FR 3066a
OMB No. 7100-0351
Approval expires July 31, 2022
FR 3067
OMB No. 7100-0355
Approval expires March 31, 2023

The Federal Reserve Payments Study

Survey Period: Calendar Year 2021

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

---- Glossary with Examples ----

Glossary with Examples

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

Institution Profile

GENERAL TERMINOLOGY

Your institution

"Your institution" refers to the participating depository institution at its highest organizational level (i.e., holding company, if applicable), including all affiliates. Only report data associated with your institution 's U.S. domiciled accounts (i.e., those accounts located within the 50 U.S. states, D.C., or U.S. territories such as Guam, Puerto Rico, or U.S. Virgin Islands), including both domestic and cross-border transactions.

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.

Average of Monthly Totals

For the average of monthly totals calculations, please sum the number or balance of accounts at the end of each month and then divide by 12.

	Account 1		Account 2		Account 3	
	Account Open	End-of-Month Balance	Account Open	End-of-Month Balance	Account Open	End-of-Month Balance
Jan	Yes	$2,726	Yes	$497	No	Not Applicable
Feb	Yes	$2,196	Yes	$418	No	Not Applicable
Mar	Yes	$2,706	Yes	$226	No	Not Applicable
Apr	Yes	$1,553	Yes	$267	No	Not Applicable
May	Yes	$2,735	Yes	$397	No	Not Applicable
Jun	Yes	$2,899	Yes	$550	No	Not Applicable
Jul	Yes	$2,213	Yes	$176	No	Not Applicable
Aug	Yes	$2,933	Yes	$685	No	Not Applicable
Sep	Yes	$2,853	Yes	$723	Yes	$8,660
Oct	Yes	$2,352	Yes	$704	Yes	$9,329
Nov	Yes	$2,730	Yes	$0	Yes	$9,994
Dec	Yes	$1,664	Yes	$0	Yes	$9,015

	Sum	
	Number of Open Accounts	Sum of End-of-Month Balances
	2	$3,223
	2	$2,614
	2	$2,932
	2	$1,820
	2	$3,132
	2	$3,449
	2	$2,389
	2	$3,618
	3	$12,236
	3	$12,385
	3	$12,724
	3	$10,679
Sum	28	$71,201
	Divide by 12 months and round to nearest whole number	Divide by 12
Report Average	**2 accounts**	**$5,933 in balances**

Account type definitions

Consumer account

An account for personal use by an individual or household from which payments are commonly made.

Business/government account

An account owned by an organization (i.e., business, government, non-depository financial institution, or not-for-profit organization) from which payments are commonly made.

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

General-purpose prepaid card

General-purpose prepaid cards are network-branded "open-loop" prepaid cards that are capable of being processed through a dual-message network as well as one or more single-message networks.

General-purpose credit card

General-purpose credit cards, include charge cards or co-branded credit cards, are capable of being processed through a credit card network.

Virtual card

Virtual cards are used for online or over the phone purchases and do not require the accountholder to have a physical card. Virtual cards may provide greater security than a physical card because they use a unique card number, expiration date, and security code that is only valid at specific merchants or for a specific amount of time. Virtual cards may be issued for single or multiple transaction use, and they may or may not be loaded to digital wallets.

SURVEY ITEMS

DEPOSIT ACCOUNTS

1. Did your institution issue general-purpose prepaid cards and hold accounts associated with them in 2021?

If "Yes," please include such accounts in totals, as appropriate, in items **2** and **3** below. If you partner with a white-label issuer, please report "No" to this question and zero for general-purpose prepaid card program accounts and balances in items **2** and **3** below. **(Note: This instruction differs from previous surveys which requested that general-purpose prepaid card program accounts be excluded).**

Please ensure your answer on this page is consistent with your answer to item **3** in the Debit & GP Prepaid Cards section. If your answer on this page is "No," please report "No" for item **3** and "0" for items **5.b** and its subsets and **6.b** and its subsets in the Debit & GP Prepaid Cards section.

2. Transaction deposit accounts (including Demand Deposit Accounts (DDAs)) = 2.a + 2.b

Average of monthly totals means the average of end-of-month totals for each of the months in 2021.

A transaction deposit account is a deposit account for personal use by an individual or household or owned by an organization from which payments are commonly made.

We use your institution 's deposit balances as a sizing measure which contributes to the accuracy of our estimates of national aggregate payment volumes.

Include:

- Checking accounts
- Negotiable order of withdrawal (NOW) accounts
- Share draft accounts
- General-purpose prepaid card program accounts associated with cards for which your institution is the issuer, including accounts of your individual customers or prepaid accounts managed by a third party **(Note: The inclusion of general-purpose prepaid card program accounts in transaction deposits differs from previous surveys which requested that such accounts be excluded)**

Do not include:

- Savings accounts
- Money market deposit accounts (MMDAs)
- Certificates of deposit (CDs)
- Prepaid card program accounts issued on your institution 's behalf by another institution
- Credit card accounts
- Accounts of foreign governments and official institutions
- Accounts of other depository institutions
- Retail sweep program accounts (item **5** below)
- Wholesale sweep program accounts (item **7** below)

► **Example 1:** Assume your institution had only one customer in 2021. Your customer had a student checking account that was open the entire year. He also had a savings account and a credit card with your institution, but that is not relevant as these types of accounts are not included. The accountholder had an end-of-month balance of $1,000 from January through August. From September through December, he had an end-of-month balance of $1,500. Please report 1 transaction deposit account with a balance of $1,167. For accounts, the calculation is as follows: (1 account x 12 months open) / 12 months in 2021 = 1 account. For balances, the calculation is as follows: ($1,000 end-of-month balance x 8 months + $1,500 end-of-month balance x 4 months) / 12 months in 2021 = $1,167 in balances.

► **Example 2:** Assume your institution had only two customers in 2021, Joe and Jill. Your customer, Joe, has a checking account open for the months of January through June with a balance of $1,000 at the end of each month, and closed his account on June 30. Your other customer, Jill, has a checking account open from July through December, with a balance of $3,000 at the end of July and then $0 at the end of each month thereafter. In this example, report 1 account = (1 account x 6 months open + 1 account x 6 months open)/12 months in 2021 with a balance of $750 = ($1,000 end-of-month balance x 6 months + $3,000 end-of-month balance x 1 month + $0 end-of-month balance x 5 months) / 12 months in 2021 for the 2021 calendar year. Alternatively, if Joe had not closed his account but maintained a $0 balance from July to December, report 1.5 accounts = (1 account x 6 months open + 2 accounts x 6 months open) / 12 months in 2021 with a balance of $750 = ($1,000 end-of-month balance x 6 months + $3,000 end-of-month balance x 1 month + $0 end-of-month balance x 5 months) / 12 months in 2021.

2.a Consumer accounts

Please see the **GENERAL TERMINOLOGY** section above for the definition of consumer accounts.

► **Example:** Your only customer has a student checking account with an average monthly balance of $2,000 at your institution that was open during the entire year of 2021. He also has a savings account and a credit card with your institution. In this example, please report 1 consumer account = 1 account x 12 months open / 12 months in 2021 with a balance of $2,000 = $2,000 end-of-month balance x 12 months / 12 months in 2021 for the 2021 calendar year. The $2,000 balance reported is the average of end-of-month totals for each of the months in 2021.

2.b Business/government accounts

Please see the **GENERAL TERMINOLOGY** section above for the definition of business/government accounts.

► **Example:** Your customer has a business checking account with an average monthly balance of $6,000 at your institution that was open during the entire year of 2021. He also has a corporate credit card account with your institution. In this example, please report 1 business/government account = 1 account x 12 months open / 12 months in 2021 with a balance of $6,000 = $6,000 end-of-month balance x 12 months / 12 months in 2021 for the 2021 calendar year. The $6,000 balance reported is the average of end-of-month totals for each of the months in 2021.

3. Transaction deposit accounts (including Demand Deposit Accounts (DDAs)) (repeat item 2) = 3.a + 3.b

Repeat item **2** above. Average of monthly totals means the average of end-of-month totals for each of the months in 2021.

A transaction deposit account is a deposit account for personal use by an individual or household or owned by an organization from which payments are commonly made.

Include:

- Checking accounts
- Negotiable order of withdrawal (NOW) accounts
- Share draft accounts
- General-purpose prepaid card program accounts associated with cards for which your institution is the issuer, including accounts of your individual customers or prepaid accounts managed by a third party **(Note: The inclusion of prepaid card program accounts in transaction deposits differs from previous surveys which requested that such accounts be excluded)**

Do not include:

- Savings accounts
- Money market deposit accounts (MMDAs)
- Certificates of deposit (CDs)
- Prepaid card program accounts issued on your institution 's behalf by another institution
- Credit card accounts
- Accounts of foreign governments and official institutions
- Accounts of other depository institutions
- Retail sweep program accounts (item **5** below)
- Wholesale sweep program accounts (item **7** below)

► **Example 1:** Your customer has a student checking account with an average monthly balance of $3,500 at your institution that was open during the entire year of 2021. He also has a savings account and a credit card with your institution. Please report 1 transaction deposit account = 1 account x 12 months open / 12 months in 2021 with a balance of $3,500 = $3,500 end-of-month balance x 12 months / 12 months in 2021. The $3,500 balance reported is the average of end-of-month totals for each of the months in 2021.

► **Example 2:** Your customer, Joe, has a checking account open for the months of January through June with a balance of $1,000 at the end of each month. Your other customer, Jill, has a checking account open from July through December, with a balance of $3,000 at the end of July and then $0 at the end of each month thereafter. In this example, report 1 average checking account = (1 account x 6 months open + 1 account x 6 months open) / 12 months in 2021 with a balance of $750 = ($1,000 end-of-month balance x 6 months + $3,000 end-of-month balance x 1 month + $0 end-of-month balance x 5 months) / 12 months in 2021 for the 2021 calendar year.

3.a General-purpose prepaid card program accounts

These are accounts for both reloadable and non-reloadable open-loop prepaid cards for which your institution was the issuer. Your customer may or may not be able to add additional funds to this card after it has been issued and use these funds to shop, transfer money, or pay bills. If your answer is "No" to item **1** above, please report "0" here.

Include:

- General-purpose prepaid card programs managed by both your institution and a third-party
- Individual and pooled general-purpose prepaid card program accounts for which your institution is the issuer. (Count each pooled account as 1 account.)
- Consumer and business/government general-purpose open-loop reloadable prepaid card program accounts
- Consumer and business/government general-purpose open-loop non-reloadable prepaid card program accounts
- Open-loop gift card accounts
- Payroll prepaid card program accounts
- FSA/HSA medical card accounts
- Government-administered general-purpose open-loop prepaid card program accounts
- Customer refund and incentive card accounts
- Consumer and business/government general-purpose prepaid card program accounts for which only virtual cards are issued (no physical card)

Do not include:

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

► **Example:** John has an open-loop prepaid card issued by your institution that he reloads every month for his grocery shopping. His prepaid card program account contains an additional prepaid card used by his spouse. In this example, you would report 1 general-purpose prepaid card program account = 1 account x 12 months open / 12 months in 2021 its respective average end-of-month balance.

3.b All other accounts

Include:

- Checking accounts
- Negotiable order of withdrawal (NOW) accounts
- Share draft accounts

Do not include:

- Prepaid card program accounts
- Savings accounts
- Money market deposit accounts (MMDAs)
- Certificates of deposit (CDs)
- Credit card accounts
- Accounts of foreign governments and official institutions
- Accounts of other depository institutions
- Retail sweep program accounts (item **5** below)
- Wholesale sweep program accounts (item **7** below)

► **Example:** Your customer has a student checking account with an average monthly balance of $3,500 at your institution that was open during the entire year of 2021. He also has a prepaid card program account and savings account with your institution. Please report 1 transaction deposit account = 1 account x 12 months open / 12 months in 2021 with a balance of $3,500 = $3,500 end-of-month balance x 12 months / 12 months in 2021. The $3,500 balance reported is the average of end-of-month totals for each of the months in 2021.

4. Did your institution or any of its affiliates employ the use of a retail sweep program (i.e., reserve sweep program) during calendar year 2021?

Understanding if your institution used a retail sweep program will help inform our estimation process. In a retail sweep, a depository institution transfers funds between a customer 's transaction accounts (both consumer and business/government) and that customer 's savings and money market deposit accounts (MMDAs) 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. This practice does not adversely impact the accountholder but allows the institution to reduce nonearning assets.

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.

Do not consider wholesale sweep program accounts (item **7** below). If your answer to this question is "No," please report "0" for item **5** below.

5. Retail sweep program accounts (i.e., reserve sweep program accounts) = 5.a + 5.b

Average of monthly totals means the average of end-of-month totals for 2021. If your answer is "No" to item **3** above, please report "0" here.

We use your institution 's sweep account balances as an additional sizing measure to improve the accuracy of national aggregate payment volumes.

Include:

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

Do not include:

- Checking accounts
- Negotiable order of withdrawal (NOW) accounts
- Share draft accounts
- Transaction deposit accounts (item **2** above)
- Wholesale sweep program accounts (item **7** below)
- Accounts and balances of any savings-type account not associated with transaction deposit accounts under a sweep program
- General ledger accounts (the sub-accounts that have sweeps tied to them should be reported individually, rather than as one general ledger account)

► **Example:** Your customer has a student checking account with an average monthly balance of $3,500 at your institution. He also has a savings account with an average monthly balance of $15,000 with your institution, which includes a sweep to his checking account as needed to cover payments. Your institution also has a corporate customer with a savings account with an average monthly balance of $30,000 which includes a sweep to the company 's checking account. Please report 1 consumer sweep account = 1 account x 12 months open / 12 months in 2021 with a balance of $15,000 = $15,000 end-of-month balance x 12 months / 12 months in 2021. The $15,000 balance reported is the average of end-of-month totals for each of the months in 2021. Please report 1 business/government sweep account = 1 account x 12 months open / 12 months in 2021 with a balance of $30,000 = $30,000 end-of-month balance x 12 months / 12 months in 2021. The $30,000 balance reported is the average of end-of-month totals for each of the months in 2021.

5.a Consumer accounts

Please see the **GENERAL TERMINOLOGY** section above for the definition of consumer accounts.

► **Example:** Your customer has a student checking account with an average monthly balance of $2,000 at your institution that was open during the entire year of 2021. He also has a savings account and a credit card with your institution. In this example, please report 1 consumer account = 1 account x 12 months open / 12 months in 2021 with a balance of $2,000 = $2,000 end-of-month balance x 12 months / 12 months in 2021 for the 2021 calendar year. The $2,000 balance reported is the average of end-of-month totals for each of the months in 2021.

5.b Business/government accounts

Please see the **GENERAL TERMINOLOGY** section above for the definition of business/government accounts.

► **Example:** Your institution also has a corporate customer with a savings account with an average monthly balance of $30,000 which includes a sweep to the company 's checking account. Please report 1 business/government sweep account = 1 account x 12 months open / 12 months in 2021 with a balance of $30,000 = $30,000 end-of-month balance x 12 months / 12 months in 2021. The $30,000 balance reported is the average of end-of-month totals for each of the months in 2021.

6. Did your institution provide a wholesale sweep program (i.e., corporate sweep program) to your business accountholders during calendar year 2021?

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.

Do not consider retail sweep program accounts (item **5** above). If your answer to this question is "No," please report "0" for item **7** below.

7. Wholesale sweep program accounts

Average of monthly totals means the average of end-of-month totals for 2021. If your answer is "No" to item **6** above, please report "0" here.

