The Federal Reserve Payments Study

Survey Period: Calendar Year 2016

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

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

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

Retail sweep program account-type definitions

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

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

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

Wholesale sweep program account-type definitions

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

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 1 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 2016.

➲ 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

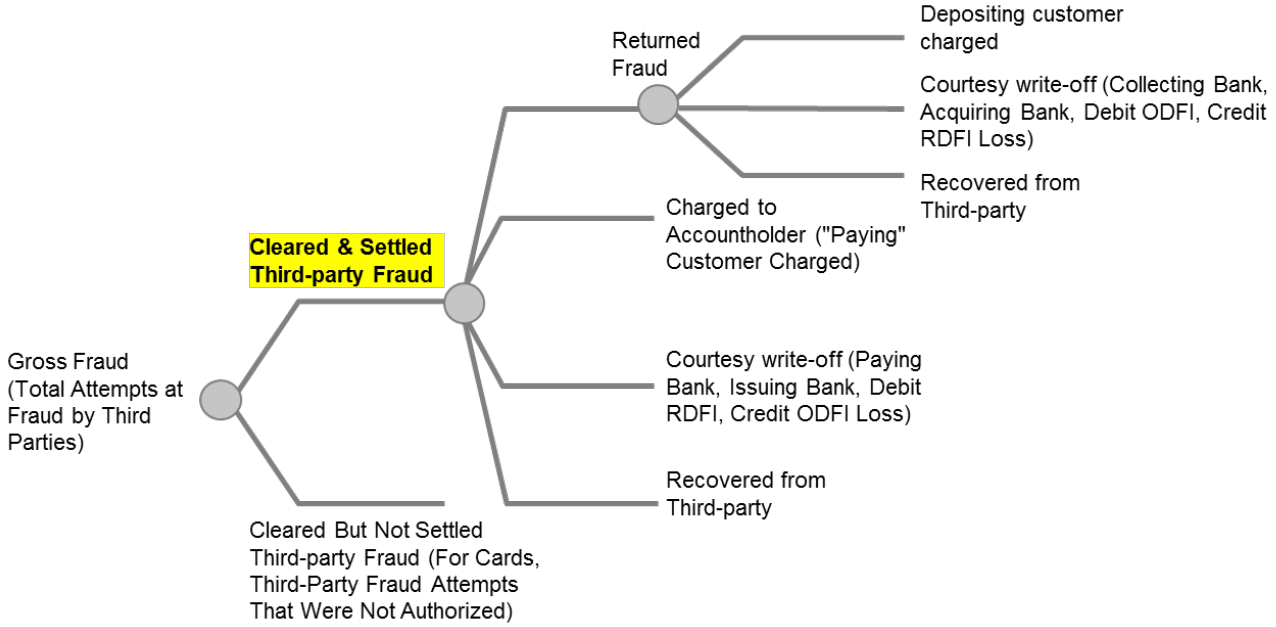
Check (or share draft) –
A negotiable instrument drawn on a depository institution. For this study, please follow these guidelines:

Checks include…	Checks do not include…
▪ Checks by individuals, business 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 your institution by a correspondent banking customer, which is 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 fraud transactions. It is not a loss of funds measure, nor is it a measure of fraud attempts. It is a measure of the extent that third-parties not authorized to conduct transactions are able to penetrate the system and effect settlement between banks, or create a book transfer of funds if it happens within an institution. The definition includes third-party fraud with all types of outcomes that may or may not include a loss to various entities, but constitutes a fraud attempt that manage to create funds transfer, if only temporary. The definition is depicted below within the hierarchy of fraud attempts visible to your institution. The definition of fraud in this study is highlighted in yellow to show that cleared and settled third-party fraud includes at least six different categories of fraud outcomes.



SURVEY ITEMS

1) Did your institution outsource check processing to another organization (i.e., its "processor") during calendar year 2016?

If your institution does not have the ability to 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 2016, 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 they may respond on your behalf. If your institution outsourced check processing for part of 2016, please also request that 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?

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 2016?

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 present 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

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 (as opposed to 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, 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 includes non-check documents which should be excluded here in item **5**.

► Example: Your customer wrote a check to pay her water bills. If your institution has a depository relationship with this water company, these checks will be "on-us" deposited checks. Others will be presented to your institution as inclearings from other depository institutions through the Federal Reserve, local clearinghouses or directly for same-day settlement.

➲ 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) Checks drawn on your institution for which another institution was the "bank of first deposit"

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, local clearinghouse, or directly for same-day settlement, to your institution for payment. Please report 1 check with a value of $125.

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

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

Include:

- All checks cleared between your affiliates. These checks are a subset of total deposited checks, 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 them in this volume.

► Example: Your customer wrote a check to her babysitter for $65, 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. Please report 1 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 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. Please report 1 check with a value of $98.

7) Third-party fraudulent checks drawn at your institution

All third-party fraudulent unauthorized checks drawn on your institution which 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 where funds were 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 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 didn't 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 an item misread, posted erroneously to her account for $110. For this question, please report 1 transaction for $2,000.

► Example 2: Daniel is an accountholders 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, not him. Your institution made an inquiry into the fraud claim and was able to determine that Daniel indeed was the person who wrote the check and made a false claim of fraud. For this question, please don't report the transaction as fraud since this 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 platform according to NACHA rules and format conventions. For this study, please follow these guidelines:

ACH entries include…	ACH entries do not include…
▪ Debits & credits sent and received ▪ On-us entries ▪ Network entries ▪ Returns	▪ Addenda records ▪ Zero-dollar items (e.g. NOCs, Prenotes) ▪ Deletes/Reversals

Originating Depository Financial Institution (ODFI) –

The Originating Depository Financial Institution (ODFI) is 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 RDFI is the depository institution that accepts and posts ACH transactions to customer accounts.

Network ACH entry –

A network ACH entry is one that is cleared through a network operator (i.e., the Fed or EPN).

In-house on-us ACH entry (cleared within your institution and not through the Fed or EPN) –

An in-house on-us ACH entry is one for which your institution is both the ODFI and the RDFI without the use of a network operator (i.e., the Fed 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 Entries –

A Direct Exchange ACH entry is one that is exchanged directly between your institution and another without the use of a network operator (i.e., the Fed 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 offset ACH entry is an on-us entry used to effect settlement by an ODFI. For example, when acting as ODFI for 100, $1,000 credit entries for a corporate accountholder, an ODFI might originate a single $100,000 debit entry to draw funds from the originator's funding account.

Balanced File –

Balanced files contain offsetting entries that automatically credits or debits the customer's DDA account 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 –

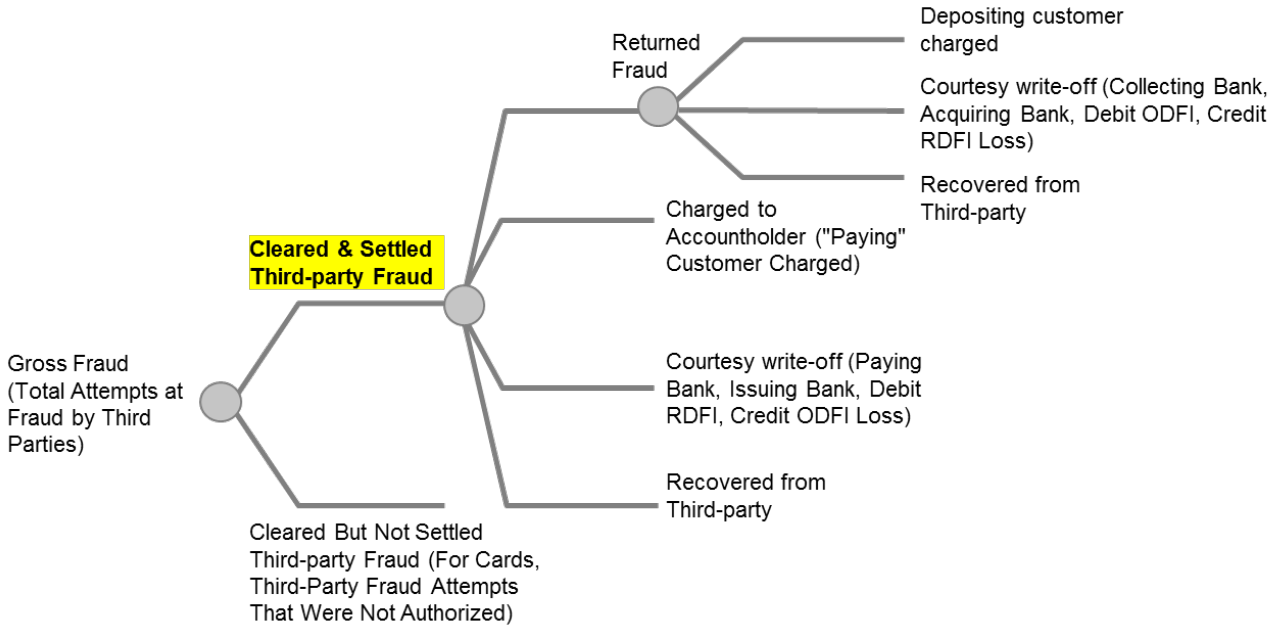
Unbalanced files do not have an offsetting entry that automatically credits or debits the customer's DDA account for the debit and/or credit originated. After receiving the file from the accountholder, the ODFI will then originate the offset entries to balance the file. Most institutions prefer to receive unbalance 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 or ENR entry cannot be a same day entry. Network ACH same day credit entries became effective as of September 23, 2016.

