to-person (P2P) "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 SMS/text message

Do not include:
- Business/government-to-person
- Transfers from small business accounts to consumer accounts
- Received P2P transfers from an accountholder at another institution

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

► Example 1: Your customer paid $100 using Popmoney to his 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 his 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**.