We use your institution 's sweep account balances as an additional sizing measure to improve the accuracy of national aggregate payment volumes.

Include:

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

Do not include:

- Checking accounts
- Negotiable order of withdrawal (NOW) accounts
- Share draft accounts
- Transaction deposit accounts (item **2** above)
- Retail sweep program accounts (item **5** above)
- Accounts and balances of any savings-type account not associated with transaction deposit accounts under a sweep program

► **Example**: Your corporate customer has a business checking account with an average monthly balance of $3,500 at your institution. The company also has a business savings account with an average monthly balance of $50,000 with your institution, which includes an overnight sweep into an investment account. Please report 1 wholesale sweep program account = 1 account x 12 months open / 12 months in 2021 with a balance of $50,000 = $50,000 end-of-month balance x 12 months / 12 months in 2021. The $50,000 balance reported is the average of end-of-month totals for each of the months in 2021.

CREDIT CARD ACCOUNTS

8. Did your institution issue general-purpose credit cards and hold accounts associated with them in 2021?

If "Yes," please include the number of and balances for these accounts in items **9** and **10** below. If another institution issues credit cards on your behalf, please exclude them. If you partner with a white-label issuer, please report "No" to this question and zero for accounts and balances in items **9** and **10** below. **(Note: Credit card accounts questions appeared in the General-Purpose Credit Cards section of previous surveys.)**

Please ensure your answer on this page is consistent with your answer to item **1** in the GP Credit Cards section. If your answer is "No" on this page, please report "No" for item **1** and "0" for items **4** through **9** in the GP Credit Cards section.

9. Total general-purpose credit card accounts = 9.a + 9.b

Include general-purpose credit card accounts for which your institution was the issuer. Please report account totals, not cards (e.g., if a customer and their spouse both have a card under the same account, please report as 1 account). If your answer is "No" to item **8** above, please report "0" here.

Average of monthly totals means the average of end-of-month totals for each of the months in 2021.

Include:

- All general-purpose credit card accounts, including zero-balance active accounts, with a credit line and the ability to transact
- Accounts for general-purpose credit cards your institution issues on behalf of another institution
- Virtual general-purpose credit card accounts

Do not include:

- Any credit card accounts for which your institution was not the card issuing institution
- 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
- Debit or prepaid card program accounts
- Transaction deposit accounts
- Closed accounts

► **Example:** Tom, your consumer customer, has one credit card issued by your institution. Joe 's Diner, your corporate customer, has a corporate credit card account with separate cards for each of their ten employees. In this example, you would report 2 credit card accounts = 2 accounts x 12 months open / 12 months in 2021.

9.a Consumer accounts

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

Include:

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

Do not include:

- Business/government credit card accounts

► **Example:** Tom used his credit card issued by your institution to buy a $40 pair of jeans. His wife then used another card linked to the same account to buy $15 worth of candy. In this example, you would report 1 consumer credit card account = 1 account x 12 months open / 12 months in 2021.

9.b Business/government accounts

These include all credit cards accounts that are for business/government accountholders. Please see the **GENERAL TERMINOLOGY** section above for the definition of business/government accounts.

Include:

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

Do not include:

- Consumer credit card accounts

► **Example:** Your corporate accountholder made a purchase of $500 with a corporate credit card issued by your institution. An employee of the same institution then used her own credit card linked to the same account to make a purchase of $100. In this example, you would report 1 business/government credit card account = 1 account x 12 months open / 12 months in 2021.

10. Consumer general-purpose credit card accounts (repeat item 9.a) = 10.a + 10.b + 10.c + 10.d

Please repeat item **9.a** above. These include general-purpose credit cards for which your institution was the issuer. If your answer is "No" to item **8** above, please report "0" here. If you are unable to report items **10.a**, **10.b**, **10.c**, and **10.d** below, please explain in the comments field. In this case, report "NR" for those items and report balances for items **10.d.1** and **10.d.2** below.

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

Average of monthly totals means the average of end-of-month totals for each of the months in 2021.

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

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

► **Example:** Joe has a credit card issued by your institution. He has never made a purchase on this card, although the card account has been activated. In this example, you would report 1 credit card account = 1 account x 12 months open / 12 months in 2021 with a balance of $0 = $0 end-of-month balance x 12 months / 12 months in 2021.

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

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

Include:

- Balances associated with balance transfers received for which interest has not started accruing yet
- New accounts for which there is a promotional period of interest-free spend

► **Example:** Jay has a credit card issued by your institution, and he is a transactor (i.e., he pays the balance in full each cycle). He uses this card to make purchases occasionally and had $300 outstanding at the end of last cycle. Jay has until the end of the next billing cycle to pay the balance before interest is applied. Sarah also has a credit card issued by your institution. She has carried a balance of $500 on her account for the past two cycles; however, her card is currently in a promotional period of interest free spend. In this example, you would report 2 credit card accounts = 2 accounts x 12 months open / 12 months in 2021 with a balance of $800 = $300 end-of-month balance + $500 end-of-month balance.

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

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

► **Example:** Rachael has a credit card issued by your institution, and she is a revolver (i.e., she carries a balance from one cycle to the next). She frequently uses this card to make purchases, and she had a balance of $500 that was outstanding at the end of the prior month, of which interest was applied to her bill this month. She did not make any purchases on the card this month, so the total balance at the end of this cycle is still $500. In this example, you would report 1 credit card account = 1 account x 12 months open / 12 months in 2021 with a balance of $500 end-of-month balance. Do not include interest.

10.d With current and revolving balances = 10.d.1 + 10.d.2

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

► **Example:** Sarah has a credit card issued by your institution. She frequently uses this card to make purchases, and she had a balance of $500 that was outstanding at the end of the prior month, of which interest was applied to her bill this month. She then spent an additional $200 on the same card this month, of which interest has not yet been applied. In this example, you would report 1 credit card account = 1 account x 12 months open / 12 months in 2021 with a balance of $700 = $500 end-of-month balance + $200 end-of-month balance.

10.d.1 Current balance

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

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

10.d.2 Revolving balance

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

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

Checks

GENERAL TERMINOLOGY

Your institution

"Your institution" refers to the participating depository institution at its highest organizational level (i.e., holding company, if applicable), including all affiliates. Only report data associated with your institution 's U.S. domiciled accounts (i.e., those accounts located within the 50 U.S. states, D.C., or U.S. territories such as Guam, Puerto Rico, or U.S. Virgin Islands), including both domestic and cross-border transactions.

Checks paid

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

Checks paid include…	Checks paid do not include…
▪ Checks written by individuals, businesses, or government entities ▪ Traveler 's checks drawn on your institution ▪ Money orders drawn on your institution ▪ Cashier 's checks drawn on your institution ▪ Official checks drawn on your institution ▪ Teller 's checks drawn on your institution ▪ Payable through drafts drawn on your institution ▪ Truncated checks (i.e., image exchange) ▪ Checks paid that were subsequently returned (outgoing)	▪ 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) ▪ Payable through drafts drawn on another institution (not your institution)

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." A correspondent banking relationship is when your institution holds balances for an unaffiliated depository institution in a due-to account and performs check clearing services on its behalf.

Account type definitions

Consumer account

A transaction deposit or savings account for personal use by an individual or household from which check payments can be made.

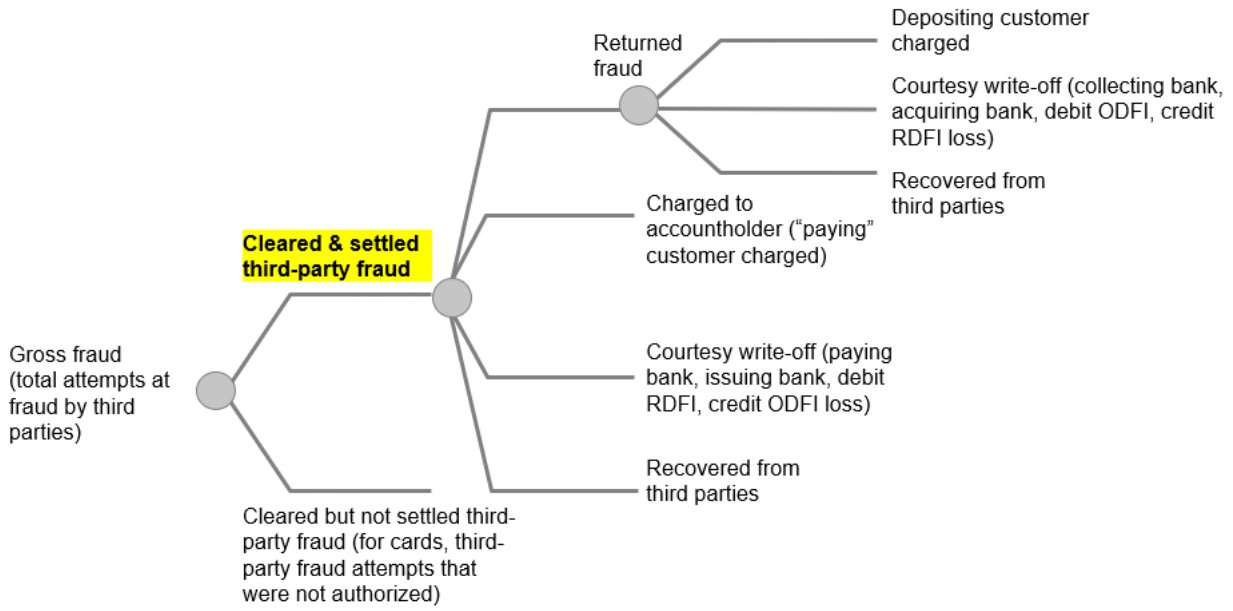
Business/government account

A transaction deposit or savings account owned by an organization (i.e., business, government, non-depository financial institution, or not-for-profit organization) from which check payments can be made.

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

Third-party fraud

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



SURVEY ITEMS

CHECK PROFILE

1. Did your institution outsource check processing to another organization (i.e., its "processor") during calendar year 2021?

If your institution cannot process checks internally and outsources this process to a third-party vendor, please answer "Yes" to this question. If your institution outsourced check processing for part of 2021, please answer "Yes."

If your answer to this question is "No," please report "Not applicable" for item **1.a** below.

Note: If your answer to this question is "Yes," please request the necessary data from your institution 's payments processor, or provide them with a PDF copy of the survey so that they may respond on your behalf. If your institution outsourced check processing for part of 2021, please also request the necessary data from your institution 's payments processor and combine it with check totals that were processed by your institution.

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

If possible, please report your institution 's check volume processed by another organization. If your answer is "No" to item **1.a** above, please report all check volume processed by your institution and explain in the comments box at the end of this section.

2. Are you able to exclude non-check documents from "total checks drawn on your institution" in items 0 and 6 below?

Non-check documents are "other" items processed on check sorters (e.g., batch headers, general ledger tickets, cash-in or cash-out tickets, deposit slips). Even if you are unable to exclude non-check documents, please report all check volumes drawn on your institution, including non-check documents.

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

Some institutions call this "on-we" volume, which should be reported entirely under item **5.b** below if possible. Even if you are unable to report "on-us" volume in item **5.b**, please report all checks drawn on your institution in item **0** and **6** below.

4. Did your institution process checks for an unaffiliated depository institution as part of a correspondent banking relationship during calendar year 2021?

If your answer is "No," please report "0" for items **5.a.2** and **8.b** below.

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

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

CHECK PAYMENTS

Checks drawn on your institution. Your customer is the payer.

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

These are all cleared and settled, domestic and cross-border checks (or share drafts) for which your institution was the paying bank as defined by Federal Reserve Regulation CC: Availability of Funds and Collection of Checks (Reg. CC).

Note: Count each unique check only once, and avoid these two common mistakes: 1) Do not double-count electronic check presentment (ECP) items if your institution received an electronic file with paper to follow, and 2) if your institution performed proof-of-deposit processing, **do not** calculate total checks drawn on your institution as the difference between prime pass and transit check volumes. Prime pass volume includes non-check documents, which should be excluded.

Include:

- Usually, the personal and business checks written by your accountholder customers, as well as checks written on behalf of your institution. Do not forget the following:
  - Controlled disbursement checks, if applicable
  - Official checks, including cashier 's checks, teller 's checks, and treasurer 's checks (i.e., those guaranteed by your institution and drawn on your institution 's account)
  - Checks presented to your institution as paying bank but were 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)

Do not include:

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

► **Example:** Your customer wrote a check for $57 to pay her water bill. If your institution has a depository relationship with this water company, these checks are "on-us" deposited checks. In this example, you would report 1 check with a value of $57 in items **0** above and **5.b** below.

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

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

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

Include:

- Inclearings 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)
- Checks deposited and drawn on different affiliates of your institution (some call this "on-we" volume)

► **Example:** Your customer wrote a check for $125 to pay for her groceries. The grocery store has a depository relationship with an unaffiliated depository institution. After processing the grocer 's deposit, that institution (i.e., the "collecting bank") presented the check through the Federal Reserve, through a local clearinghouse, or directly for same-day settlement to your institution for payment. In this example, you would report 1 check with a value of $125.

5.a.1 Inclearings

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

Include:

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

Do not include:

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

► **Example:** Your customer wrote a check for $125 to pay for her groceries. The grocery store has a depository relationship with an unaffiliated depository institution. After processing the grocer 's deposit, that institution (i.e., the "collecting bank") presented the check to your institution for payment. In this example, you would report 1 check with a value of $125.

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

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

Include:

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

Do not include:

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

► **Example:** Your customer paid a retailer using a check (i.e., the check was drawn on your institution). The retailer deposited this check at a depository institution other than your institution. The bank of first deposit outsourced its checking processing to your institution as part of a correspondent banking relationship. The institution (your correspondent customer) deposited the check with your institution for processing and forward collection.

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

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

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

Include:

- All checks cleared between your affiliates, which include but are not limited to the following:
  - Checks deposited in your branches
  - Checks received from other internal departments (e.g., wholesale or retail lockbox, currency/coin vault operations, loan payments processing operations)

- Checks deposited by corporate clients (typically in the evening) directly to your item-processing operations (i.e., pre-encoded or un-encoded deposits or remote capture deposits)
- Checks deposited and drawn on different affiliates of your institution (some call this "on-we" volume)

Do not include:

- Inclearings received from the Federal Reserve, a clearinghouse, or another institution (i.e., same-day settlement)
- 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

► **Example:** Your customer wrote a $65 check to her babysitter, who also happened to be your customer. When the babysitter deposited the check, your institution was both the collecting institution and the paying institution on this check. In this example, you would report 1 check with a value of $65.

6. Total checks drawn on your institution (repeat item 0) = 6.a + 6.b

Repeat item **0** above. These are all cleared and settled, domestic and cross-border checks (or share drafts) for which your institution was the paying bank as defined by Federal Reserve Regulation CC: Availability of Funds and Collection of Checks (Reg. CC).

Note: Count each unique check only once, and avoid these two common mistakes: 1) Do not double-count electronic check presentment (ECP) items if your institution received an electronic file with paper to follow, and 2) if your institution performed proof-of-deposit processing, **do not** calculate total checks drawn on your institution as the difference between prime pass and transit check volumes. Prime pass volume includes non-check documents, which should be excluded.

Include:

- Usually, the personal and business checks written by your accountholder customers, as well as checks written on behalf of your institution. Do not forget the following:
  - Controlled disbursement checks, if applicable
  - Official checks, including cashier 's checks, teller 's checks, and treasurer 's checks (i.e., those guaranteed by your institution and drawn on your institution 's account)
  - Checks presented to your institution as paying bank but were 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)

Do not include:

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

► **Example:** Sarah, your customer, wrote a check for $57 to pay her water bill. The water company is also a client of your institution, and they wrote a check to their power company for $2,000. In this example, you would report 2 checks with a value of $2,057 in item **6** above, 1 check with a value of $57 for item **6.a** below, and 1 check with a value of $2,000 in item **6.b** below.