Third-party fraud –

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



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 2016?

If your answers 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 2016?

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, and item **7** and its subsets below.

3) Did your institution originate forward ACH debits (not including returns or offset entries) during calendar year 2016?

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 2016?

Offset entries are internal settlements for ACH transactions by an ODFI. In most cases, institutions offset (or move) the funds from the DDA account of the account holder to an "in process" account before the funds get 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 their employees $1,000 each electronically through ACH. In order 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 account to your institution's "in process" account (this is a suspense account owned by your institution which settles internally or with the network operator, i.e., the Fed or EPN). Lastly, your institution will do a net settlement of money with the network operator (i.e., the FED 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, and **9** and its subsets. Please provide instructions in the comments section at the end of the questionnaire's page 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 2016?

Please provide the number of balanced files received from your accountholders during calendar year 2016.

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 the percentage of the total settlement files that ACH balanced files constituted (estimate) during calendar year 2016.

If your institution is unable to provide the number of balanced files received during calendar year 2016, 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 2016?

Please provide the number of unbalanced files received from your accountholders during calendar year 2016.

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 the percentage of the total settlement files that ACH unbalanced files constituted (estimate) during calendar year 2016.

If your institution is unable to provide the number of unbalanced files received during calendar year 2016, 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 2016?

The effective date for network same-day settlement of credits was September 23, 2016. However, some institutions may have used proprietary systems prior to this date.

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)

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 your institution originated 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 Fed or EPN). Please 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 your institution originated here.

► Example: Your corporate customer paid 5 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 Fed or EPN). Please report 5 transactions for $2,500.

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

All ACH credit entries not cleared through the Fed or EPN 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 your institution originated 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. 10 of its employees have deposit accounts at your institution. To credit the accounts of those 10 employees, your institution originated in-house on-us credit entries to forego clearing fees from the Fed or EPN. For this question, please report 10 transactions for $8,000.

6.c) Direct exchange ACH credit entries originated

All ACH credit entries originated not cleared through the Fed 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 Fed 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. 5 of those employees bank at institutions with which you have established direct exchange relationships in order to forego clearing fees from the Fed or EPN. You originated payment via direct exchange to the 5 employees who bank at these institutions. For this question, please report 5 transactions for $3,750.

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

Repeat item **6** above. 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 your institution originated 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 Fed or EPN). Please 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 same-day settlement

These are credit entries for which your institution was the ODFI 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.

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 doesn't bank with your institution. Since the payment of this bill was urgent, your customer decided to utilize the same-day settlement option your institution began offering on September 23, 2016. Since the ACH credit is sent to an unaffiliated institution, your institution sent the ACH entries through a network operator (i.e., the Fed or EPN). For this question, please report 1 entry for $2,500.

7.b) ACH credit entries originated non-same-day settlement

These are credit entries for which your institution was the ODFI and 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 Fed or EPN). The settlement of money occurred on a different day than the transmission of the file. For this question, please report 50 transactions for $120,000.

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

Only third-party fraudulent unauthorized ACH credit entries, which cleared and settled, for which your institution was the ODFI and resulted in transfer of funds to the RDFI. These entries would typically be fraudulent payments resulting from an account takeover by an unauthorized third party. Please report any third-party ACH transactions regardless of whether or not the funds were recovered by your accountholder.

Include:

- Only fraudulent cleared and settled ACH credit transactions originated that were not authorized by your institution's accountholders (third-party fraud). If the fraudulent transaction is on-us, cleared and settled means that 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 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. For this question, please 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. In order to wrongly retrieve the last salary paid 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

Only third-party fraudulent unauthorized ACH credit entries for which your institution was the ODFI and resulted in transfer of funds to the RDFI the same day the settlement file was sent. Please report any third-party ACH transactions regardless of whether or not the funds were recovered by your accountholder

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 5 payments for $1,000 each to an account he maintains under a false name. The funds were made available to the perpetrator's account the same day the transactions cleared. For this question, please report 5 transactions for $5,000.

► Example 2: A small business accountholder at your institution originates vendor payments via ACH through your online portal. He just recently acquired an expensive tool for his business and paid for it via ACH, which funds settled on the same day the file was transferred. The tool malfunctioned after five days of use and the vendor didn't offer any kind of 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

Only third-party fraudulent unauthorized ACH credit entries for which your institution was the ODFI and resulted in transfer of funds to the RDFI in a different day the settlement file was sent. Please report any third-party ACH transactions regardless of whether or not the funds were recovered by your accountholder

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 3 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. For this question, please report 3 transactions for $9,000.

► Example 2: A small business accountholder at your institution originates vendor payments via ACH through your online portal. He just recently acquired an expensive tool for his business and paid for it via ACH, which funds settled two days after the file was transferred. The tool malfunctioned after five days of use and the vendor didn't offer any kind of 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 & Outgoing Returns

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

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

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 insurance monthly bill payments of $75. His biller (the insurance company) originated debit entries through another depository institution (i.e., the ODFI) that your institution received and posted to your customer's account. For this question, please 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 cell phone monthly bill payment of $50. His biller (cell phone company) originated debit entries through another depository institution (i.e., the ODFI) that your institution received and posted to your customer's account. For this question, please report 12 transactions for $600.

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

All ACH debit entries not cleared through the Fed or EPN for which your institution was both the ODFI and RDFI for the purpose of moving funds from one account to another at your institution.

Include:

- 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. 20 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 in order to forego clearing fees from the Fed or EPN. For this question, please report 240 transactions for $10,800.

9.c) Direct exchange ACH debit entries received

All ACH credit entries received not cleared through the Fed 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, not your corporate customer, collected monthly payments of $30 from its customers by originating ACH debit entries using a different institution as its ODFI. 10 of those customers bank at your institution. Your

institution has established direct exchange relationships with the ODFI in order to forego clearing fees from the Fed or EPN. To debit the accounts of those customers, your institution received debits entries via direct exchange. For this question, please report 120 transactions for $3,600.

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

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

Include:

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

Do not include:

- ACH entries returned to your institution unpaid (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. For this question, please report 1 transaction for $86.

11) Third-party fraudulent forward ACH debit entries your institution received

Only third-party fraudulent unauthorized ACH debit entries, which cleared and settled, for which your institution was the RDFI and resulted in transfer of funds to the ODFI. Please report any fraudulent third-party ACH transaction regardless of whether or not the funds were recovered by your accountholder.

Include:

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

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

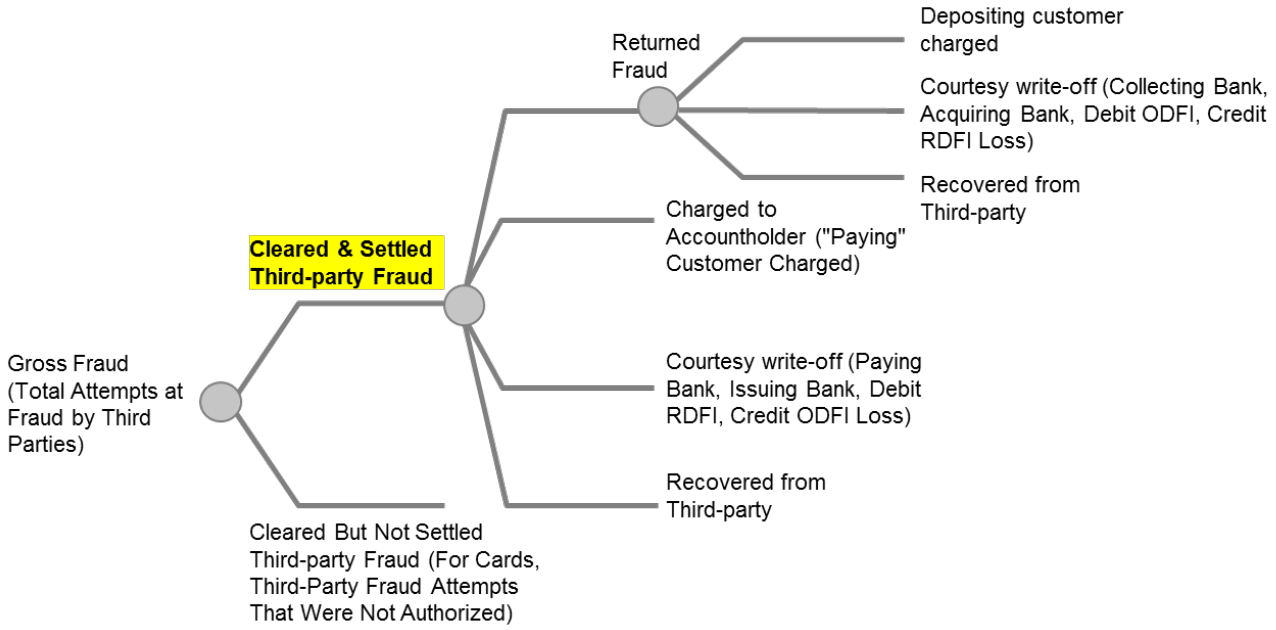
► Example 1: A fraudster opened a commercial bank account for a fictitious home cleaning service at another institution and originated unauthorized bill payments from hundreds of consumer accounts. Five of those accounts were at your institution, and each was debited once for $200. The received debit ACH transactions cleared and settled with the ODFI. The $1,000 debited from your accountholders were made available to the fraudster's account. For this question, please report 5 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 is an example of first-party fraud (false claim of fraud), do not include this transaction in item **11**.

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



SURVEY ITEMS

1) Did your institution originate wires on behalf of an unaffiliated depository institution during calendar year 2016 (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 at the end of the page of the questionnaire.

2) Did an unaffiliated depository institution originate wires on behalf of your institution during calendar year 2016?

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 at the end of the page of the questionnaire.

3) Total wire transfer originations (outgoing)

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. Please report 1 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. Please report 1 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 provides them with the ability to transfer money between 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. Please report 1 wire transaction for $25,000.

4) Total wire transfer originations (outgoing)

Repeat item **3** from above. 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. Please report 1 transaction for $15,000.

➲ Wire transfer originations = Consumer originated wire transfers (item **4.a**) + Business/government originated wire transfers (item **4.b**).

4.a) Consumer originated wire transfers

Include:

- All wire transfers originated from consumer accounts of any type at your institution

Do not include:

- Business/government wire transfers
- Small business wire transfers

► Example: Your retail customer has a daughter in college. Your institution originated a wire transfer on behalf of this retail customer to the school to fund his daughter's college tuition via Fedwire for $35,000. The school may or may not have a depository relationship with your institution. The school may or may not have a U.S. domiciled account. Please report 1 transaction for $35,000.

4.b) Business/government originated wire transfers

Include:

- Wire transfers originated from business/government (including non-depository financial institutions) accounts of any type at your institution
- Small business wire transfers originated
- 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:

- Consumer wire transfers

► Example 1: Your institution originated a wire transfer on behalf of your corporate customer to pay its third-party vendor via Fedwire for $16,000. The vendor may or may not have a depository relationship with your institution, and the vendor may or may not have a U.S. domiciled account. Please report 1 transaction for $16,000.

► Example 2: Your institution originated a wire transfer via Fedwire to pay the bank's advertising agency $100,000. Please report 1 transaction for $100,000.

5) Total wire transfer originations (outgoing)

Repeat item **3** from above. 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. Please report 1 transaction for $15,000.

➲ Wire transfer originations = Domestic (U.S.) payee (item **5.a**) + Foreign payee (item **5.b**).

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

Include:

- All wire transfers originated from accounts at your institution that were sent to another U.S.-domiciled account

Do not include:

- Foreign wire transfers

► Example: Your institution originated a wire transfer via Fedwire on behalf of your corporate accountholder to pay its third-party vendor for $32,000. The vendor has a U.S. domiciled account. Please report 1 transaction for $32,000.

5.b) Foreign payee

Include:

- All wire transfers originated from accounts at your institution that were sent to an account outside the U.S.

Do not include:

- Domestic wire transfers

► Example: Your institution originated a wire transfer via Fedwire on behalf of your corporate accountholder to pay its third-party vendor for $55,000. The vendor has an account outside the U.S. Please report 1 transaction for $55,000.

6) Third-party fraudulent wire transfers your institution originated

All third-party fraudulent unauthorized wire transfer originations which subsequently cleared and settled. Please report any third-party fraudulent wire originations regardless of whether or not 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 two wires for $5,000 and $10,000 respectively to an account he maintained under a false name. One account was at your institution and the other was at a second institution. The transactions were cleared and settled, and the funds became available to the perpetrator. For this question, please report 2 transactions for $15,000.

► Example 2: Jennifer is a small business accountholder at your institution and she originated a wire payment for $40,000 through your online portal to her brother. After a heated conversation with her brother, Jennifer decided to recover the money previously transferred to him. She opened a fraudulent claim with your institution, stating 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 is an example of first-party fraud (false claim of fraud), do not include this transaction in item **6**.

➲ Third-party fraudulent wire transfers your institution originated = Fraudulent wires sent through a network or a correspondent bank (item **6.a**) + Fraudulent book transfers (item **6.b**).

6.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 the same 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. There was a transfer of funds between the originating and receiving accounts. The receiving account was an unaffiliated institution. Please report 1 transaction for $5,000.

► Example 2: Jennifer is a small business accountholder at your institution and she originated a wire payment for $40,000 through your online portal to her brother, who banks at a different institution. After a heated conversation with her brother, Jennifer decided to recover the money previously transferred to him. She opened a fraudulent claim with your institution, stating 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 is an example of first-party fraud (false claim of fraud), do not include this transaction in item **6.a**.

6.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: Dave is an accountholder at your institution. He buys and sells antiques at an online auction website for a living. The auction website was compromised and his username, password, and bank account information were stolen online. The perpetrator originated three wire transfers for $7,000 each to three separate accounts. One of the receiving parties is also an accountholder at your institution, and the money gets transferred through your internal wire transfer platform. For this question, please report 1 transaction for $7,000.

► Example 2: Jennifer is a small business accountholder at your institution and she originated a wire payment for $40,000 through your online portal to her brother, who also banks at your institution. The transfer of funds was done by your internal wire transfer platform. After a heated conversation with her brother, Jennifer decided to recover the money previously transferred to him. She opened a fraudulent claim with your institution, stating 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 is an example of first-party fraud (false claim of fraud), do not include this transaction in item **6.b**.

7) Third-party fraudulent wire transfers your institution originated

Repeat item **6** from above. All third-party fraudulent unauthorized wire transfer originations which subsequently cleared and settled. Please report any third-party fraudulent wire originations regardless of whether or not 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 two wires for $5,000 and $10,000 respectively to an account he maintained under a false name. One account was at your institution and the other was at a second institution. The transactions were cleared and settled, and the funds became available to the perpetrator. For this question, please report 2 transactions for $15,000.

► Example 2: Jennifer is a small business accountholder at your institution and she originated a wire payment for $40,000 through your online portal to his brother. After a heated conversation with her brother, Jennifer decided to recover the money previously transferred to him. She opened a fraudulent claim with your institution, stating 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 is an example of first-party fraud (false claim of fraud), do not include this transaction in item **7**.

➲ Third-party fraudulent wire transfers your institution originated = Fraudulent consumer originated wire transfers (item **7.a**) + Fraudulent business/government originated wire transfers (item **7.b**).

7.a) Consumer originated wire transfers

Include:

- Fraudulent wire transfers originated from consumer accounts of any type at your institution

Do not include:

- Business/government wire transfers
- Small business wire transfers

► Example 1: Trevor is a retail customer at your institution. His mail gets stolen from his house while he is out on vacation. Some of the letters stolen contained his personal bank account information. The perpetrator created a fake identification and originated one wire transfer for $8,500 at one of your institution's branches. The transaction was cleared and settled, and the funds became available to the perpetrator. Please report 1 transaction for $8,500.

► Example 2: Trevor is a retail customer at your institution. His wife, Shirley, who is also an authorized user of the account, initiated a wire transfer to another account. Trevor is unaware of this transfer and opens a fraud claim for the transaction with your institution. Your institution investigates the transaction and is able to verify that there was no wrongdoing in the transfer of funds. Since this is an example of first-party fraud (false claim of fraud), do not include this transaction in item **7.a**.

7.b) Business/government originated wire transfers

Include:

- Fraudulent wire transfers originated from business/government (including non-depository financial institutions) accounts of any type at your institution
- Fraudulent small business wire transfers originated
- Fraudulent settlement/bank business wire transfers

Do not include:

- Consumer wire transfers

► Example 1: A corporate customer's employee forgets his work laptop at a convention center. A perpetrator steals the laptop and logs in at your institution website with the saved username and password in the computer's browser. The perpetrator then originates a wire transfer for $15,000 to his account. The transaction was cleared and settled, and the funds became available to the perpetrator. For this question, please report 1 transaction for $15,000.