6.a From consumer accounts

All checks paid from consumer accounts of any kind. Please see the **GENERAL TERMINOLOGY** section above for the definition of consumer accounts.

Include:

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

Do not include:

- Checks paid from business/government accounts

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

6.b From business/government accounts

All checks paid from business/government accounts of any kind. Please see the **GENERAL TERMINOLOGY** section above for the definition of business/government accounts.

Include:

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

Do not include:

- Checks paid from consumer accounts

► **Example:** Your corporate customer, Joe 's Shoes, wrote a check for $3,000 to one of his suppliers. In this example, you would report 1 check for $3,000.

7. Third-party fraudulent checks drawn on your institution

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

Include:

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

Do not include:

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

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

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

CHECK DEPOSITS

Checks deposited with and collected by your institution. Your customer is the beneficiary.

8. Total checks deposited at your institution = 8.a + 8.b

These include checks that were drawn on your institution (i.e., "on-us" checks for which your institution was the "bank of first deposit," item **5.b** above, "on-us" checks deposited by correspondent customers), item **5.a.2** above, and checks drawn on other depository institutions (i.e., transit checks), which are not measured in this questionnaire as a discrete question.

Include:

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

► **Example 1:** A customer deposited a check by using your institution 's app on his smartphone for $100. Another customer walked into one of your institution 's branches and deposited a check for $250. In this example, both types of checks would be included for a total of two deposits in the amount of $350.

► **Example 2:** Multiple local retailers have a depository relationship with your institution. These retailers received checks from their customers. Some of the retailers scanned and captured images of these checks for deposit. Others delivered paper checks to your institution for deposit. In this example, both types of checks would be included.

8.a Checks deposited by non-depository institutions = 8.a.1 + 8.a.2

Checks deposited at your institution by consumers, businesses, or government entities.

Do not include:

- Checks deposited by depository institution customers (i.e., respondent banks) as part of a correspondent customer relationship

► **Example 1:** Mike wrote a check to pay his physician. Mike may or may not have a depository relationship with your institution. The physician 's office, which has a depository relationship with your institution, deposited the check at your local branch. You were the bank of first deposit for this check.

► **Example 2:** Grace wrote a check to pay her babysitter. Grace may or may not have a depository relationship with your institution. The babysitter, who has a depository relationship with your institution, deposited the check into his account electronically by capturing an image of the check with his smartphone and sending the image to your institution. You were the bank of first deposit for this check.

8.a.1 Image deposits

Checks deposited by means of the accountholders capturing and transmitting an image of each check for deposit. These accountholders can be consumers, businesses, or government entities, The paper check was truncated by the accountholder at the point of capture/deposit and your institution is the bank of first deposit.

Do not include:

- Paper check deposits
- Deposited checks for which your institution performed image capture at a branch, ATM, or other processing center

► **Example 1:** Kevin wrote a check to purchase a TV at a local electronics store. Kevin may or may not have a depository relationship with your institution. The electronics store, which has a depository relationship with your institution, captured the image of the check and transmitted the image to your institution for deposit. You were the bank of first deposit for this check.

► **Example 2:** Grace wrote a check to pay her babysitter. Grace may or may not have a depository relationship with your institution. The babysitter, who has a depository relationship with your institution, deposited the check into his account electronically by capturing an image of the check with his smartphone and sending the image to your institution. You were the bank of first deposit for this check.

8.a.2 All other deposits

Paper checks deposited at your institution by consumers, businesses, or government entities. These checks can be received from several deposit channels (e.g., branch, lockbox). Include deposited checks for which your institution performed image capture at a branch, ATM, or other processing center.

Do not include:

- Checks deposited as images
- ACH check conversion entries
- Correspondent check deposits

► **Example:** Your customer deposited his paycheck drawn on an unaffiliated depository institution at an ATM located at your branch. The ATM captured an image of the check, which was truncated at that time. The image was cleared via image exchange. Because the check was deposited at the ATM as paper, it should be reported here and not in item **8.a.1** above)

8.b Checks deposited by depository institution customers (correspondent check deposits)

Checks deposited by a correspondent customer (i.e., a depository institution) either as paper or image.

Do not include:

- Deposits made by consumer or business/government depositors
- ACH check conversion entries

► **Example 1:** Amanda wrote a check to pay her babysitter. The babysitter deposited the check at a depository institution, which happened to be your correspondent customer. As a correspondent bank, your institution holds balances for this depository institution in a due-to account and performs check clearing services on its behalf. This depository institution captured an image of the check and deposited it via image cash letter transmission to your institution for processing. Amanda may or may not be an accountholder at your institution (i.e., you may or may not be the paying bank for this item).

► **Example 2:** Your institution processes checks for another institution as part of a correspondent banking relationship. This institution takes in paper check deposits at its branches. In order to clear those paper checks, your correspondent customer deposited them at your institution in a paper cash letter for subsequent processing.

9. Third-party fraudulent checks deposited at your institution

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

Include:

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

Do not include:

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

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

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

OUTGOING RETURNS

All checks received for payment by your institution that were returned unpaid.

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

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

Include:

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

Do not include:

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

► **Example:** Your customer wrote a check for $98 that was deposited (at your institution or another) and presented for payment. Your customer 's account had insufficient funds and no overdraft protection. Your institution returned the check unpaid. In this example, you would report 1 check with a value of $98.

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

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

Include:

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

Do not include:

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

► **Example:** Your customer wrote a check for $98 that was deposited at another institution and presented for payment. Your customer 's account had insufficient funds and no overdraft protection. Your institution returned the check unpaid to the collecting institution. In this example, you would report 1 check with a value of $98.

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

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

Include:

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

Do not include:

- Checks your institution returned unpaid to another institution

► **Example:** Your customer wrote a check for $200 that was deposited at your institution and presented for payment. Your customer 's account had insufficient funds and no overdraft protection. Your institution returned the check unpaid to your accountholder. In this example, you would report 1 check with a value of $200.

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

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

Include:

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

Do not include:

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

► **Example:** Your customer wrote a check for $98 that was deposited (at your institution or another) and presented for payment. Your customer 's account had insufficient funds and no overdraft protection. Your institution returned the check unpaid. In this example, you would report 1 check with a value of $98.

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

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

Include:

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

Do not include:

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

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

11.a.1 Remotely created checks

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

Include:

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

Do not include:

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

► **Example:** Sam is an accountholder at your institution, and his mobile banking account was hacked. The perpetrator created a check remotely for $2,000 from Sam 's account, which your institution did not pay per Sam 's instructions to stop all check payments from his account due to his account being hacked. In this example, you would report 1 transaction for $2,000.

11.a.2 Forgery/suspected forgery

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

Include:

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

Do not include:

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

► **Example:** Joe is an accountholder at your institution, and his checkbook was stolen. The perpetrator wrote a check for $3,000 from Joe 's checkbook, which your institution did not pay due to suspected forgery on the check. In this example, you would report 1 transaction for $3,000.

11.a.3 Other unauthorized

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

Include:

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

Do not include:

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

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

11.b Nonsufficient funds

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

Include:

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

Do not include:

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

► **Example:** Your customer wrote a check for $98 that was deposited (at your institution or another) and presented for payment. Your customer 's account had insufficient funds and no overdraft protection. Your institution returned the check unpaid. In this example, you would report 1 check with a value of $98.

11.c Duplicate presentment

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

Include:

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

Do not include:

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

► **Example:** Your customer wrote a check for $150 that was deposited (at your institution or another) and presented for payment. This was erroneously presented twice at the collecting institution, for a total of two checks for a total of $300. Your institution returned the duplicate check unpaid. In this example, you would report 1 check with a value of $150.

11.d Other (including administrative returns)

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

Include:

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

Do not include:

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

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

ACH

GENERAL TERMINOLOGY

Your institution

"Your institution" refers to the participating depository institution at its highest organizational level (i.e., holding company, if applicable), including all affiliates. Only report data associated with your institution 's U.S. domiciled accounts (i.e., those accounts located within the 50 U.S. states, D.C., or U.S. territories such as Guam, Puerto Rico, or U.S. Virgin Islands), including both domestic and cross-border transactions.

ACH entries

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

ACH entries include…	ACH entries do not include…
▪ Debits received and credits sent ▪ Debits originated and credits received ▪ Direct exchange ▪ On-us entries ▪ Network entries ▪ Entries that were subsequently returned (outgoing)	▪ Addenda records ▪ Zero-dollar items (e.g., NOCs, Prenotes) ▪ Deletes/reversals

Originating Depository Financial Institution (ODFI)

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

Receiving Depository Financial Institution (RDFI)

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

Network ACH entry

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

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

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

Direct Exchange ACH entry

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

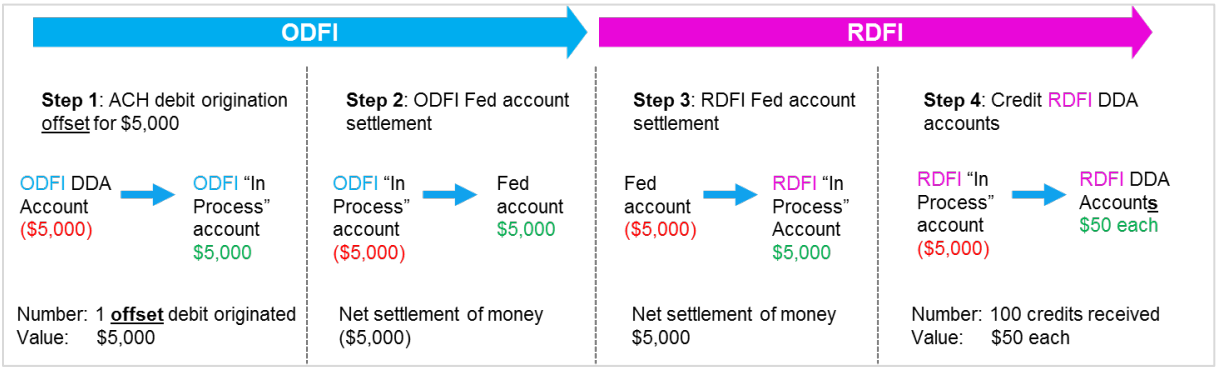
Offset ACH entry

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

Using the example above, if a business account at your institution pays payroll to 100 employees for $50 each (ODFI credit origination), this payment generates 100 credit originations for a total of $5,000. The offset transaction is 1 debit origination for a total of $5,000. The number of offset transactions may vary depending on the institution. Some institutions might do a one-to-one offset transaction per payment origination.

Example assumptions

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



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

Balanced file

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

Unbalanced file

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

Same-day ACH entry

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

Account type definitions

Consumer account

A transaction deposit or savings account for personal use by an individual or household from which ACH payments can be made.

Business/government account

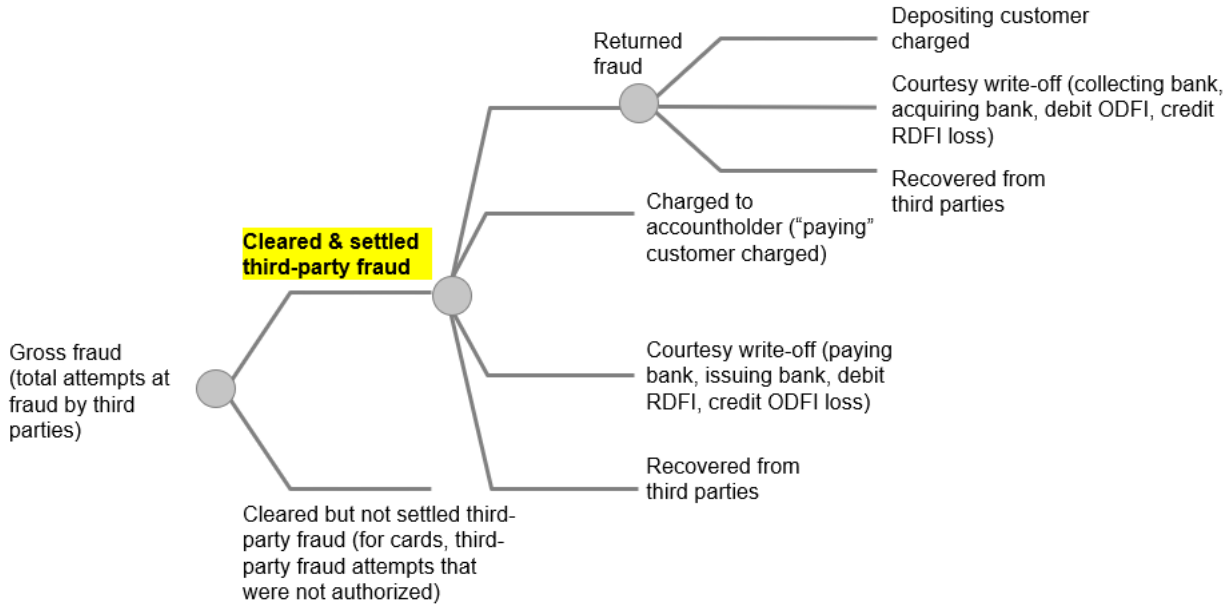
A transaction deposit or savings account owned by an organization (i.e., business, government, non-depository financial institution, or not-for-profit organization) from which ACH payments can be made.

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

Third-party fraud

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

include a loss to various entities but constitutes a fraud attempt that manages to create a funds transfer, if only temporary. The definition is depicted below within the hierarchy of fraud attempts visible to your institution. The definition of fraud in this study is highlighted in yellow to show that cleared and settled third-party fraud includes at least six different categories of fraud outcomes.



SURVEY ITEMS

ACH PROFILE

1. Did your institution post transactions from other payment instruments to your Demand Deposit Account (DDA) system using your ACH platform during calendar year 2021?

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

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

2. Did your institution originate forward ACH credits (not including returns or offset entries) during calendar year 2021?

Some institutions refer to forward originations as "live items." 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**, **7**, **8**, and **9** and their subsets below.

3. Did your institution originate forward ACH debits (not including returns or offset entries) during calendar year 2021?

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

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

4. Did your institution originate offset ACH debit or credit entries during calendar year 2021?

An offset ACH entry is an on-us entry used to effect settlement by an originating depository financial institution (ODFI). For example, when acting as ODFI for one hundred credit entries for $1,000 each for a corporate accountholder, an ODFI might originate a single $100,000 debit entry to draw funds from the originator 's funding account. In most cases, institutions offset (or move) the funds from the accountholder 's DDA to an "in process" account before the funds are settled with the Fed, EPN, or internally. If your answer is "No," please report "Not applicable" for items **4.a** and **4.b** below.

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

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

Even if you are not able to exclude all offset volumes from balanced files, please report the number and value of your institution 's forward ACH entries and third-party fraud for all items below.

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

Even if you are not able to exclude all offset volumes from unbalanced files, please report the number and value of your institution 's forward ACH entries and third-party fraud for all items below.

5. Did your institution offer same-day settlement of ACH credit originations during calendar year 2021?

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

ACH ORIGINATIONS

Your institution is the originating depository financial institution (ODFI).

Originating Depository Financial Institution (ODFI)

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

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

CREDIT ENTRIES ORIGINATED

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

Your customer is the payer.