► Example 2: Joe's plumbing is a corporate customer at your institution. Joe initiated a wire transfer to pay for supplies. The corporate accountant, who is unaware of this payment initiated by Joe, opens a fraud claim with your institution after he is unable to match the transfer of funds to any previous outstanding debt. Your institution investigates

the transaction and is able to verify that the transaction was authorized by an account user and is not actual fraud. Since this is an example of first-party fraud (false claim of fraud), do not include this transaction in item **7.b**.

8) Third-party fraudulent wire transfers your institution originated

Repeat item **6** from above. All third-party fraudulent unauthorized wire transfer originations which subsequently cleared and settled. Please report any third-party fraudulent wire originations regardless of whether or not 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

► Example1: 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 two wires for $5,000 and $10,000 respectively to an account he maintained under a false name. One account was at your institution and the other was at a second institution. The transactions were cleared and settled, and the funds became available to the perpetrator. For this question, please report 2 transactions for $15,000.

► Example 2: Jennifer is a small business accountholder at your institution and she originated a wire payment for $40,000 through your online portal to his brother. After a heated conversation with her brother, Jennifer decided to recover the money previously transferred to him. She opened a fraudulent claim with your institution, stating 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 is an example of first-party fraud (false claim of fraud), do not include this transaction in item **8**.

➲ Third-party fraudulent wire transfers your institution originated = Fraudulent domestic (U.S.) payee wire transfers (item **8.a**) + Fraudulent foreign payee wire transfers (item 8**.b**).

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

Include:

- Fraudulent wire transfers originated from accounts at your institution that were sent to another U.S.-domiciled account

Do not include:

- Foreign wire transfers

► Example 1: Jane is an accountholder at your institution. She hosted a large charity event at her house and left her computer unlocked. During the event a perpetrator logged in to her bank account using the saved log in credentials in her browser and originated a wire transfer for $10,000 to a U.S. domiciled account. The transaction was cleared and settled, and the funds became available to the perpetrator. For this question, please report 1 transaction for $10,000.

► Example 2: Trevor is a retail customer at your institution. His wife, Shirley, who is also an authorized user of the account, initiated a wire transfer to another account domiciled in the U.S. Trevor is unaware of this transfer and opens a fraud claim for the transaction with your institution. Your institution investigates the transaction and is able to verify that there was no wrongdoing in the transfer of funds. Since this is an example of first-party fraud (false claim of fraud), do not include this transaction in item **8.a.**

8.b) Foreign payee

Include:

- Fraudulent wire transfers originated from accounts at your institution that were sent to an account outside the U.S.

Do not include:

- Domestic wire transfers

► Example 1: Michelle is an accountholder at your institution. During a recent trip oversees, her computer bag is stolen. The perpetrator was able to retrieve her log in credentials to your institution's website and her banking information. The perpetrator originated four wire transfers for a total of $19,000 to bank accounts outside the U.S. The transactions were cleared and settled, and the funds became available to the perpetrator. For this question, please report 4 transactions for $19,000.

► Example 2: Trevor is a retail customer at your institution. His wife, Shirley, who is also an authorized user of the account, initiated a wire transfer to another account domiciled outside the U.S. Trevor is unaware of this transfer and

opens a fraud claim for the transaction with your institution. Your institution investigates the transaction and is able to verify that there was no wrongdoing in the transfer of funds. Since this is an example of first-party fraud (false claim of fraud), do not include this transaction in item **8.b.**

Debit and Prepaid Cards

GENERAL TERMINOLOGY

Debit and prepaid card transactions –
All purchase and bill pay transactions made with debit cards or open-loop prepaid cards used for point-of-sale (POS) transactions. These transactions can be authenticated by either a Personal Identification Number (PIN) or by a signature. Transactions may originate, e.g., at a physical point of sale, via telephone, or via the Internet. For this study, please follow these guidelines:

Debit and prepaid card transactions include…	Debit and prepaid 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 ▪ 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 ▪ Credit card transactions ▪ Transfers by a corporate customer to fund its employees' payroll card accounts ▪ Electronic Benefit Transfer (EBT) card transactions

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 a recipient to authorize transfer 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 (POS) or bill pay transactions made with closed-loop (private-label) prepaid cards

Do Not Include:

- Open-loop (network branded) prepaid, 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 (POS) 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)

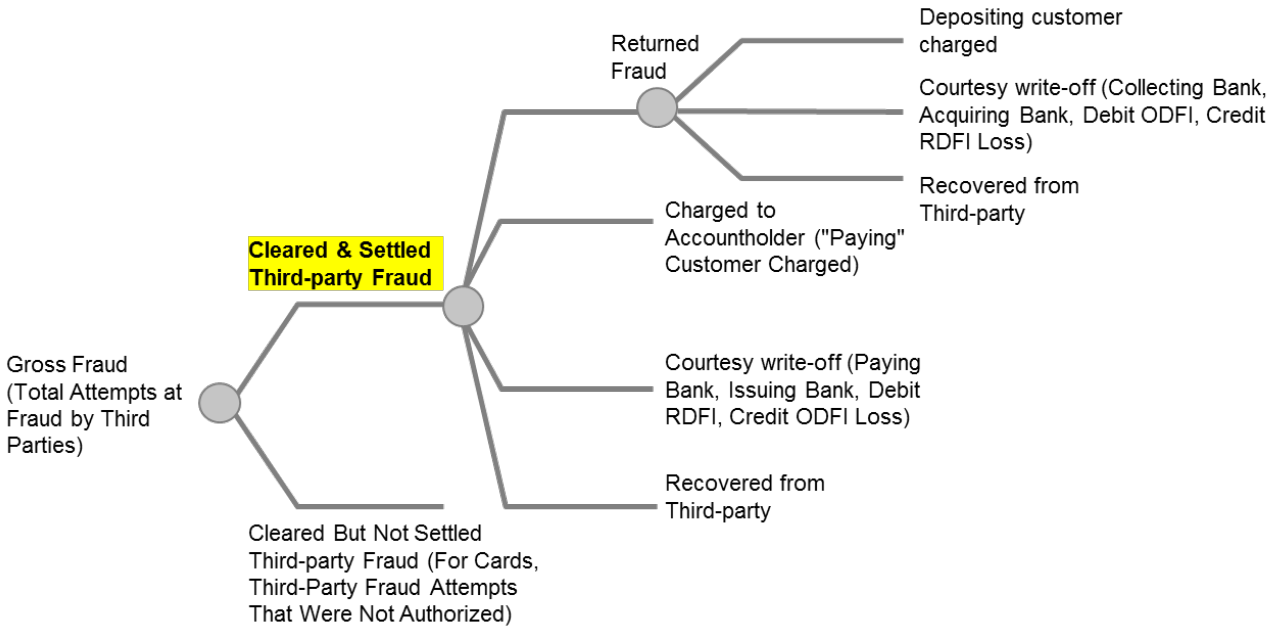
Do not include:

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



SURVEY ITEMS

1) Did your institution have general-purpose debit cards in circulation in 2016 for which your institution was the issuer?

Cards issued by your institution, including those that your institution issued and are managed by a third-party, 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.

2) Number of general-purpose debit cards

For **cards in force**, report only debit cards that can be used at the point of sale, were issued by your institution, activated by your institution's accountholders, had not expired at the end of a month, and draw on the transaction deposit accounts reported in item **1** in the Institution Profile section.

For **cards with purchase activity**, report only debit cards that had at least one point-of-sale (POS) and/or bill pay activity during the time period. Do not include cards that were only used to withdraw cash.
Please report the average of the end-of-month totals for 2016 for consumer accounts (item **2.a**) and business/government accounts (item **2.b**).

Include:

- Small business accounts under business/government accounts

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 is **No** to item **1** above, please report "0" here. Average of monthly totals means the average of end-of-month totals for each of the months in 2016.

► Example: Your institution issued 3 general-purpose debit cards to accountholders and the cards have been activated and have not expired. The debit cards can all be used to make purchases. All cards are chip-enabled, and 2 cards have purchase activity during the month, but all have the ability to be used at the point of sale during the time period. For this questions, please report 3 cards in force and 2 cards in force w/ purchase activity.

➲ Total general-purpose debit cards = Consumer general-purpose debit cards (item **2.a**) + Business/government general-purpose debit cards (item **2.b**).

2a) Consumer

Consumer debit **cards in force** and **with purchase activity** that can be used at the point of sale, were issued by your institution, draw on the transaction deposit accounts reported in item 1 in the Institution Profile section, and are in force at the end of the month. Please report the average of the end-of-month totals for 2016.

Do not include:

- Debit and ATM cards that cannot be used to make purchases at the point-of-sale (POS)

► Example: Your institution issued 1,000 debit cards to your customers. Of those 1,000 cards, 200 can were issued to Consumer accounts and only 180 were activated. Only 150 of those 180 Consumer accounts made a purchase during 2016. For this question, please report 180 cards in force, and 150 cards in force with purchase activity.

2b) Business/government

Business/government debit **cards in force** and **with purchase activity** that can be used at the point of sale, were issued by your institution, draw on the transaction deposit accounts reported in item 1 in the Institution Profile section, and are in force at the end of the month. Please report the average of the end-of-month totals for 2016.

Do not include:

- Debit and ATM cards that cannot be used to make purchases at the point-of-sale (POS)

► Example: Your institution issued 1,000 debit cards to your customers. Of those 1,000 cards, 800 can were issued to Business/government accounts and only 700 were activated. Only 600 of those 700 Business/government accounts made a purchase during 2016. For this question, please report 700 cards in force, and 600 cards in force with purchase activity.

3) Number of general-purpose debit cards

Repeat item **2** from above. For **chip enabled cards**, report only debit cards with chip technology (e.g., EMV or RFID chip-enabled cards or other form factors) that can be used at the point of sale, were issued by your institution, draw on the transaction deposit accounts reported in item **1** in the Institution Profile section, and are in force at the end of the month.

Do not include: ATM-only cards that cannot be used to make purchases at the point of sale, prepaid cards, or credit cards.

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

► Example: Your institution issued a chip enabled debit card to an accountholder and the card has not expired. The debit card was activated and can be used to make purchases. This card may or may not have had purchase activity during the month, but has the ability to be used at the point of sale during the time period. For this question please report 1 chip enabled card in force.

➲ Total general-purpose debit cards = Consumer general-purpose debit cards (item **3.a**) + Business/government general-purpose debit cards (item **3.b**).

3.a) Consumer

Consumer chip enabled debit cards in force that can be used at the point of sale, were issued by your institution, draw on the transaction deposit accounts reported in item **1** in the Institution Profile section, and are in force at the end of the month. Please report the average of the end-of-month totals for 2016.

Do not include:

- Debit and ATM chip enabled cards that cannot be used to make purchases at the point-of-sale (POS)

► Example: Your institution issued 1,000 chip enabled debit cards to your customers. Of those 1,000 cards, 200 can were issued to Consumer accounts and only 180 were activated. Only 150 of those 180 Consumer accounts made a purchase during 2016. For this question, please report 180 cards in force chip enabled.

3.b) Business/government

Business/government chip enabled debit cards in force that can be used at the point of sale, were issued by your institution, draw on the transaction deposit accounts reported in item **1** in the Institution Profile section, and are in force at the end of the month. Please report the average of the end-of-month totals for 2016.

Do not include:

- Debit and ATM chip enabled cards that cannot be used to make purchases at the point-of-sale (POS)

► Example: Your institution issued 1,000 chip enabled debit cards to your customers. Of those 1,000 cards, 800 can were issued to Business/government accounts and only 700 were activated. Only 600 of those 700 Business/government accounts made a purchase during 2016. For this question, please report 700 cards in force chip enabled.

4) Did your institution offer its customers general-purpose prepaid cards issued by another financial institution during calendar year 2016?

Note: If your answer to this question is **Yes**, please do not include these cards (or associated transactions) in your answers below.

5) Did your institution have general-purpose prepaid cards in circulation in 2016 for which your institution was the issuer?

Cards issued for prepaid card programs managed by your institution or managed by a third party for which your institution was the issuer and that route transactions over a general-use debit card network.

Include:

- General-purpose prepaid, gift, and payroll cards
- FSA (flexible spending account) cards issued by your institution
- HSA (health savings account) cards issued by your institution
- HRA (health reimbursement arrangement) cards issued by your institution

Do not include:

- Debit cards
- Closed-loop prepaid cards
- Credit cards
- Electronic benefit transfer (EBT) cards

Note: If your answer to this question is **No**, please report "0" for items **6, 7** and its subsets**, 8** and **9.b** below.

6) General-purpose prepaid card program accounts

Accounts for both reloadable and non-reloadable prepaid cards for which your institution was the issuer.

Include:

- General-purpose prepaid, gift, or payroll cards
- Card programs managed by your institution and card programs managed by a third-party
- Include 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: If your answer is **No** to item **5** above, please report "0" here. Average of monthly totals means the average of end-of-month totals for each of the months in 2016.

► Example: 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.

7) Number of general-purpose prepaid cards

For **cards in force,** report only prepaid cards that can be used at the point of sale, were issued by your institution, had not expired at the end of a month, and drawn on prepaid card program accounts listed in item **6** above.

For **cards with purchase activity**, report only prepaid cards that had at least one point-of-sale (POS) and/or bill pay activity during the time period. Do not include cards that were only used to withdraw cash.
Please report the average of the end-of-month totals for 2016 for consumer accounts (item **7.a**) and business/government accounts (item **7.b**).

Do not include:
- ATM-only cards
- Debit card
- Closed-loop prepaid cards
- Credit cards

Note: If your answer is **No** to item **5** above, please report "0" here. Average of monthly totals means the average of end-of-month totals for each of the months in 2016.

► Example: Your institution issued 100 Visa gift cards to several accountholders. The cards have not expired and all of the cards can be used to make purchases. 20 of those prepaid cards do not have any purchase activity, but still have the ability to be used at the point of sale during the time period. The rest of the prepaid cards have been used to make at least one purchase. For this question, please report 100 cards in force and 80 cards in force with purchase activity.

➲ Total general-purpose prepaid cards = Consumer general-purpose prepaid cards (item **7.a**) + Business/government general-purpose prepaid cards (item **7.b**).

7.a) Consumer

Consumer prepaid cards in force and with purchase activity that can be used at the point of sale, were issued by your institution, had not expired at the end of a month, and draw on prepaid card program accounts listed in item **6** above. Please report the average of the end-of-month totals for 2016.

Do not include:
- ATM-only cards
- Debit card
- Closed-loop prepaid cards
- Credit cards

► Example: Your institution issued 1,000 Visa gift cards to your customers. Of those 1,000 cards, 200 can were issued to Consumer accounts. Only 150 of those 200 Consumer accounts made a purchase during 2016. For this question, please report 200 cards in force (since Visa gift cards are automatically activated), and 150 cards in force with purchase activity.

7.b) Business/government

Business/government prepaid cards in force and with purchase activity that can be used at the point of sale, were issued by your institution, had not expired at the end of a month, and drawn on prepaid card program accounts listed in item **6** above. Please report the average of the end-of-month totals for 2016.

Do not include:
- ATM-only cards
- Debit card
- Closed-loop prepaid cards
- Credit cards

► Example: Your institution issued 1,000 Visa gift cards to your customers. Of those 1,000 cards, 800 can were issued to Business/government accounts. Only 700 of those 800 Business/government accounts made a purchase during 2016. For this question, please report 800 cards in force (since Visa gift cards are automatically activated), and 700 cards in force with purchase activity.

8) Number of general-purpose prepaid cards

Repeat item **7** from above. For **chip enabled prepaid cards**, report only prepaid cards with chip technology (e.g., EMV or RFID chip-enabled cards or other form factors) that can be used at the point of sale, were issued by your institution, had not expired at the end of a month, and drawn on prepaid card program accounts listed in item **6** above.

Do not include:

- Non-chip enabled prepaid cards
- ATM-only cards
- Debit card
- Closed-loop prepaid cards
- Credit cards

Note: If your answer is **No** to item **5** above, please report "0" here. Average of monthly totals means the average of end-of-month totals for each of the months in 2016.

► Example: Your institution issued 100 reloadable EMV prepaid cards to several accountholders. The cards have not expired and all of the cards were activated. 15 of those prepaid cards do not have any purchase activity, but still have the ability to be used at the point of sale during the time period. The rest of the prepaid cards have been used to make at least one purchase. For this question, please report 100 cards in force and 85 cards in force with purchase activity.

➲ Total general-purpose prepaid cards = Consumer general-purpose prepaid cards (item **8.a**) + Business/government general-purpose prepaid cards (item **8.b**).

8.a) Consumer

Consumer chip enabled prepaid cards in force that can be used at the point of sale, were issued by your institution, had not expired at the end of a month, and drawn on prepaid card program accounts listed in item **6** above. Please report the average of the end-of-month totals for 2016.