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

Include:

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

Do not include:

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

► **Example:** Your corporate customer paid 15 of its employees $300 each electronically through the ACH network. Ten of these employees have deposit accounts at your institution. To credit those ten employees ' accounts, your institution originated in-house on-us credit entries. Your institution originated the credit entries on behalf of your customer for the five employees that do not have a deposit account at your institution and sent them through your chosen network operator (i.e., the Federal Reserve or EPN). In this example, you would report 15 transactions for $4,500.

6.a Network

Network ACH entries: A network ACH entry is one that is cleared through a network operator (i.e., the Federal Reserve or EPN). Please consider all network ACH entries, including network on-us ACH entries (those for which your institution is both the ODFI and the receiving depository financial institution (RDFI)) and volume sent or received by a correspondent bank on behalf of your institution via a network operator.

Include:

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

Do not include:

- ACH entries cleared directly between your institution and another (i.e., direct exchange ACH entries)

► **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 Federal Reserve or EPN). In this example, you would report 5 transactions for $2,500.

6.b In-house on-us

In-house on-us ACH entries: 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 Federal Reserve or EPN), for clearing or settlement. In-house on-us entries result in the movement of funds from one account to another within your institution.

Include:

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

Do not include:

- 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 these employees have deposit accounts at your institution. To credit those 10 employees ' accounts, your institution originated in-house on-us credit entries. In this example, you would report 10 transactions for $8,000.

6.c Direct exchange

Direct exchange ACH entries: A direct exchange ACH entry is one that is exchanged directly between your institution and another. Some institutions call these "direct send" entries. Direct exchange does not include volume sent or received by a correspondent bank on behalf of your institution. Correspondent volume should be included with Network ACH entries.

Include:

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

Do not include:

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

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

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

Your customer is the payer.

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

Include:

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

Do not include:

- Returns of ACH entries received by your institution
- 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 15 of its employees $300 each electronically through the ACH network. Ten of these employees have deposit accounts at your institution. To credit those ten employees ' accounts, your institution originated in-house on-us credit entries. Your institution originated the credit entries on behalf of your customer for the five employees that do not have a deposit account at your institution and sent them through your chosen network operator (i.e., the Federal Reserve or EPN). In this example, you would report 15 transactions for $4,500.

7.a From consumer accounts

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

Include:

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

Do not include:

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

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

7.b From business/government accounts

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

Include:

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

Do not include:

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

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

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

Your customer is the payer.

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

Include:

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

Do not include:

- Returns of ACH entries received by your institution
- 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 15 of its employees $300 each electronically through the ACH network. 10 of these employees have deposit accounts at your institution. To credit those 10 employees ' accounts, your institution originated in-house on-us credit entries. Your institution originated the credit entries on behalf of your customer for the 5 employees that do not have a deposit account at your institution and sent them through your chosen network operator (i.e., the Federal Reserve or EPN). In this example, you would report 15 transactions for $4,500

8.a Same-day settlement

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

Include:

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

Do not include:

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

► **Example:** Your corporate customer, Sally 's Plumbing, initiated a one-time bill payment for $2,500 to one of its vendors, ABC Supplies, through the ACH network. The vendor does not bank with your institution. Since the payment of this bill was urgent, your customer decided to use the same-day settlement option your institution began offering on September 23, 2016. Since the ACH credit was sent to an unaffiliated institution, your institution sent the ACH entries through a network operator (i.e., the Federal Reserve or EPN). In this example, you would report 1 entry for $2,500.

8.b Non-same-day settlement

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

Include:

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

Do not include:

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

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

9. Forward ACH credit entries your institution originated and identified as third-party payments fraud (fraudulent ODFI credits) = 9.a + 9.b

Your customer is the payer.

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

Include:

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

Do not include:

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

► **Example 1:** A small business accountholder at your institution originated vendor payments via ACH through your online portal. His PC was compromised by malware, and his login credentials were stolen. The perpetrator originated 10 payments for $10,000 each to an account he maintains under a false name. The funds were then made available to the perpetrator 's account after the transactions cleared and settled. One day later, the same perpetrator attempted to initiate 5 more payments of $5,000 each. The accountholder had already alerted your institution to the previous fraud, so your institution put a hold on the account and these funds were never made available to the perpetrator. In this example, you would report 10 transactions for $100,000.

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

9.a Same-day settlement

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

Include:

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

Do not include:

- Fraudulent ACH credit entries originated and settled non-same-day

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

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

9.b Non-same-day settlement

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

Include:

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

Do not include:

- Fraudulent ACH credit entries originated and settled same-day

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

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

DEBIT ENTRIES ORIGINATED

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

Your customer is the payee.

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

Include:

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

Do not include:

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

► **Example:** Your corporate customer billed 10 of its suppliers $100 each electronically through the ACH using your institution as its ODFI. 5 of these employees have deposit accounts at your institution. To debit those 10 employees ' accounts, your institution originated in-house on-us debit entries to avoid clearing fees from the Federal Reserve or EPN. One employee has a deposit account with an institution in which you have a direct exchange relationship. For this employee, your institution originated an ACH debit entry via direct exchange. For the other four employees, your institution originated ACH debit entries through the network. In this example, you would report 10 transactions for $1,000.

11. Forward ACH debit entries your institution originated and identified as third-party payments fraud (fraudulent ODFI debits)

Your customer is the payee.

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

Include:

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

Do not include:

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

► **Example:** Jill is a small business accountholder at your institution. Her PC was compromised by malware, and her login credentials were stolen. The perpetrator originated 10 fake bills for $10,000 each to ten of Jill 's suppliers. The perpetrator maintained control of your client 's account while the transactions cleared and settled, so the funds were made available to him. Two days later, the same perpetrator attempted to initiate 5 more bills of $5,000 each. The accountholder had already alerted your institution to the previous fraud, so your institution put a hold on the account and these funds were never made available to the perpetrator. In this example, you would report 10 transactions for $100,000.

ACH RECEIPTS

Your institution is the receiving depository financial institution (RDFI).

Receiving Depository Financial Institution (RDFI)

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

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

CREDIT ENTRIES RECEIVED

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

Your customer is the payee.

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

Include:

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

Do not include:

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

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

13. Forward ACH credit entries your institution received and identified as third-party payments fraud (fraudulent RDFI credits)

Your customer is the payee.

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

Include:

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

Do not include:

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

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

DEBIT ENTRIES RECEIVED

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

Your customer is the payer.

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

Include:

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

Do not include:

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

► **Example:** Your corporate customer, a cable company, collected monthly payments of $50 from its 30 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 $50 each. In this example, you would report 30 for $1,500.

14.a Network

Network ACH entries: A network ACH entry is one that is cleared through a network operator (i.e., the Federal Reserve or EPN). Please consider all network ACH entries, including those for which your institution is both the ODFI and RDFI (i.e., network on-us ACH entries), and volume sent or received by a correspondent bank on behalf of your institution via a network operator.

Include:

- Network non-offset ACH debit entries received

Do not include:

- ACH entries cleared directly between your institution and another (i.e., direct exchange ACH entries)

► **Example:** Your customer has set up direct debit of his checking account for a recurring, monthly cell phone bill payment of $50. His biller, the cell phone company, originated debit entries through another depository institution (i.e., the ODFI), and your institution received and posted these debit entries to your customer 's account. In this example, you would report 12 transactions for $600.

14.b In-house on-us

In-house on-us ACH entries: 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 Federal Reserve or EPN), for clearing or settlement. In-house on-us entries result in the movement of funds from one account to another within your institution.

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

Include:

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

Do not include:

- In-house on-us credits your institution originated

► **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 to avoid clearing fees from the Federal Reserve or EPN. In this example, you would report 240 transactions for $10,800.

14.c Direct exchange

Direct exchange ACH entries: A direct exchange ACH entry is one that is exchanged directly between your institution and another. Some institutions call these "direct send" entries. Direct exchange does not include volume sent or received by a correspondent bank on behalf of your institution. Correspondent volume should be included with Network ACH entries.

Include:

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

Do not include:

- Debit ACH entries originated
- In-house on-us credit entries your institution originated

► **Example:** A cable company that is not your corporate customer collected monthly payments of $30 from its customers by originating ACH debit entries using a different institution as its ODFI. 10 of those customers bank at your institution. Your institution has established direct exchange relationships with the ODFI to avoid clearing fees from the Federal Reserve or EPN. To debit the accounts of those customers, your institution received debit entries via direct exchange. Please report 120 transactions for $3,600.

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

Your customer is the payer.

Repeat item **14** above. These include all cleared and settled, domestic and cross-border, network, on-us, and direct exchange ACH debit entries for which your institution was the ODFI.

Include:

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

Do not include:

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

► **Example:** Your corporate customer, a cable company, collected monthly payments of $50 from its 30 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 $50 each. In this example, you would report 30 for $1,500.

15.a For consumer accounts

Please refer to the **GENERAL TERMINOLOGY** section above for the definition of consumer accounts.

Include:

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

Do not include:

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

► **Example:** Your consumer customer, Paul, received a bill payment of $500 from his landlord, which was sent electronically through the ACH. Your institution received the debit entry on behalf of Paul. In this example, you would report 1 transaction for $500.

15.b For business/government accounts

Please refer to the **GENERAL TERMINOLOGY** section above for the definition of business/government accounts.

Include:

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

Do not include:

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

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

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

Your customer is the payer.

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

Include:

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

Do not include:

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

► **Example:** Your corporate customer, a cable company, collected monthly payments of $50 from its 30 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 $50. In this example, you would report 30 for $1,500.

16.a Same-day settlement

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

Include:

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

Do not include:

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

► **Example:** Your corporate customer, Mike 's Hardware, received a one-time bill payment for $2,500 from one of its customers, Sally 's Supplies, through the ACH network. Sally 's Supplies does not bank with your institution. Since the payment of this bill was urgent, Sally 's Supplies decided to use the same-day settlement option. In this example, you would report 1 entry for $2,500.

16.b Non-same-day settlement

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

Include:

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

Do not include:

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

► **Example:** Your customer has set up direct debit of his checking account for a recurring, monthly cell phone bill payment of $50. His biller, the cell phone company, originated debit entries through another depository institution (i.e., the ODFI). Your institution received and posted these debit entries to your customer 's account. The settlement of money occurred on a different day than the transmission of the file. In this example, you would report 12 transactions for $600.

17. Forward ACH debit entries your institution received and identified as third-party payments fraud (fraudulent RDFI debits) = 17.a + 17.b

Your customer is the payer.

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

Include:

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

Do not include:

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

► **Example 1:** A fraud originator opened a commercial bank account for a fictitious housecleaning service at another institution. He then originated unauthorized bill payments for hundreds of consumer accounts, 5 of which were at your institution. Each of those accounts was debited once for $200. The received debit ACH transactions cleared and settled with the ODFI. The $1,000 debited from your accountholders was made available to the perpetrator 's account. In this example, you would 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 cleared and settled a day later, but Jim claimed the transaction as fraudulent since he needs the $150 to pay part of his rent. Since this transaction is an example of first-party fraud (false claim of fraud), it should not be included in item **17** above.

17.a Same-day settlement

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

Include:

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

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

17.b Non-same-day settlement

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

Include:

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

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

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

OUTGOING RETURNS

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

These are ACH debit entries that your institution received and were subsequently returned by your institution, the RDFI. Your customer is the payer for the forward debit being returned.

Include:

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

Do not include:

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

► **Example:** Your customer pays his utility bill through the utility company 's website. The utility company 's bank (which may or may not be your institution) originates a debit ACH entry for $86. However, your customer 's account has insufficient funds, and your institution returns the ACH entry unpaid. In this example, you would report 1 transaction for $86.

Wire Transfers

GENERAL TERMINOLOGY

Your institution

"Your institution" refers to the participating depository institution at its highest organizational level (i.e., holding company, if applicable), including all affiliates. Only report data associated with your institution 's U.S. domiciled accounts (i.e., those accounts located within the 50 U.S. states, D.C., or U.S. territories such as Guam, Puerto Rico, or U.S. Virgin Islands), including both domestic and cross-border transactions.

Account type definitions

Consumer account

A transaction deposit or savings account for personal use by an individual or household from which wire payments can be made.

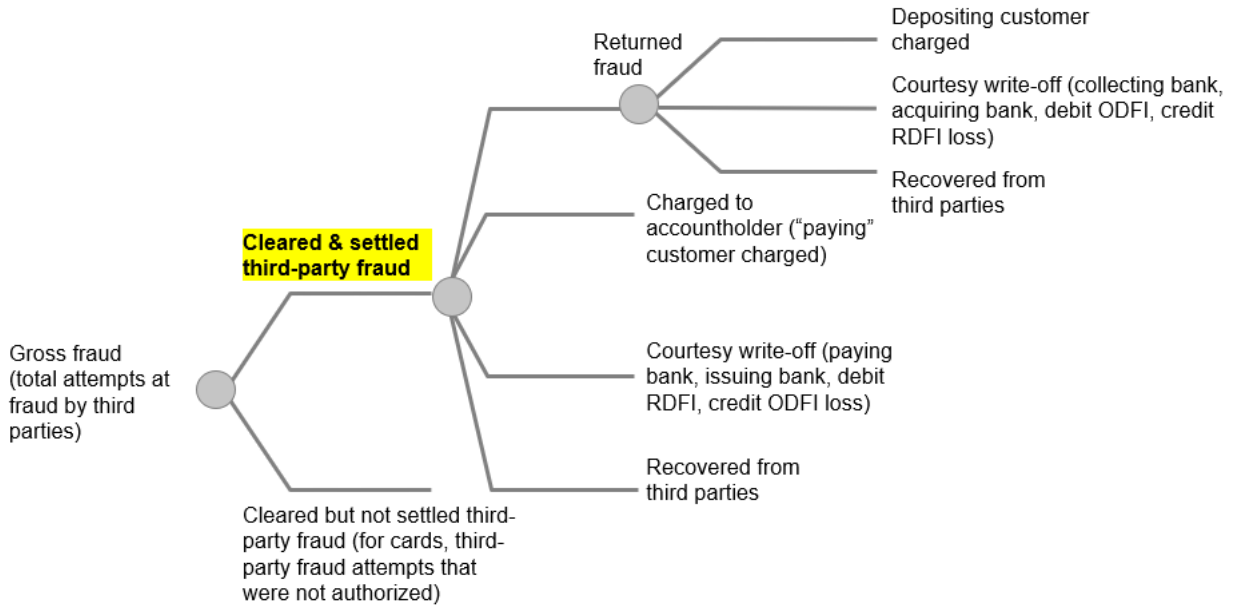
Business/government account

A transaction deposit or savings account owned by an organization (i.e., business, government, non-depository financial institution, or not-for-profit organization) from which wire payments can be made.

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

Third-party fraud

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



SURVEY ITEMS

WIRE TRANSFERS ORIGINATED (OUTGOING)

Your customer is the payer. Include wires for which your institution is the payer (referred to as "settlement/bank business").

1. Did your institution originate wires on behalf of an unaffiliated depository institution during calendar year 2021 (i.e., correspondent volume)?

If your answer to this question is "No," please report "Not applicable" for 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 this section. Even if you are unable to exclude these volumes, please report all wires originated by your institution below.

2. Did an unaffiliated depository institution originate wires on behalf of your institution during calendar year 2021?

If your answer to this question is "No," please report "Not applicable" for item **2.a** below.

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

If your answer is "Yes, in some cases," please explain in the comments box at the end of this section. Even if you are unable to include these volumes, please report all wires originated by your institution below.

3. Total wire transfer originations (outgoing) = Error! Reference source not found. + Error! Reference source not found.

These include all cleared and settled, domestic and cross-border wire transfers originated by your institution 's U.S. domiciled accountholders with either a domestic or foreign beneficiary.

Include:

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

Do not include:

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

► **Example:** Your institution originated a $15,000 wire transfer on behalf of your corporate customer to pay its third-party vendor via Fedwire. The vendor may or may not have a depository relationship with your institution. The vendor may or may not have a U.S. domiciled account. In this example, you would report 1 transaction for $15,000.

3.a From consumer accounts

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

Include:

- Wire transfers originated from consumer accounts of any type

Do not include:

- Wire transfers originated from business/government accounts

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

► **Example:** Your institution originated a wire transfer for $10,000 on behalf of your consumer customer to pay his daughter 's college tuition. Your institution originated the wire on behalf of your customer to the school to fund his daughter 's college tuition via Fedwire. The school may or may not have a depository relationship with your institution. The school may or may not have a U.S. domiciled account. In this example, you would report 1 transaction for $10,000.

3.b From business/government accounts = 3.b.1 + 3.b.2

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

Include:

- Wire transfers originated from business/government accounts

Do not include:

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

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

3.b.1 Settlement/bank business

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

Include:

- Settlement/bank business wire transfers

Do not include:

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

► **Example:** Your institution originated a wire transfer of $12,000 via Fedwire to pay the bank 's advertising agency. In this example, you would report 1 wire transaction for $12,000.

3.b.2 All other business/government

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

Include:

- Wire transfers originated from business/government accounts.

Do not include:

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

► **Example:** Your institution originated a wire transfer of $5,000 on behalf of your corporate customer to pay its third-party vendor via Fedwire. The vendor may or may not have a depository relationship with your institution. The vendor may or may not have a U.S. domiciled account. In this example, you would report 1 wire transaction for $5,000.

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

Repeat item **3** above. These include all cleared and settled, domestic and cross-border wire transfers originated by your institution 's U.S. domiciled accountholders with either a domestic or foreign beneficiary.

Include:

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

Do not include:

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

► **Example:** Your institution originated a $15,000 wire transfer on behalf of your corporate customer to pay its third-party vendor via Fedwire. The vendor may or may not have a depository relationship with your institution. The vendor may or may not have a U.S. domiciled account. In this example, you would report 1 transaction for $15,000.

4.a Domestic (U.S.) payee

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

Include:

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

Do not include:

- Wire transfers sent to a foreign payee

► **Example:** Your institution originated a wire transfer for $10,000 on behalf of your New York based corporate customer to pay its third-party vendor, also located in New York, via Fedwire. Your client is a U.S. domiciled accountholder. In this example, you would report 1 transaction for $10,000.

4.b Foreign payee

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

Include:

- Wire transfers sent to a foreign payee

Do not include:

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

► **Example:** Your institution originated a wire transfer for $10,000 on behalf of your New York based corporate customer to pay its third-party vendor, located in Spain, via Fedwire. Your client is a U.S. domiciled accountholder. In this example, you would report 1 transaction for $10,000.

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

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

Include:

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

Do not include:

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

► **Example:** Your institution originated a $15,000 wire transfer on behalf of your corporate customer to pay its third-party vendor via Fedwire. The vendor may or may not have a depository relationship with your

institution. The vendor may or may not have a U.S. domiciled account. In this example, you would report 1 transaction for $15,000.

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

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

Include:

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

Do not include:

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

► **Example:** Your institution originated a wire transfer for $10,000 on behalf of your corporate customer to pay its third-party vendor via Fedwire. The vendor does not have a depository relationship with your institution. In this example, you would report 1 transaction for $10,000.

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

These are internal wire transfers that were made using your wire platform.

Include:

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

Do not include:

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

► **Example:** Your corporate customer has multiple accounts at your institution, and your institution allows this customer to transfer money among these accounts as a service. These wires are sent over your internal wire platform rather than over a network. Your customer made a wire transfer of $25,000 through your institution 's wire platform for this purpose. In this example, you would report 1 wire transaction for $25,000.

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

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

Include:

- Cleared and settled third-party 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. A fraudulent "on-us" wire transfer is considered cleared and settled if funds were made available to the receiving accountholder
- Fraudulent book transfers (i.e., internal transfers using your institution 's wire platform)

Do not include:

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

► **Example 1:** A small business accountholder at your institution originated a wire payment through your online portal. His PC was compromised by malware, and his login credentials were stolen. The perpetrator originated a wire for $5,000 to an account at your institution and a wire for $10,000 to an account at another institution, both of which accounts were maintained under a false name. The transactions cleared and settled, and the funds became available to the perpetrator. One day later, the same perpetrator attempted to initiate another wire payment of $5,000 to an account at your institution. The small business accountholder had already alerted your institution to the previous fraud, so your institution put a hold on the account and these funds were never made available to the perpetrator. In this example, you would report 2 transactions for $15,000.

► **Example 2:** Jennifer, a small business accountholder at your institution, originated a wire payment of $40,000 to her brother through your online portal. After a heated conversation with her brother, Jennifer decided to recover the money that had been transferred to him. She opened a fraudulent claim with your institution, stating that her brother had logged in to her account and made the wire transfer to his account without her consent. Your institution was able to verify that this was a false, fraudulent claim and that there

was no wrongdoing in the transfer of funds. Since this transaction is an example of first-party fraud (false claim of fraud), it should not be included in item **6** above.

6.a Domestic (U.S) payee

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

Include:

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

Do not include:

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

► **Example:** John is an accountholder at your institution. His email was hacked, and the perpetrator used his username and password to login to his bank account. The perpetrator originated a wire transfer for $5,000 to a second account in New York maintained under a false name, which subsequently cleared and settled in the perpetrator 's account. A transfer of funds occurred between the originating and receiving accounts. The receiving account was with an unaffiliated institution. In this example, you would report 1 transaction for $5,000.

6.b Foreign payee

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

Include:

- Fraudulent wire transfers sent to a foreign payee

Do not include:

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

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

WIRE TRANSFERS RECEIVED (INCOMING)

Your customer is the payee. Include wires received for which your institution is the payee.

7. Did your institution receive wires on behalf of an unaffiliated depository institution during calendar year 2021 (i.e., correspondent volume)?

If your answer to this question is "No," please report "Not applicable" for item **7.a** below.

7.a If your answer is "Yes" to item 7 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 this section. Even if you are unable to exclude these volumes, please report all wires originated by your institution below.

8. Did an unaffiliated depository institution receive wires on behalf of your institution during calendar year 2021?

If your answer to this question is "No," please report "Not applicable" for item **8.a** below.

8.a If your answer is "Yes" to item 8 above, are you able to include these volumes in your answers below?

If your answer is "Yes, in some cases," please explain in the comments box at the end of this section. Even if you are unable to include these volumes, please report all wires originated by your institution below.

9. Total wire transfer receipts (incoming)

All wire transfers received by your institution which were sent through a network or a correspondent bank, as well as internal book transfers (i.e., internal transfers using your institution 's wire platform).

Include:

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

Do not include:

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

► **Example:** Your institution received a $3,000 wire transfer on behalf of your corporate customer, Sam 's Grocery, from their client via Fedwire. Sam 's Grocery 's client may or may not have a depository relationship with your institution, and they may or may not have a U.S. domiciled account. In this example, you would report 1 wire transaction for $3,000.

10. Third-party fraudulent wire transfer receipts (incoming)

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

Include:

- Cleared and settled third-party fraudulent funds transfers received using the large-value systems (i.e., Fedwire and CHIPS), including those originated on your institution 's behalf by a correspondent. A fraudulent "on-us" wire transfer is considered cleared and settled if funds were made available to the receiving accountholder

Do not include:

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

► **Example:** A hacker compromised Joe 's PC by malware and stole his login credentials. The perpetrator originated a wire for $10,000 to an account at your institution, which was maintained under a false name. The transaction cleared and settled, and the funds became available to the perpetrator. Joe alerted his institution of the fraudulent transaction, and they subsequently reached out to your institution for a return of the fraudulent wire payment. In this example, you would report 1 transaction for $10,000.

Debit and General-Purpose Prepaid Cards

Note: For brevity, we will refer to "general-purpose non-prepaid debit cards" as "debit cards" and "general-purpose prepaid debit cards" as "prepaid cards" in the glossary and the questionnaire. This section covers debit card payments from typical transaction or "checking" accounts, and general-purpose or "network-branded" prepaid card payments from prepaid card program accounts held by your institution.

GENERAL TERMINOLOGY

Your institution

"Your institution" refers to the participating depository institution at its highest organizational level (i.e., holding company, if applicable), including all affiliates. Only report data associated with your institution 's U.S. domiciled accounts (i.e., those accounts located within the 50 U.S. states, D.C., or U.S. territories such as Guam, Puerto Rico, or U.S. Virgin Islands), including both domestic and cross-border transactions.

Average of Monthly Totals

For the average of monthly totals calculations, please sum the number or balance of accounts at the end of each month and then divide by 12.

	Account 1		Account 2		Account 3		Sum	
	Account Open	End-of-Month Balance	Account Open	End-of-Month Balance	Account Open	End-of-Month Balance	Number of Open Accounts	Sum of End-of-Month Balances
Jan	Yes	$2,726	Yes	$497	No	Not Applicable	2	$3,223
Feb	Yes	$2,196	Yes	$418	No	Not Applicable	2	$2,614
Mar	Yes	$2,706	Yes	$226	No	Not Applicable	2	$2,932
Apr	Yes	$1,553	Yes	$267	No	Not Applicable	2	$1,820
May	Yes	$2,735	Yes	$397	No	Not Applicable	2	$3,132
Jun	Yes	$2,899	Yes	$550	No	Not Applicable	2	$3,449
Jul	Yes	$2,213	Yes	$176	No	Not Applicable	2	$2,389
Aug	Yes	$2,933	Yes	$685	No	Not Applicable	2	$3,618
Sep	Yes	$2,853	Yes	$723	Yes	$8,660	3	$12,236
Oct	Yes	$2,352	Yes	$704	Yes	$9,329	3	$12,385
Nov	Yes	$2,730	Yes	$0	Yes	$9,994	3	$12,724
Dec	Yes	$1,664	Yes	$0	Yes	$9,015	3	$10,679
Sum							28	$71,201
							Divide by 12 months and round to nearest whole number	Divide by 12
Report Average							**2 accounts**	**$5,933 in balances**

Debit card transactions

Includes all transactions made with debit cards via any debit card network (details below) and associated with non-prepaid accounts held by your institution reported in question 3.b of the *Institution Profile* section of this survey. (Prepaid card transactions are defined below.) Most debit cards are capable of being processed through a dual-message network as well as one or more single-message networks. Includes cash-back transactions at the point of sale but does not include cash withdrawals (typically from an automated teller machine (ATM) or over the counter at a bank branch). Transactions may originate at a physical point of sale or remotely such as via mail order, telephone order, or online, such as through e-commerce or bill pay sites via an app or web browser. For this study, please follow these guidelines:

Debit card transactions include…	**Debit card transactions do not include…**
▪ Transactions made with Visa, MasterCard, Discover, or American Express branded cards and cleared over dual-message networks. These are	▪ ATM withdrawals ▪ Credit card transactions ▪ Prepaid card transactions

Debit card transactions include…	Debit card transactions do not include…
typically called signature-based or offline debit card transactions. ▪ Transactions made with debit cards and cleared over a general-purpose single-message network. Transactions originated in other countries with debit cards issued from U.S. domiciled accounts ▪ Debit card cash-back transactions at the point of sale	▪ Transfers by a corporate customer to fund its employees ' payroll card accounts ▪ Electronic Benefits Transfer (EBT) card transactions made using a proprietary network (e.g., Quest network) for that purpose ▪ Payroll card transactions by the cardholder

Prepaid card transactions

Prepaid card transactions are the portion of debit card transactions associated with prepaid debit card accounts held by your institution and reported in question 3.a of the *Institution Profile* section of this survey. Include all transactions made with network-branded prepaid "open-loop" prepaid cards. Most prepaid cards are capable of being processed through a dual-message network as well as one or more single-message networks. Includes cash-back transactions at the point of sale but does not include cash withdrawals (typically from an automated teller machine (ATM) or over the counter at a bank branch). Transactions may originate at a physical point of sale or remotely such as via mail order, telephone order, or online, such as through e-commerce or bill pay sites via an app or web browser. For this study, please follow these guidelines:

Prepaid card transactions include…	Prepaid card transactions do not include…
▪ Transactions made with Visa, MasterCard, Discover, or American Express branded prepaid cards and cleared over dual-message networks ▪ Transactions made with prepaid cards and cleared over a general-purpose, single-message network ▪ Transactions made in other countries with prepaid cards issued from U.S. domiciled accounts ▪ Open-loop general-purpose prepaid card transactions ▪ Open-loop gift card transactions ▪ Payroll card transactions by the cardholder ▪ FSA/HSA prepaid medical cards ▪ Customer refund and incentive prepaid cards ▪ Prepaid card cash-back transactions at the point of sale	▪ Closed-loop prepaid card transactions ▪ ATM withdrawals ▪ Debit card transactions ▪ Credit card transactions ▪ Transfers by a corporate customer to fund its employees ' payroll card accounts ▪ Electronic Benefits Transfer (EBT) card transactions made using a proprietary network (e.g., Quest network) for that purpose

Digital wallet

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

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

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

General-purpose prepaid card

Since general-purpose and prepaid cards function similarly to debit cards and use the same "rails" to process payments, they are distinguished from debit cards primarily by the way your institution classifies the associated transaction account. Functionality of prepaid card program accounts is typically limited to "loading" funds and spending with the card. These cards are often marketed as gift cards or offered to underbanked consumers as a

checking account alternative. Some prepaid cards, such as payroll and medical benefits cards, are sponsored by businesses as a way of transferring funds to consumers.

Prepaid card payments processed via network-branded card networks are called "general-purpose prepaid card payments" to distinguish them from private-label, or "closed loop," prepaid cards, which should not be included in reported volumes. Debit cards are, by design, general-purpose or "open loop" and do not have a corresponding private-label or "closed loop" counterpart to prepaid cards.

Virtual card

Virtual cards are used for online or over the phone purchases and do not require the accountholder to have a physical card. Virtual cards may provide greater security than a physical card because they use a unique card number, expiration date, and security code that is only valid at specific merchants or for a specific amount of time. Virtual cards may be issued for single or multiple transaction use, and they may or may not be loaded to digital wallets.

Contactless card

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

Account type definitions

Consumer account

A transaction deposit or savings account for personal use by an individual or household from which payments can be made.

Business/government account

A transaction deposit or savings account owned by an organization (i.e., business, government, non-depository financial institution, or not-for-profit organization) from which payments can be made.

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

Open-loop prepaid cards

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

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

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

Closed-loop prepaid cards

Closed-loop prepaid cards are excluded from this survey. Include only transactions with open-loop prepaid cards in this survey.

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

Reloadable prepaid cards

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

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

Gift cards

Prepaid cards that are marketed as gift-giving alternatives to cash, checks, and gift certificates or as loyalty cards with payment capabilities. Include non-reloadable network-branded general-purpose open-loop prepaid cards in reported totals. Do not include closed-loop prepaid cards that are typically merchant or shopping center branded.