Do not include:

- Debit and ATM chip enabled cards

► Example: Your institution issued 1,000 reloadable EMV prepaid cards. Of those 1,000 cards, 200 were issued to Consumer accounts and only 180 were activated. Only 150 of those 180 Consumer accounts made a purchase during 2016. For this question, please report 180 cards in force chip enabled.

8.b) Business/government

Business/government chip prepaid cards in force that can be used at the point of sale, were issued by your institution, had not expired at the end of a month, and drawn on prepaid card program accounts listed in item **6** above. Please report the average of the end-of-month totals for 2016.

Do not include:

- Debit and ATM chip enabled cards

► Example: Your institution issued 1,000 reloadable EMV prepaid cards. Of those 1,000 cards, 800 were issued to Business/government accounts and only 700 were activated. Only 600 of those 700 Business/government accounts made a purchase during 2016. For this question, please report 700 cards in force chip enabled.

9) Total general-purpose debit and prepaid card transactions

All transactions over any debit card network for which your institution was the issuer. All point-of-sale (POS) or bill pay transactions made by debit and 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
- 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 a Visa gift card issued by your institution to purchase a $70 jacket at a department store. Please report 2 transactions for $120.

➲ Total general-purpose debit and prepaid card transactions = General-purpose debit card transactions (item **9.a**) + General-purpose prepaid card transactions (item **9.b**).

9.a) General-purpose debit card transactions

All debit card transactions for which your institution was the card issuer and where funds were debited from a regular transaction deposit account.

Include:

- Transactions over any debit card network from consumer and business/government accounts

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 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 to purchase $100 of clothes at a department store. Please report 2 transactions for $150.

9.b) General-purpose prepaid card transactions

All prepaid card transactions for which your institution was the card issuer.

Include:

- Transactions over any debit 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 **5** above, please report "0" here.

► Example: Your accountholder bought a $65 pair of shoes at a department store using a network-branded gift card issued by your institution. Please report 1 transaction for $65.

10) Total general-purpose debit and prepaid card transactions

Repeat item **9** above. All transactions over any debit card network for which your institution was the issuer. All point-of-sale (POS) or bill pay transactions made by debit and 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
- 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 a Visa gift card issued by your institution to purchase a $70 jacket at a department store. Please report 2 transactions for $120.

➲ Total general-purpose debit and prepaid card transactions = Transactions from consumer accounts (item **10.a**) + Transactions from business/government accounts (item **10.b**).

10.a) Transactions from consumer accounts

All transactions over any debit card network for which your institution was the issuer made by consumer accountholders. If your answer is **No** to item **1** and **5** 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 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 withdrawal $500. For this question, please report one 1 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. For this question, please report one 1 transaction for $40.

10.b) Transactions from business/government accounts

All transactions over any debit card network for which your institution was the issuer made by business/government accountholders. If your answer is **No** to item **1** and **5** 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. Please report 1 transaction for $50.

► Example 2: 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. Please report 2 transactions for $700.

11) Total general-purpose debit and prepaid card transactions

Repeat item **9** from above. All transactions over any debit card network for which your institution was the issuer. All point-of-sale (POS) or bill pay transactions made by debit and prepaid 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
- 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 a Visa gift card issued by your institution to purchase a $70 jacket at a department store. Please report 2 transactions for $120.

➲ Total general-purpose debit and prepaid card transactions = Person-present transactions (item **11.a**) + Remote transactions (item **11.b**).

11.a) Person-present transactions

All general-purpose debit and prepaid card transactions for which the card user is physically present along 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 only. Please report the total transactions for digital wallet authentication (item **11.a.1**), EMV chip card authentication (item **11.a.2**), magnetic stripe authentication (item **11.a.3**)**,** and all other authentication methods including keyed in transactions, RFID, manual imprint, etc. (item **11.a.4**).

If the transaction is authorized via PIN, please report this volume under EMV chip card authentication (item **11.a.2**) if the card has a chip, or under magnetic stripe authentication (item **11.a.3**) 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)
- Intermediated transactions at the point of sale (e.g., Square, Clover, iZettle, etc.)
- 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 debit card, loaded into his digital wallet (Apple Pay). He physically tapped his phone into the POS device to pay for lunch, using NFC technology. Please report 1 transaction for $15.

11.b) Remote transactions

All general-purpose debit and prepaid card transactions for which the card user does not physically present the card to authorize the transaction, including mail-order transactions, telephone-order transactions, and internet transactions. Please report the total transactions for digital wallet authentication (item **11.b.1**), manually entered online authentication (item **11.b.2**), and all other authentication methods including phone orders, mail orders, etc. (item **11.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). Please report 2 transactions for $565.

12) Total general-purpose debit and prepaid card transactions

Repeat item **9** from above. All transactions over any debit card network for which your institution was the issuer. All point-of-sale (POS) or bill pay transactions made by debit and prepaid cards processed over either signature payment card networks or PIN payment card networks.

Include:

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

Do not include:

- ATM withdrawals
- 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 a Visa gift card issued by your institution to purchase a $70 jacket at a department store. Please report 2 transactions for $120.

➲ Total general-purpose debit and prepaid card transactions = Digital wallet (mobile) transactions (item **12.a**) + Non-digital wallet transactions (item **12.b**).

12.a) Digital wallet (mobile) transactions

All general-purpose debit and prepaid card transactions made via a digital wallet (e.g., Apple Pay, Android Pay, Samsung Pay, PayPal Mobile, etc.), this can include purchasing items on-line with a computer, using a smartphone to purchase something at a store, or 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 or prepaid card not via a digital wallet

► Example: Your customer bought lunch for $15 with his debit card, loaded into his digital wallet (Apple Pay). He physically tapped his phone into the POS device to pay for lunch, using NFC technology. He then proceeded to buy groceries for $100 with his debit card by swiping the card in a magnetic reader. For this question, please report 1 transaction for $15.

12.b) Non-digital wallet transactions

All general-purpose debit and 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 debit or prepaid card not via a digital wallet

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 proceeded to buy a $65 pair of shoes in a mobile application paying with the same debit card with his digital wallet (Android Pay). Please report 1 transaction for $500.

13) Third-party fraudulent general-purpose debit & prepaid card transactions

All third-party unauthorized debit and prepaid card transactions, before any recoveries or chargebacks, for which your institution was the card issuer. Please report any fraudulent third-party debit and prepaid card transactions regardless of whether or not the transaction resulted in a loss of funds

Include:

- Debit and 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: Your accountholder's debit card issued by your institution was stolen. The perpetrator used the card and made 1 purchase worth $1,000. Another of your accountholder's prepaid cards was stolen and the perpetrator made 1 purchase for $300. For this question, please report two 2 transactions for $1,300.

► Example 2: Your accountholder claimed her debit card was stolen and used to purchase a $500 TV in an electronics store. After an investigation by your institution, it was determined that this purchase was in fact made by your accountholder on her card. Since this is an example of first-party fraud (false claim of fraud), do not include this transaction in item **13**.

➲ Third-party fraudulent general-purpose debit and prepaid card transactions = Person-present transactions (item **13.a**) + Remote transactions (item **13.b**).

13.a) Person-present transactions

Only third-party fraudulent debit card transactions for which the card user was physically present along with the card at the point of sale, including POS transactions, NFC transactions, MST transactions, manually entered transactions, RFID transactions, QR code transactions, or barcode transactions. Include all third-party unauthorized debit card transactions, before any recoveries or chargebacks. Please report any fraudulent third-party debit card transactions regardless of whether or not the transaction resulted in a loss of funds. Please report the total transactions for digital wallet authentication (item **13.a.1**), EMV chip card authentication (item **13.a.2**), magnetic stripe authentication (item **13.a.3),** and all other authentication methods including keyed in transactions, RFID, manual imprint, etc. (item **13.a.4**).

If the fraudulent transaction is authorized via PIN, please report this volume under EMV chip card authentication (item **13.a.2**) if the card has a chip, or under magnetic stripe authentication (item **13.a.3**) if the card doesn't have a chip.

Include:

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

Do not include:

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

► Example 1: Your accountholder's debit card was stolen. The perpetrator used the card and made two purchases totaling $1,000 over the internet. He then proceeded to buy lunch for $35 at a restaurant using the stolen card. For this question, please report 1 transaction for $35.

► Example 2: Your accountholder's prepaid card was stolen. The perpetrator used the card and made two purchases totaling $60 over the internet. He then proceeded to buy lunch for $15 at a restaurant using the stolen card. For this question, please report 1 transactions for $15.

► **Example** 3: Your accountholder claimed her debit card was stolen and used to purchase a $500 TV in an electronics store. After an investigation by your institution, it was determined that this purchase was in fact made by your accountholder on her card. Since this is an example of first-party fraud (false claim of fraud), do not include this transaction in item **13.a**.

13.b) Remote transactions

Only third-party fraudulent debit card transactions for 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 or not the transaction resulted in a loss of funds. Please report the total transactions for digital wallet authentication (item **13.b.1**), manually entered online authentication (item **13.b.2**), and all other authentication methods including phone orders, mail orders, etc. (item **13.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 and purchased a TV for $500 at a store by fraudulently signing the receipt. He then proceeded to use the stolen card to buy an item online for $250. For this question, please report 1 transaction for $250.

► Example 2: Your accountholder's reloadable prepaid card was stolen. The perpetrator used the card and purchased a TV for $500 at a store by fraudulently signing the receipt. He then proceeded to use the stolen card to buy an item online for $25. For this question, please report 1 transaction for $25.

► Example 3: Your accountholder claimed his debit card was stolen and used to purchase a $20 video game online. After an investigation by your institution, it was determined that this purchase was in fact made by your accountholder on his card. Since this is an example of first-party fraud (false claim of fraud), do not include this transaction in item **13.b**.

14) Third-party fraudulent general-purpose debit & prepaid card transactions

Repeat item **13** from above. All third-party unauthorized debit and prepaid card transactions, before any recoveries or chargebacks, for which your institution was the card issuer. Please report any fraudulent third-party debit and prepaid card transactions regardless of whether or not the transaction resulted in a loss of funds

Include:

- Debit and 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 debit card issued by your institution was stolen. The perpetrator used the card and made 1 purchase worth $1,000. Another of your accountholder's prepaid card was stolen and the perpetrator made 1 purchase for $300. For this question, please report two 2 transactions for $1,300.

► **Example** 2: Your accountholder claimed her debit card was stolen and used to purchase a $500 TV in an electronics store. After an investigation by your institution, it was determined that this purchase was in fact made by your accountholder on her card. Since this is an example of first-party fraud (false claim of fraud), do not include this transaction in item **14**.

➲ Third-party fraudulent general-purpose debit and prepaid card transactions = Digital wallet (mobile) transactions (item **14.a**) + Non-digital wallet transactions (item **14.b**).

14.a) Digital wallet transactions

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

Include:

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

Do not include:

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

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

► Example 2: Your accountholder claimed his smartphone was stolen and used to make a $400 in-app purchase with the digital wallet installed in the smartphone, charging the purchase to his debit card. After an investigation by your institution, it was determined that this purchase was in fact made by your accountholder on his card. Since this is an example of first-party fraud (false claim of fraud), do not include this transaction in item **14.a**.

14.b) Non-digital wallet transactions

Only non-digital wallet general-purpose debit and prepaid 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 or not the transaction resulted in a loss of funds.

Include:

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

Do not include:

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

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

► Example 2: Your accountholder claimed her debit card was stolen and used to purchase a $500 TV in an electronics store. After an investigation by your institution, it was determined that this purchase was in fact made by your accountholder on her card. Since this is an example of first-party fraud (false claim of fraud), do not include this transaction in item **14.b**.

15) Total cash-back at point of sale

All debit card transactions (item **9.a**) and prepaid card transactions (item **9.b**) for which your institution was the card issuer and the accountholders received cash back at the point of sale. This includes 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 debit card at the grocery store to purchase $50 worth of food. She entered her PIN to authorize the transaction and also requested $20 cash-back. For this question, please report 1 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. For this question, please report 1 transaction for $50.

Credit Card Transactions

GENERAL TERMINOLOGY

Credit card transactions –
All transactions made with credit or charge cards issued by your institution, meaning your institution owns the receivable. 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	▪ Debit card transactions ▪ Prepaid card transactions ▪ Transfers by a corporate customer to fund its employees' payroll card accounts ▪ Convenience checks ▪ Balance transfers ▪ Cash advances

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) from which payments can be made.

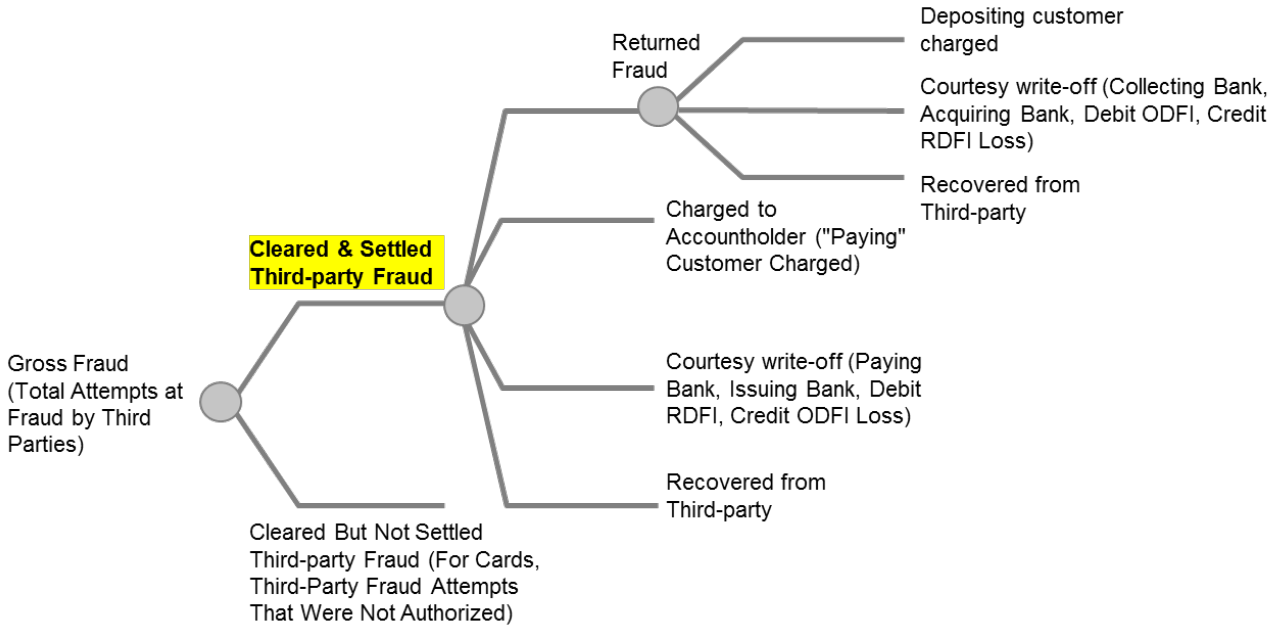
Note: Please report small business accounts under business/government accounts, if possible.

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 will be the credit limit (or some percentage thereof). It also includes 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 for making purchases, paying bills or transferring 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 fraud transactions. It is not a loss of funds measure, nor is it a measure of fraud attempts. It is a measure of the extent that third-parties not authorized to conduct transactions are able to penetrate the system and effect settlement between banks, or create a book transfer of funds if it happens within an institution. The definition includes third-party fraud with all types of outcomes that may or may not include a loss to various entities, but constitutes a fraud attempt that manage to create funds transfer, if only temporary. The definition is depicted below within the hierarchy of fraud attempts visible to your institution. The definition of fraud in this study is highlighted in yellow to show that cleared and settled third-party fraud includes at least six different categories of fraud outcomes.



SURVEY ITEMS

1) Did your institution have general-purpose credit cards in circulation in 2016 for which your institution was the issuer?

Credit or charge 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 could only be used at a limited set of merchants and that did 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) Total general-purpose credit card accounts

Unsecured or secured credit and charge card accounts for which your institution owns the receivables. Please report average monthly totals for consumer accounts (item **2.a**) and business/government accounts (item **2.b**). Average of monthly totals means the average of end-of-month totals for each of the months in 2016. 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

3) Consumer general-purpose credit card accounts

Please repeat item **2.a** from above. 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 **3.a**) and consumer accounts with revolving balances (item **3.b**). Average of monthly totals means the average of end-of-month totals for each of the months in 2016. 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

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 2016.

► Definition for current balances: Current balances are the portion for which the transaction posted during the current period.

► Definition for revolving balances: Revolving balances are the portion for which the transaction posted prior to the current statement period.

4) Number of general-purpose credit cards

Credit cards linked to the accounts listed in item **2** above that were in force during the month. Please report average monthly totals for consumer accounts (item **4.a**) and business/government accounts (item **4.b**).

For **cards in force**, report only credit cards that have been issued by your institution, activated by your accountholder, and have not expired as of end of month.

For **cards with purchase activity**, report only credit cards that had at least one point-of-sale (POS) and/or bill pay activity during the time period.

Do not include:

- Debit cards
- ATM-only cards
- Prepaid cards

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 2016.

► Example: Your institution issued 3 credit cards to accountholders and the cards have been activated and have not expired. All cards are chip-enabled and 2 cards have been used to make a purchase, but all of the cards have the ability to be used at the point of sale during the time period. For this questions, please report 3 cards in force and 2 cards in force w/ purchase activity.