Payroll cards

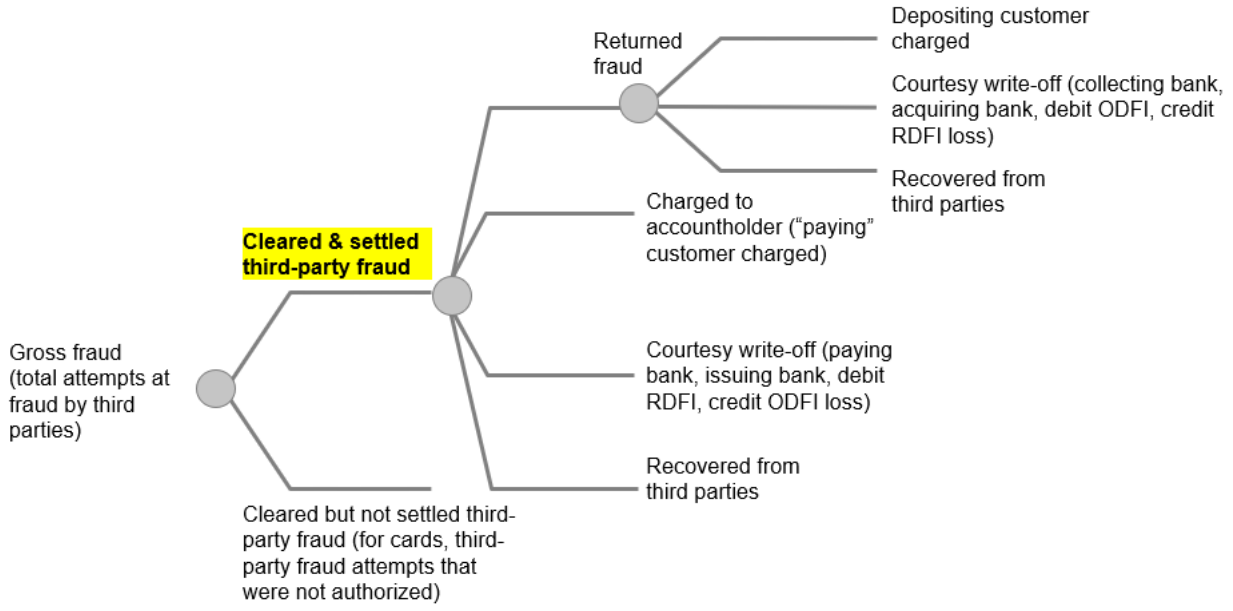
Reloadable, prepaid "ATM" cards issued to disburse employee wages; typically marketed as a means to replace paper check or cash wages to unbanked employees.

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

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

Third-party fraud

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



SURVEY ITEMS

Your institution is the issuer. Your customer is the payer, accountholder, or cardholder.

1. Did your institution have debit cards in circulation in 2021 for which your institution was the issuer?

An issuing bank issues the card, holds the accounts from which payments are drawn, and is responsible for paying the acquiring bank. Also include cards issued by your institution that are managed by a third-party, and for which your institution routes transactions over a general-use debit card network. If your answer to this question is "No," please report "0" for items **5.a** and its subsets, and **6.a** and its subsets below.

Include:

- Debit cards associated with transaction deposit accounts reported item **3.b** in the Institution Profile section
- Debit cards (not including prepaid cards) that can be used to make purchases at the point of sale

Do not include:

- ATM-only cards, prepaid cards, credit cards, or EBT cards

2. Did your institution offer its customers general-purpose prepaid cards issued by another financial institution during calendar year 2021?

General-purpose prepaid cards include but are not limited to: payroll prepaid cards, open-loop gift cards, government-administered open-loop prepaid cards, FSA/HSA medical cards, and open-loop customer refund and incentive cards. If your answer is "Yes," please exclude these volumes from all items below.

2.a If your answer is "Yes" to item 2 above, are you able to exclude card counts and transaction volume data from general-purpose prepaid cards issued by another financial institution from your answers below?

3. Did your institution have general-purpose prepaid cards in circulation in 2021 for which your institution was the issuer?

An issuing bank issues the card, holds the account from which payments are drawn, and is responsible for paying the acquiring bank for debit card payments. Also include cards issued for prepaid card programs managed by your institution or managed by a third-party and that route transactions over a debit card network. If your answer to this question is "No," please report "Not applicable" for item **3.a**, and "0" for items **5.b** and **6.b** and their subsets below.

Include:

- General-purpose repaid cards associated with transaction deposit accounts reported in item **3.a** of the Institution Profile section
- Types of general-purpose prepaid cards:
  - Consumer and business/government general-purpose open-loop reloadable prepaid cards. Examples of reloadable prepaid cards include payroll prepaid cards, FSA/HSA medical cards, open-loop gift cards, and government-administered open-loop gift cards
  - Consumer and business/government general-purpose open-loop non-reloadable prepaid cards. Examples of non-reloadable prepaid cards include open-loop customer refund and incentive cards, open-loop gift cards, and government-administered open-loop gift cards

Do not include:

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

3.a If your answer is "Yes" to item 3 above, are you able to include all general-purpose prepaid card counts and transaction volumes (as well as from business/government general-purpose prepaid card programs) in your answers below?

If your answer is "Yes, in some cases," please explain in the comments box at the end of this section. Even if your answer is "No," please report your data for all items below and explain in the comment box at the end of this section.

4. Did your institution provide virtual debit cards or virtual general-purpose prepaid cards as a product/service in 2021 for which your institution was the issuer? (Note: Virtual cards are different from digital wallets.)

Please see the **GENERAL TERMINOLOGY** section above for the definition of virtual cards. If your answer is "Yes," please exclude virtual cards from the counts in item **5** but include virtual card transactions for all items starting with item **6** below.

Include:

- Virtual debit cards associated with transaction deposit accounts reported in the Institution Profile section
- Virtual consumer and business/government general-purpose open-loop reloadable prepaid cards
- Virtual consumer and business/government general-purpose open-loop non-reloadable prepaid cards

Do not include:

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

5. Number of physical debit and general-purpose prepaid cards = 5.a + 5.b

Average of monthly totals means the average of end-of-month totals for each of the months in 2021.

Report debit and general-purpose prepaid cards associated with transaction deposit accounts reported in the Institution Profile section. If your answer is "No" to items **1** and **3** above, please report "0" here.

For cards in force report only debit and general-purpose prepaid cards that can be used at the point of sale, were issued by your institution, activated by your institution 's accountholders, have not expired at the end of a month, and draw on the transaction deposit accounts reported in items **2** and **3** in the Institution Profile section.

For cards in force with purchase activity, report only debit and general-purpose prepaid cards that had at least one point-of-sale (POS) and/or bill payment in a month. Do not include cards that were only used to withdraw cash.

5.a Debit cards = 5.a.1 + 5.a.2

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

Include:

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

Do not include:

- Virtual cards, ATM-only cards, prepaid cards, credit cards, or EBT cards

► **Example:** Your institution has 500 consumer and business banking accounts, with 500 debit cards issued that are related to these accounts at the end of January through July. Of these debit cards, 450 cards have been activated and are not expired, 25 cards have not been activated yet, 20 cards have been activated but are now expired, and 5 are virtual cards. Of the 450 cards that have been activated and are not expired, 350 had purchase activity. In this example, you would report 450 debit cards in force and 350 in force with purchase activity for January through July.

At the end of August through December, your institution had the same number of accounts with debit cards issued to them. Of these debit cards, 480 cards have been activated and are not expired, 10 cards have not been activated yet, 6 cards have been activated but are now expired, and 4 are virtual cards. Of the 480 cards that have been activated and are not expired, 300 had purchase activity. In this example, you would report 480 debit cards in force and 300 in force with purchase activity for August through December.

For the number of cards in force, the calculation is as follows: [(450 cards x 7 months open) + (480 cards x 5 months open)] / 12 months = 463 cards in force

For the number of cards in force with purchase activity, the calculation is as follows: [(350 cards x 7 months open) + (300 cards x 5 months open)] / 12 months = 329 cards in force with purchase activity

5.a.1 Consumer

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

Include:

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

Do not include:

- Virtual cards, ATM-only cards, prepaid cards, credit cards, EBT cards, or any type of business card

► **Example:** Your institution has 400 personal banking accounts, with 400 debit cards issued that are related to these accounts at the end of January through July. Of these debit cards, 350 cards have been activated and are not expired, 25 cards have not been activated yet, 20 cards have been activated but are now expired, and 5 are virtual cards. Of the 350 cards that have been activated and are not expired, 300 had purchase activity. In this example, you would report 350 debit cards in force and 300 in force with purchase activity for January through July.

At the end of August through December, your institution had the same number of accounts with debit cards issued to them. Of these debit cards, 380 cards have been activated and are not expired, 10 cards have not been activated yet, 6 cards have been activated but are now

expired, and 4 are virtual cards. Of the 380 cards that have been activated and are not expired, 200 had purchase activity. In this example, you would report 380 debit cards in force and 200 in force with purchase activity for August through December.

For the number of cards in force, the calculation is as follows: [(350 cards x 7 months open) + (380 cards x 5 months open)] / 12 months = 362 cards in force

For the number of cards in force with purchase activity, the calculation is as follows: [(300 cards x 7 months open) + (200 cards x 5 months open)] / 12 months = 258 cards in force with purchase activity

5.a.2 Business/government

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

Include:

- Debit cards associated with business/government transaction deposit accounts reported in the Institution Profile section

Do not include:

- Virtual cards, ATM-only cards, prepaid cards, credit cards, EBT cards, or any type of consumer card

► **Example:** Your institution has 1,000 business banking accounts, with 1,000 debit cards issued that are related to these accounts at the end of January through July. Of these debit cards, 900 cards have been activated and are not expired, 50 cards have not been activated yet, 40 cards have been activated but are now expired, and 10 are virtual cards. Of the 900 cards that have been activated and are not expired, 700 had purchase activity. In this example, you would report 900 debit cards in force and 700 in force with purchase activity for January through July.

At the end of August through December, your institution had the same number of accounts with debit cards issued to them. Of these debit cards, 950 cards have been activated and are not expired, 25 cards have not been activated yet, 20 cards have been activated but are now expired, and 5 are virtual cards. Of the 950 cards that have been activated and are not expired, 800 had purchase activity. In this example, you would report 950 debit cards in force and 800 in force with purchase activity for August through December.

For the number of cards in force, the calculation is as follows: [(900 cards x 7 months open) + (950 cards x 5 months open)] / 12 months = 921 cards in force

For the number of cards in force with purchase activity, the calculation is as follows: [(700 cards x 7 months open) + (800 cards x 5 months open)] / 12 months = 742 cards in force with purchase activity.

5.b General-purpose prepaid cards = 5.b.1 + 5.b.2

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

Include:

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

Do not include:

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

► **Example:** Your institution has 500 general-purpose open-loop prepaid accounts, with 500 prepaid cards issued that are related to these accounts at the end of January through July. Of these prepaid cards, 450 cards have been activated and are not expired, 25 cards have not been activated yet, 20 cards have been activated but are now expired, and 5 are virtual cards. Of the 450 cards that have been activated and are not expired, 350 had purchase activity. In this example, you would report 450 prepaid cards in force and 350 in force with purchase activity for January through July.

At the end of August through December, your institution had the same number of accounts with prepaid cards issued to them. Of these prepaid cards, 480 cards have been activated and are not expired, 10 cards have not been activated yet, 6 cards have been activated but are now expired, and 4 are virtual cards. Of the 480 cards that have been activated and are not expired, 300 had purchase activity. In this example, you would report 480 prepaid cards in force and 300 in force with purchase activity for August through December.

For the number of cards in force, the calculation is as follows: [(450 cards x 7 months open) + (480 cards x 5 months open)] / 12 months = 463 cards in force

For the number of cards in force with purchase activity, the calculation is as follows: [(350 cards x 7 months open) + (300 cards x 5 months open)] / 12 months = 329 cards in force with purchase activity

5.b.1 Reloadable

These are accounts for reloadable open-loop prepaid cards which may be loaded with money multiple times. Please see the **GENERAL TERMINOLOGY** section above for the definition of reloadable accounts.

► **Example:** Your institution has 400 reloadable general-purpose open-loop prepaid accounts, with 400 prepaid cards issued that are related to these accounts at the end of January through July. Of these prepaid cards, 350 cards have been activated and are not expired, 25 cards have not been activated yet, 20 cards have been activated but are now expired, and 5 are virtual cards. Of the 350 cards that have been activated and are not expired, 300 had purchase activity. In this example, you would report 350 prepaid cards in force and 300 in force with purchase activity for January through July.

At the end of August through December, your institution had the same number of accounts with prepaid cards issued to them. Of these prepaid cards, 380 cards have been activated and are not expired, 10 cards have not been activated yet, 6 cards have been activated but are now expired, and 4 are virtual cards. Of the 380 cards that have been activated and are not expired, 200 had purchase activity. In this example, you would report 380 prepaid cards in force and 200 in force with purchase activity for August through December.

For the number of cards in force, the calculation is as follows: [(350 cards x 7 months open) + (380 cards x 5 months open)] / 12 months = 362 cards in force

For the number of cards in force with purchase activity, the calculation is as follows: [(300 cards x 7 months open) + (200 cards x 5 months open)] / 12 months = 258 cards in force with purchase activity

5.b.2 Non-reloadable

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

► **Example:** Your institution has 1,000 non-reloadable general-purpose open-loop prepaid accounts with 1,000 prepaid cards issued that are related to these accounts at the end of January through July. Of these prepaid cards, 900 cards have been activated and are not expired, 50 cards have not been activated yet, 40 cards have been activated but are now expired, and 10 are virtual cards. Of the 900 cards that have been activated and are not expired, 700 had purchase activity. In this example, you would report 900 prepaid cards in force and 700 in force with purchase activity for January through July.

At the end of August through December, your institution had the same number of accounts with prepaid cards issued to them. Of these prepaid cards, 950 cards have been activated and are not expired, 25 cards have not been activated yet, 20 cards have been activated but are now expired, and 5 are virtual cards. Of the 950 cards that have been activated and are not expired, 800 had purchase activity. In this example, you would report 950 prepaid cards in force and 800 in force with purchase activity for August through December.

For the number of cards in force, the calculation is as follows: [(900 cards x 7 months open) + (950 cards x 5 months open)] / 12 months = 921 cards in force

For the number of cards in force with purchase activity, the calculation is as follows: [(700 cards x 7 months open) + (800 cards x 5 months open)] / 12 months = 742 cards in force with purchase activity

6. Total debit and general-purpose prepaid card transactions = 6.a + 6.b

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

Include:

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

Do not include:

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

► **Example:** Your customer bought $30 of groceries and received $20 cash back with her debit card by entering her PIN at the checkout line, for a transaction total of $50. Later that day, she used her prepaid card issued by your institution to purchase a $70 purse online. Your corporate customer used a virtual debit card to purchase $200 of paper supplies. In this example, you would report three transactions for $320.

6.a Debit card transactions = 6.a.1 + 6.a.2

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

Include:

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

Do not include:

- Prepaid card transactions
- Open-loop gift card transactions
- FSA/HSA medical card transactions
- Customer refund and incentive card transactions

► **Example:** Your customer bought $30 of groceries and received $20 cash back with her debit card by entering her PIN at the checkout line, for a transaction total of $50. Later that day, she used the same debit card issued by your institution to purchase a $350 smart watch online. In this example, you would report two transactions for $400.

6.a.1 From consumer accounts

These include all transactions made by consumer accountholders over any debit card network for which your institution was the issuer. Please see the **GENERAL TERMINOLOGY** section above for the definition of consumer accounts.

Include:

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

Do not include:

- Debit card transactions made by business/government accountholders
- Debit card cash-back transactions at the point of sale by business/government accountholders

► **Example:** Tom used his debit card issued by your institution to buy a $40 pair of jeans. Later that day, he used his debit card at the ATM to withdraw $500. In this example, you would report 1 transaction for $40.

6.a.2 From business/government accounts

These include all transactions made by business/government accountholders over any debit card network for which your institution was the issuer. Please see the **GENERAL TERMINOLOGY** section above for the definition of business/government accounts.

Include:

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

Do not include:

- Debit card transactions made by consumer accountholders
- Debit card cash-back transactions at the point of sale by consumer accountholders

► **Example:** Your corporate accountholder made a purchase of $500 with a corporate debit card issued by your institution. Later that day, he withdrew $200 in cash over the counter at one of your branch locations using the same debit card. In this example, you would report 1 transaction for $500.

6.b General-purpose prepaid card transactions = 6.b.1 + 6.b.2

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

Include:

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

Do not include:

- Debit card transactions

► **Example:** Your customer bought $30 of groceries and received $20 cash back with her prepaid card by entering her PIN at the checkout line, for a transaction total of $50. Later that day, she used the same prepaid card issued by your institution to purchase a $70 jacket at a department store. In this example, you would report 2 transactions for $120.

6.b.1 From reloadable accounts

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

Include:

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

Do not include:

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

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

► **Example:** Before going to the mall, Joe reloaded his prepaid card issued by your institution with $500. At the mall, Joe used his prepaid card to buy a $100 jacket. Later in the week, he used his prepaid card at the ATM to withdraw $200. In this example, you would report 1 transaction for $100.

6.b.2 From non-reloadable accounts

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

Include:

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

Do not include:

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

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

7. Total debit and general-purpose prepaid card transactions (repeat item 6) = 7.a + 7.b

Repeat item **6** above. These include all cleared and settled, domestic and cross-border transactions over any debit or prepaid card network for which your institution was the issuer. Include all point-of-sale or bill-pay transactions made by debit cards or prepaid cards processed over either signature payment card networks or PIN payment card networks. If your answer is "No" to items **1** and **3** above, please report "0" here.

Include:

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

Do not include:

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

► **Example:** Your customer bought $30 of groceries and received $20 cash back with her debit card by entering her PIN at the checkout line, for a transaction total of $50. Later that day, she used her prepaid card issued by your institution to purchase a $70 purse online. Your corporate customer used a virtual debit card to purchase $200 of paper supplies. In this example, you would report two transactions for $320.

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

These include all debit and prepaid card transactions for which the card user is physically present with the card at the point of sale.

Include:

- In-person transactions
- In-person mobile transactions (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)
- In-person contactless card transactions (i.e., "tap and pay" physical cards, fobs, or stickers)
- In-person intermediated transactions (e.g., Square, Clover, Zettle)
- In-person card-not-present transactions (i.e., key-entered transactions)

Do not include:

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

► **Example:** Your customer bought a coat for $100 with his debit card by entering his PIN at the checkout line. Later that day, he bought a $40 train ticket with his prepaid card with his digital wallet (Apple Pay) at the checkout. For this example, you would report 2 transactions for $140.

7.a.1 With a PIN

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

Include:

- In-person transactions authenticated via PIN

Do not include:

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

► **Example:** Your customer bought lunch for $15 with his debit card by entering his PIN at the checkout line. Later that day, he bought a $30 sweater with his prepaid card by signing the receipt at the checkout. In this example, you would report 1 transaction for $15.

7.a.2 Without a PIN

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

Include:

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

Do not include:

- In-person transactions authenticated via PIN
- Remote transactions

► **Example:** Your customer bought lunch for $15 with his debit card by entering his PIN at the checkout line. Later that day, he bought a $30 sweater with his prepaid card by signing the receipt at the checkout. For this example, you would report 1 transaction for $30.

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

These include all 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 with either a domestic or foreign payee.

Include:

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

Do not include:

- In-person transactions
- In-person mobile transactions (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)
- In-person contactless card transactions (i.e., "tap and pay" physical cards, fobs, or stickers)
- In-person intermediated transactions (e.g., Square, Clover, Zettle)
- In-person card-not-present transactions (i.e., key-entered transactions)

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

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

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

Include:

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

Do not include:

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

► **Example:** Your customer purchased a $100 item on a Chinese internet website from a Chinese (foreign) merchant with his debit card by entering his debit card number, name, and address. He then proceeded to buy $70 of groceries from a New York grocery store (U.S.-based merchant) in a mobile application not at the point of sale (in-app transaction), paying with his prepaid card with his digital wallet (Google Pay). In this example, you would report 1 transaction for $70 under item **7.b.1**. [Note that the foreign payee transaction for $100 would be reported under item **7.b.2** below].

7.b.2 Foreign payee

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

Include:

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

Do not include:

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

► **Example:** Your customer purchased a $100 item on a Chinese internet website from a Chinese (foreign) merchant with his debit card by entering his debit card number, name, and address. He then proceeded to buy $70 of groceries from a New York grocery store (U.S.-based merchant) in a mobile application not at the point of sale (in-app transactions), paying with his prepaid card with his digital wallet (Google Pay). In this example, you would report 1 transaction for $100 under item **7.b.2**. [Note that the domestic payee transaction for $70 would be reported under item **7.b.1** above].

8. Total debit and general-purpose prepaid card transactions (repeat item 6) = 8.a + 8.b + 8.c

Repeat item **6** above. These include all cleared and settled, domestic and cross-border transactions over any debit or prepaid card network for which your institution was the issuer. Include all point-of-sale or bill-pay transactions made by debit cards processed over either signature payment card networks or PIN payment card networks. If your answer is "No" to items **1** and **3** above, please report "0" here.

Include:

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

Do not include:

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

► **Example:** Your customer bought $30 of groceries and received $20 cash back with her debit card by entering her PIN at the checkout line, for a transaction total of $50. Later that day, she used the same debit card issued by your institution to purchase a $70 purse online. Your corporate customer used a virtual debit card to purchase $200 of paper supplies. In this example, you would report two transactions for $320.

8.a In-person contactless card transactions

These are all cleared and settled, domestic and cross-border debit and prepaid card transactions made via a contactless card.

Include:

- Transactions for which a physical card or token was "tapped" or "waved" to pay at the POS terminal

Do not include:

- Debit and prepaid card-on-file e-commerce transactions (cardholder-initiated or merchant-initiated) (i.e., installment payment)
- Transactions made via digital wallets

► **Example:** Your customer bought lunch for $15 with his debit card. He physically tapped his card on the POS device to pay for lunch, using NFC technology. He then ordered a $30 dinner in a mobile application, paying with his prepaid card via his digital wallet (Apple Pay). In this example, you would report 1 transaction for $15.

8.b Digital wallet transactions = 8.b.1 + 8.b.2

These are all cleared and settled, domestic and cross-border debit and prepaid card transactions made via a digital wallet, including tokenized digital wallet.

Include:

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

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

Do not include:

- Debit and prepaid card-on-file e-commerce transactions (cardholder-initiated or merchant-initiated) (i.e., installment payment)
- Transactions for which a physical card or token was "tapped" to pay at the POS terminal (i.e., contactless card transaction)

► **Example:** Your customer bought lunch for $10 with his debit card, which was loaded into his digital wallet (Apple Pay). He physically tapped his phone on the POS device to pay for lunch, using NFC technology. He then ordered a $30 dinner in a mobile application, paying with his prepaid card via his digital wallet (Apple Pay). In this example, you would report 2 transactions for $40.

8.b.1 In-person

These include debit and prepaid card transactions for which an electronic device, such as a smartphone, smart watch, or activity tracker, was "tapped" or "waved" to pay at the POS terminal (e.g., Apple Pay, Samsung Pay, Google Pay, Fitbit Pay). Such payments are considered contactless payments, but do not use a physical card or token

Include:

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

Do not include:

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

► **Example:** Your customer bought lunch for $15 with his debit card, which was loaded into his digital wallet (Apple Pay). He physically tapped his phone on the POS device to pay for lunch, using NFC technology. He then bought groceries for $100 with his prepaid card by tapping his card on the POS device. In this example, you would report 1 transaction for $15.

8.b.2 Remote

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

Include:

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

Do not include:

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

► **Example:** Your customer purchased a $500 item on an internet website with his debit card by entering his debit card number, name, and address. He then bought a $65 pair of shoes in a mobile application, paying with the same debit card via his digital wallet (Google Pay). In this example, you would report 1 transaction for $65.

8.c All other transactions

These are all cleared and settled, domestic and cross-border debit and prepaid card transactions made without a contactless card or digital wallet.

Do not include:

- Transactions made via digital wallets
- Transactions for which a physical card or token was "tapped" to pay at the POS terminal

► **Example:** Your customer bought lunch for $10 with his debit card. He physically tapped his card on the POS device to pay for lunch, using NFC technology. He then ordered a $30 dinner in a mobile application, paying with his prepaid card via his digital wallet (Apple Pay). Your customer then bought dessert for $7 using the same debit card by inserting the card in the POS device. In this example, you would report 1 transaction for $7.

9. Third-party fraudulent debit and general-purpose prepaid card transactions = 9.a + 9.b

These include all cleared and settled third-party unauthorized debit and prepaid card network 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 the transaction resulted in a loss of funds. If your answer is "No" to items **1** and **3** above, please report "0" here.

Include:

- Cleared and settled debit card transactions that were not authorized by a valid card user (third-party fraud)
- Cleared and settled 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
- Prepaid card transactions authorized by a valid card user as part of a scam

► **Example 1:** Your accountholder 's debit card issued by your institution was stolen. The perpetrator used the card to make one purchase worth $1,000, which was authorized at the point of sale. The perpetrator attempted to make another purchase worth $500 the next day. Your accountholder had already alerted your institution to the previous fraudulent activity and a hold had been put on her account, so the perpetrator never received funds from the second attempt. In this example, you would report 1 transaction for $1,000.

► **Example 2:** Your accountholder claimed that her debit card was stolen and used to purchase a $500 TV in an electronics store. An investigation by your institution determined that in fact your accountholder made this purchase on her card. Since this transaction is an example of first-party fraud (false claim of fraud), it should not be included in item **7.b.1** above.

9.a In-person transactions = 9.a.1 + 9.a.2

These include only third-party fraudulent debit and prepaid card transactions for which the card user is physically present at the merchant location when card data are acquired. Include digital wallet (Apple Pay, Samsung Pay) transactions at the point of sale only. Please report the total transactions using a PIN and without a PIN.

Include:

- In-person fraudulent transactions

Do not include:

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

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

► **Example 2:** Your accountholder claimed that her debit card was stolen and used to purchase a $500 TV in an electronics store. An investigation by your institution determined that in fact your accountholder made this purchase on her card. Since this transaction is an example of first-party fraud (false claim of fraud), it should not be included in item **1** above.

9.a.1 With a PIN

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

Include:

- Fraudulent in-person transactions authenticated via PIN

Do not include:

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

► **Example:** Your accountholder 's debit card was stolen, and the perpetrator watched her enter her PIN at the point of sale before stealing the card. The perpetrator then used her card and PIN to buy a $200 watch at a jewelry store. He then used the card to buy dinner for $50 at a nearby restaurant by fraudulently signing the receipt. In this example, you would report 1 transaction of $200.

9.a.2 Without a PIN

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

Include:

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

Do not include:

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

► **Example:** Your accountholder 's prepaid card was stolen, and the perpetrator watched her enter her PIN at the point of sale before stealing the card. The perpetrator then used her card and PIN to buy a $200 watch at a jewelry store. He then used the card to buy dinner for $50 at a nearby restaurant by fraudulently signing the receipt. In this example, you would report 1 transaction of $50.

9.b Remote transactions = 9.b.1 + 9.b.2

These include only third-party fraudulent debit and prepaid card transactions for which the card user does not physically present the card to authorize the transaction. Please report any fraudulent third-party debit and prepaid card transactions, regardless of whether the transaction resulted in a loss of funds. Please report the total transactions with either a domestic or foreign payee.

Include:

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

Do not include:

- In-person fraudulent transactions
- Fraudulent in-person mobile transactions (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)
- Fraudulent in-person contactless card transactions (i.e., "tap and pay" physical cards, fobs, or stickers)
- Fraudulent in-person intermediated transactions (e.g., Square, Clover, Zettle)
- Fraudulent in-person card-not-present (i.e., key-entered transactions)

► **Example 1:** Your accountholder 's debit card was stolen. The perpetrator used the card to purchase a TV for $500 at a store by fraudulently signing the receipt. He then proceeded to use the stolen card to buy an item online for $250. Both transactions were authorized. In this example, you would report 1 transaction for $250.

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

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

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

Include:

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

Do not include:

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

► **Example:** Your accountholder 's prepaid card was stolen. The perpetrator used the card to buy a $250 coat online from a French retailer. He then used the card online to buy a $15 book from a U.S. bookstore. In this example, you would report 1 transaction for $15.

9.b.2 Foreign payee

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

Include:

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

Do not include:

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

► **Example:** Your accountholder 's debit card was stolen. The perpetrator used the card to buy a $250 coat online from a French retailer. He then used the card online to buy a $15 book from a U.S. bookstore. In this example, you would report 1 transaction for $250.

10. Total debit and general-purpose prepaid cash-back at the point of sale

These include all cleared and settled, domestic and cross-border debit and prepaid card transactions for which your institution was the card issuer and in which the accountholders received cash back at the point of sale. These include both signature-based cash-back and PIN-based cash-back transactions. For cash-back value, only include the amount of cash your card users received at the point of sale. If your answer is "No" to items **1** and **3** above, please report "0" here.

Include:

- Debit and prepaid card cash-back transactions at the point of sale. For value, only report the cash value ($) portion of the transaction

Do not include:

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

► **Example:** Your customer used her debit card at the grocery store to purchase $50 of food. She entered her PIN to authorize the transaction and also requested $20 cash back. In this example, you would report 1 transaction for $20

General-Purpose Credit Cards

Note: For brevity, we will refer to "non-prepaid debit card" as "debit card" and "prepaid debit card" as "prepaid card" in this glossary.

GENERAL TERMINOLOGY

Your institution

"Your institution" refers to the participating depository institution at its highest organizational level (i.e., holding company, if applicable), including all affiliates. Only report data associated with your institution 's U.S. domiciled accounts (i.e., those accounts located within the 50 U.S. states, D.C., or U.S. territories such as Guam, Puerto Rico, or U.S. Virgin Islands), including both domestic and cross-border transactions.

Average of Monthly Totals

For the average of monthly totals calculations, please sum the number or balance of accounts at the end of each month and then divide by 12.