5) Number of general-purpose credit cards

Credit cards linked to the accounts listed in item **2** above that were in force during the month. Please report average monthly totals for consumer accounts (item **5.a**) and business/government accounts (item **5.b**).

For **chip enabled cards**, report only credit cards with chip technology (e.g., EMV or RFID chip-enabled cards or other form factors) that can be used at the point of sale, were issued by your institution, and are in force at the end of the month.

Do not include:

- Debit cards
- ATM-only cards
- Prepaid cards

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 2016.

► Example: Your institution issued 3 credit cards to accountholders and the cards have been activated and have not expired. All cards are chip-enabled and 2 cards have been used to make a purchase, but all of the cards have the ability to be used at the point of sale during the time period. For this questions, please report 3 cards in force chip enabled.

6) Total general-purpose credit card network transactions

All transactions made with credit or charge cards issued by your institution over a credit card network. Please report all transactions from consumer accounts (item **6.a**) and all transactions from business/government accounts (item **6.b**).

Include:

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

Do not include:

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

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. Please report 2 transactions for $140 in item **6** and **6.a.**

7) Total general-purpose credit card network transactions

Repeat item **6** from above. All transactions made with credit or charge cards issued by your institution over a credit card network.

Include:

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

Do not include:

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

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. Please report 2 transactions for $140.

➲ Total general-purpose credit card network transactions = Person-present transactions (item **7.a**) + Remote transactions (item **7.b**).

7.a) Person-present transactions

All credit card transactions for which the card user is physically present along 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 only. Please report the total transactions for digital wallet authentication (item **7.a.1**), EMV chip card authentication (item **7.a.2**), magnetic stripe authentication (item **7.a.3),** and all other authentication methods including keyed in transactions, RFID, manual imprint, etc. (item **7.a.4**).

If the transaction is authorized via PIN, please report this volume under EMV chip card authentication (item **7.a.2**) if the card has a chip, or under magnetic stripe authentication (item **7.a.3**) 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)
- Intermediated transactions at the point of sale (e.g., Square, Clover, iZettle, etc.)
- 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, loaded into his digital wallet (Samsung Pay). He physically tapped his phone into the POS device to pay for lunch using NFC technology. Please report 1 transaction for $15.

► Example 2: Your customer utilized an ATM to withdraw $300 as a credit card cash advance. Please report 1 transaction for $300.

► 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 person-present in item **7.a**. Digital wallet in-app transactions are considered remote transactions (item **7.b**). Please report this 1 transaction for $8.50 in item **7.b.**

7.b) Remote transactions

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 **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:

- 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 credit card by entering his credit card number, name, and address. He then proceeded to buy a $75 pair of shoes in a mobile application paying with the same credit card with his digital wallet (Android Pay). Please report 2 transactions for $575.

8) Total general-purpose credit card network transactions

Repeat item **6** from above. All transactions made with credit or charge 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 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. Please report 2 transactions for $140.

➲ Total general-purpose credit card network transactions = Digital wallet (mobile) transactions (item **8.a**) + Non-digital wallet transactions (item **8.b**).

8.a) Digital wallet (mobile) transactions

All credit card transactions made via a digital wallet (e.g., Apple Pay, Android Pay, Samsung Pay, PayPal Mobile, etc.), this can include purchasing items on-line with a computer, using a smartphone to purchase something at a store, or 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 not 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 into the POS device to pay for lunch. He then proceeded to buy groceries for $100 with his credit card by swiping the card in a magnetic reader. For this question, please report 1 transaction for $15.

8.b) Non-digital wallet transactions

All general-purpose credit 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 credit card not 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 proceeded to buy a $65 pair of shoes in a mobile application paying with the same credit card with his digital wallet (Android Pay). Please report 1 transaction for $500.

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

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

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

Do not include:
- Fraud prevented by declining a transaction
- Fraud committed by a valid card user (first-party fraud)
- Fraudulent debit card transactions
- Fraudulent prepaid card transactions
- Fraudulent ATM withdrawals
- Credit card transactions authorized by a valid card user as part of a scam
- Fraudulent Cash advances

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

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

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

9.a) Person-present transactions

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

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

Include:

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

Do not include:

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

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

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

9.b) Remote transactions

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

Include:

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

Do not include:

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

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

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

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

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

Include:

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

Do not include:

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

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

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

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

10.a) Digital wallet transactions

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

Include:

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

Do not include:

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

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

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

10.b) Non-digital wallet transactions

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

Include:

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

Do not include:

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

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

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

Cash

GENERAL TERMINOLOGY

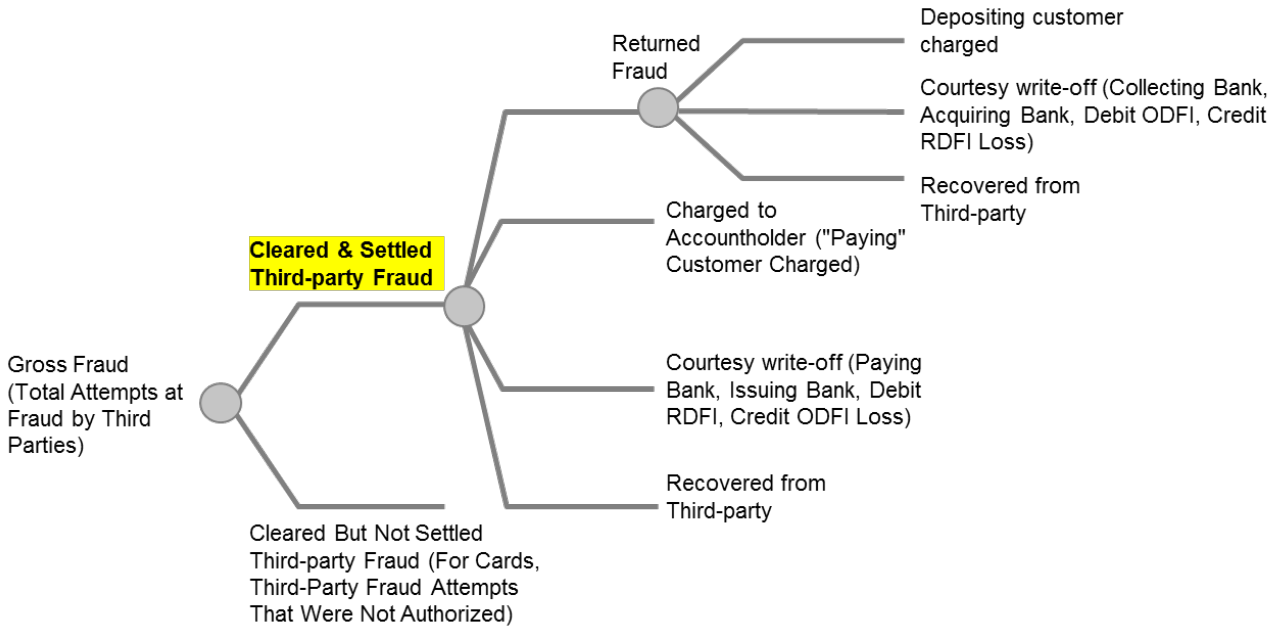
Cash withdrawals –
Cash withdrawals made by your accountholders at your ATMs, "foreign" ATMs, wholesale vaults, over-the-counter, or from remote currency management terminals (RCMTs). For this study, please follow these guidelines:

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

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

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

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



Cash Withdrawals

SURVEY ITEMS

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

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

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

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

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

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

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

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

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

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

5) Total cash withdrawals by your institution's accountholders

Total cash withdrawals made from accounts at your institution.

Include:

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

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

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

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

Include:

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

Do not include:

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

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

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

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

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

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

Include

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

Do not include:

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

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

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

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

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

Include:

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

Do not include:

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

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

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

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

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

Include:

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

Do not include:

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

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

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

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

6) Total cash withdrawals by your institution's accountholders

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

Include:

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

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

6.a) Cash withdrawals from deposit accounts

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

Do not include:

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

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

6.b) Cash withdrawals from prepaid card program accounts

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

Do not include:

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

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

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

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

Do not include:

- Cash withdrawals from deposit or prepaid accounts

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

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

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

Do not include:

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

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

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

Cards with ATM access

8) Total number of general purpose cards with ATM access

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

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

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

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

Include:

- Debit, Prepaid, and Credit cards with ATM access

Do not include:

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

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

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

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

Alternative Payment Initiation Methods

SURVEY ITEMS

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

Include:

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

Do not include:

- Payments made through the biller's website

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

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

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

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

Include:

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

Do not include:

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

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

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

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

Include:

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

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

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

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

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

Include:

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

Do not include:

- Any bill payment transactions

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

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

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

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

Include:

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

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

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

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

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

Include:

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

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

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