	Account 1		Account 2		Account 3		Sum	
	Account Open	End-of-Month Balance	Account Open	End-of-Month Balance	Account Open	End-of-Month Balance	Number of Open Accounts	Sum of End-of-Month Balances
Jan	Yes	$2,726	Yes	$497	No	Not Applicable	2	$3,223
Feb	Yes	$2,196	Yes	$418	No	Not Applicable	2	$2,614
Mar	Yes	$2,706	Yes	$226	No	Not Applicable	2	$2,932
Apr	Yes	$1,553	Yes	$267	No	Not Applicable	2	$1,820
May	Yes	$2,735	Yes	$397	No	Not Applicable	2	$3,132
Jun	Yes	$2,899	Yes	$550	No	Not Applicable	2	$3,449
Jul	Yes	$2,213	Yes	$176	No	Not Applicable	2	$2,389
Aug	Yes	$2,933	Yes	$685	No	Not Applicable	2	$3,618
Sep	Yes	$2,853	Yes	$723	Yes	$8,660	3	$12,236
Oct	Yes	$2,352	Yes	$704	Yes	$9,329	3	$12,385
Nov	Yes	$2,730	Yes	$0	Yes	$9,994	3	$12,724
Dec	Yes	$1,664	Yes	$0	Yes	$9,015	3	$10,679
Sum							28	$71,201
							Divide by 12 months and round to nearest whole number	Divide by 12
Report Average							**2 accounts**	**$5,933 in balances**

Credit card network transactions

All transactions over any credit card network made with general-purpose credit cards, charge cards or co-branded credit cards issued by your institution, meaning that your institution owns the receivables reported in question 9 of the *Institution Profile* section. Include all purchase and bill-pay transactions made with credit cards used for point-of-sale (POS) transactions. Transactions may originate at a physical point of sale or remotely such as via mail order, telephone order, or online, such as through e-commerce or bill pay sites via an app or web browser. For this study, please follow these guidelines:

Credit card network transactions include…	**Credit card network transactions do <u>not</u> include…**
▪ Network transactions made with Visa, MasterCard, Discover, or American Express branded credit cards. These include secured and unsecured credit cards. ▪ Network transactions originated in other countries with credit cards issued from U.S. domiciled accounts	▪ Debit card transactions ▪ Prepaid card transactions ▪ Convenience checks ▪ Balance transfers ▪ Cash advances ▪ Co-branded card non-network ("internal" or closed-loop) transactions

Digital wallet

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

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

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

Virtual card

Virtual cards are used for online or over the phone purchases and do not require the accountholder to have a physical card. Virtual cards may provide greater security than a physical card because they use a unique card number, expiration date, and security code that is only valid at specific merchants or for a specific amount of time. Virtual cards may be issued for single or multiple transaction use, and they may or may not be added to digital wallets.

Contactless card

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

Co-branded credit card

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

Account type definitions

Consumer account

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

Business/government account

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

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

Cash advances

A service provided by credit card and charge card issuers that allows cardholders to withdraw cash—either through an ATM or over the counter at a bank or other financial agency—up to a prescribed limit.

Note: Do not report cash advance transactions in this section of the survey.

Convenience checks

A check linked to a cardholder 's credit line that can be used to make purchases, pay bills or transfer balances from one credit account to another.

Note: Do not include convenience check transactions in this section of the survey.

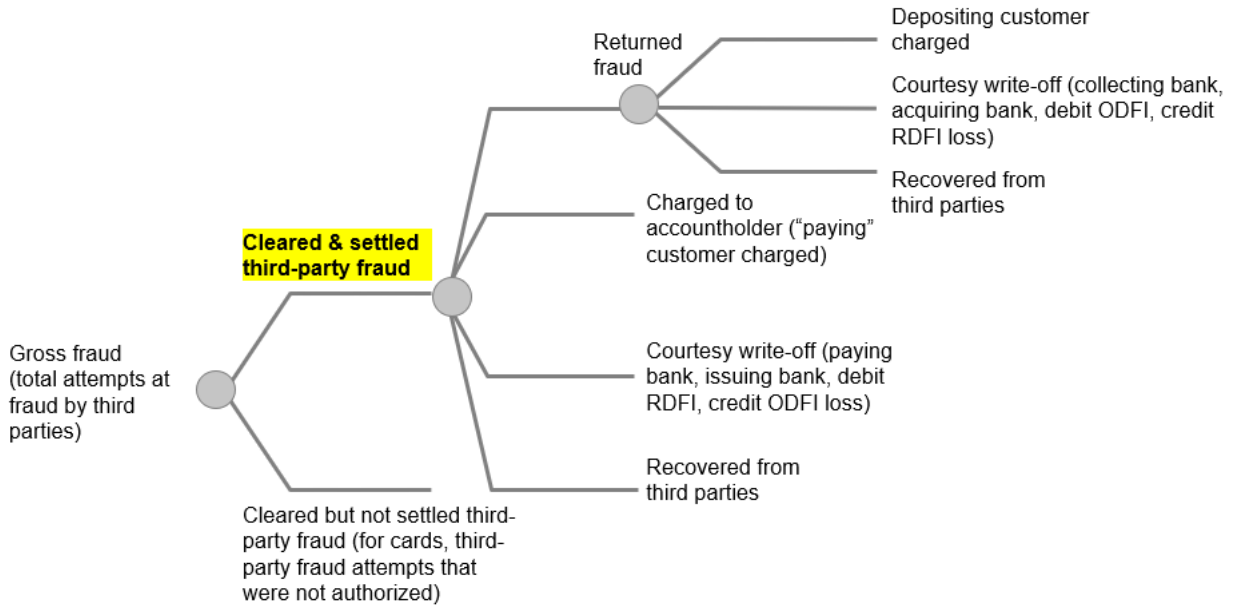
Balance transfers

The transfer by a credit card accountholder of an outstanding debt balance from one credit card account to another.

Note: Do not include balance transfers in this section of the survey.

Third-party fraud

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



SURVEY ITEMS

Your institution is the issuer. Your customer is the payer, accountholder, or cardholder.

1. Did your institution have general-purpose credit cards in circulation in 2021 for which your institution was the issuer?

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

If your answer to this question is "No," please report "Not applicable" for items **2** through **3** and "0" for items **4** through **9** below.

2. Did your institution have co-branded credit cards in circulation in 2021 for which your institution was the issuer?

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

If your answer is "Yes," please exclude "internal" (closed-loop, not using one of the above four major credit card networks) volumes from items **6**, **7**, **8**, and **9** and their subsets and report "internal" volumes in item **5** below. Please include "external" (open-loop, using one of the above four major credit card networks) volumes in your answers to items **6**, **7**, **8**, and **9** and their subsets below.

If your answer is "No," please report "Not applicable" for item **2.a** and "0" for item **5** below.

2.a If your answer is "Yes" to item 2 above and if your institution had "internal" (closed-loop, not using one of the above four major credit card networks) co-branded credit card transactions, are you able to exclude these volumes from your answers to items 6, 7, 8, and 9 and their subsets below?

If your answer is "Yes, in some cases," please explain in the comments box at the end of this section. Even if your answer is "No," please report data for items **6**, **7**, **8**, and **9** and their subsets below and explain in the comment box at the end of this section.

3. Did your institution provide virtual general-purpose credit cards as a product/service in 2021 for which your institution was the issuer? (Note: Virtual cards are different from digital wallets.)

Please see the **GENERAL TERMINOLOGY** section above for the definition of virtual cards. If your answer is "Yes," please exclude virtual cards from counts in item **4** but include virtual card transactions in items **5** through **9** below.

4. Number of physical general-purpose credit cards = 4.a + 4.b

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

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

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

Average of monthly totals means the average of end-of-month totals for each of the months in 2021.

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
- Cards for which your institution was not the issuing institution
- Transaction deposit accounts
- Closed accounts
- Virtual cards

► **Example:** Your institution has 500 credit cards issued to your consumer and business accountholders at the end of January through July. Of these credit cards, 450 cards have been activated and are not expired, 25 cards have not been activated yet, 20 cards have been activated but are now expired, and 5 are virtual cards. Of the 450 cards that have been activated and are not expired, 350 had purchase activity. In this example, you would report 450 credit cards in force and 350 in force with purchase activity for January through July.

At the end of August through December, your institution had the same number of accounts with credit cards issued to them. Of these credit cards, 480 cards have been activated and are not expired, 10 cards have not been activated yet, 6 cards have been activated but are now expired, and 4 are virtual cards. Of the 480 cards that have been activated and are not expired, 300 had purchase activity. In this example, you would report 480 credit cards in force and 300 in force with purchase activity for August through December.

For the number of cards in force, the calculation is as follows: [(450 cards x 7 months open) + (480 cards x 5 months open)] / 12 months = 463 cards in force

For the number of cards in force with purchase activity, the calculation is as follows: [(350 cards x 7 months open) + (300 cards x 5 months open)] / 12 months = 329 cards in force with purchase activity

4.a Consumer cards

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

Include:

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

Do not include:

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

► **Example:** Your institution has 400 credit cards issued to your consumer accounts at the end of January through July. Of these credit cards, 350 cards have been activated and are not expired, 25 cards have not been activated yet, 20 cards have been activated but are now expired, and 5 are virtual cards. Of the 350 cards that have been activated and are not expired, 300 had purchase activity. In this example, you would report 350 credit cards in force and 300 in force with purchase activity for January through July.

At the end of August through December, your institution had the same number of accounts with credit cards issued to them. Of these credit cards, 380 cards have been activated and are not expired, 10 cards have not been activated yet, 6 cards have been activated but are now expired, and 4 are virtual cards. Of the 380 cards that have been activated and are not expired, 200 had purchase activity. In this example, you would report 380 credit cards in force and 200 in force with purchase activity for August through December.

For the number of cards in force, the calculation is as follows: [(350 cards x 7 months open) + (380 cards x 5 months open)] / 12 months = 362 cards in force

For the number of cards in force with purchase activity, the calculation is as follows: [(300 cards x 7 months open) + (200 cards x 5 months open)] / 12 months = 258 cards in force with purchase activity

4.b Business/government cards

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

Include:

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

Do not include:

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

► **Example:** Your institution has 1,000 credit cards issued to business/government accountholders at the end of January through July. Of these credit cards, 900 cards have been activated and are not expired, 50 cards have not been activated yet, 40 cards have been activated but are now expired, and 10 are virtual cards. Of the 900 cards that have been activated and are not expired, 700 had purchase activity. In this example, you would report 900 credit cards in force and 700 in force with purchase activity for January through July.

At the end of August through December, your institution had the same number of accounts with credit cards issued to them. Of these credit cards, 950 cards have been activated and are not expired, 25 cards have not been activated yet, 20 cards have been activated but are now expired, and 5 are virtual cards. Of the 950 cards that have been activated and are not expired, 800 had purchase activity. In this example, you would report 950 credit cards in force and 800 in force with purchase activity for August through December.

For the number of cards in force, the calculation is as follows: [(900 cards x 7 months open) + (950 cards x 5 months open)] / 12 months = 921 cards in force

For the number of cards in force with purchase activity, the calculation is as follows: [(700 cards x 7 months open) + (800 cards x 5 months open)] / 12 months = 742 cards in force with purchase activity

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

These are retail merchant credit cards that are issued in partnership with a specific network processor (i.e., Visa, MasterCard, American Express, and Discover). Co-branded cards are branded with the logo of the retailer and network processor. Users can earn discounts or rewards points when they make purchases with sponsoring merchants. If your answer is "No" to item **1** or item **2** above, please report "0" here.

Include:

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

Do not include:

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

► **Example:** Your customer paid for her $200 hotel room with her credit card that was issued by your institution and co-branded with a hotel company. Later that day, she used another credit card issued by your institution to buy lunch for $20. In this example, you would report only 1 transaction for $200.

6. Total general-purpose credit card network transactions = 6.a + 6.b

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

Include:

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

Do not include:

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

► **Example:** Your customer bought $50 of groceries with her credit card. Later that day, she used the same credit card issued by your institution to purchase a $70 purse online. Your corporate customer used a virtual debit card to purchase $200 of paper supplies. In this example, you would report two transactions for $320.

6.a From consumer accounts

Please see the **GENERAL TERMINOLOGY** section above for the definition of consumer accounts.

Include:

- All network transactions made by consumer accountholders with general-purpose credit cards, charge cards, or co-branded cards issued by your institution

Do not include:

- Credit card transactions made by business/government accountholders

► **Example:** Tom used his credit card issued by your institution to buy a $40 pair of jeans. Later that day, he used his credit card at the ATM to make a $500 cash advance. In this example, you would report 1 transaction for $40.

6.b From business/government accounts

Please see the **GENERAL TERMINOLOGY** section above for the definition of business/government accounts.

Include:

- All network transactions made by business/government accountholders with general-purpose credit cards, charge cards, or co-branded cards issued by your institution

Do not include:

- Credit card transactions made by consumer accountholders

► **Example:** Your corporate accountholder made a purchase of $500 with a corporate credit card issued by your institution. Later that day, he made a cash advance using the same credit card and withdrew $200 in cash over the counter at one of your branch locations. In this example, you would report 1 transaction for $500.

7. Total general-purpose credit card network transactions (repeat item 6) = 7.a + 7.b

Repeat item **6** above. These include all cleared and settled, domestic and cross-border transactions over any credit card network for which your institution was the issuer. If your answer is "No" to item **1** above, please report "0" here.

Include:

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

Do not include:

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

► **Example:** Your customer bought $50 of groceries with her credit card. Later that day, she used the same credit card issued by your institution to purchase a $70 purse online. Your corporate customer used a virtual debit card to purchase $200 of paper supplies. In this example, you would report 2 transactions for $320.

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

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

Include:

- In-person transactions
- In-person mobile transactions (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)
- In-person contactless card transactions (i.e., "tap and pay" physical cards, fobs, or stickers)
- In-person intermediated transactions (e.g., Square, Clover, Zettle)
- In-person card-not-present transactions (i.e., key-entered transactions)

Do not include:

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

► **Example:** Your customer bought a coat for $100 with his credit card by entering his PIN at the checkout line. Later that day, he bought a $40 train ticket with his credit card with his digital wallet (Apple Pay) at the checkout. For this example, you would report 2 transactions for $140.

7.a.1 With a PIN

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

Include:

- In-person transactions authenticated via PIN

Do not include:

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

► **Example:** Your customer bought lunch for $15 with his credit card by entering his PIN at the checkout line. Later that day, he bought a $30 sweater with his credit card by signing the receipt at the checkout. In this example, you would report 1 transaction for $15.

7.a.2 Without a PIN

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

Include:

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

Do not include:

- In-person transactions authenticated via PIN
- Remote transactions

► **Example:** Your customer bought lunch for $15 with his credit card by entering his PIN at the checkout line. Later that day, he bought a $30 sweater with his credit card by signing the receipt at the checkout. For this example, you would report 1 transaction for $30.

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

These include all general-purpose credit card network 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 with either a domestic or foreign payee.

Include:

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

Do not include:

- In-person transactions
- In-person mobile transactions (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)
- In-person contactless card transactions (i.e., "tap and pay" physical cards, fobs, or stickers)
- In-person intermediated transactions (e.g., Square, Clover, Zettle)
- In-person card-not-present transactions (i.e., key-entered transactions)

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

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

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

Include:

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

Do not include:

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

► **Example:** Your customer purchased a $100 item on a Chinese internet website from a Chinese (foreign) merchant with his credit card by entering his credit card number, name, and address. He then proceeded to buy $70 of groceries from a New York grocery store in a mobile application not at the point of sale (in-app transaction), paying with the same credit card with his digital wallet (Google Pay). In this example, you would report 1 transaction for $70 under **8.b.1).** [Note that the foreign payee transaction for $100 would be reported under **8.b.2)**].

7.b.2 Foreign payee

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

Include:

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

Do not include:

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

► **Example:** Your customer purchased a $100 item on a Chinese internet website from a Chinese (foreign) merchant with his credit card by entering his credit card number, name, and address. He then proceeded to buy $70 of groceries from a New York (U.S.-based merchant) grocery store in a mobile application not at the point of sale (in-app transaction), paying with the same credit card with his digital wallet (Google Pay). In this example, you would report 1 transaction for $100 under 7.b.1. [Note that the domestic payee transaction for $70 would be reported under 7.b.2].

8. Total general-purpose credit card network transactions (repeat item 6) = 8.a + 8.b + 8.c

Repeat item **6** above. These include all cleared and settled, domestic and cross-border transactions over any credit card network for which your institution was the issuer. If your answer is "No" to item **1** above, please report "0" here.

Include:

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

Do not include:

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

► **Example:** Your customer bought $50 of groceries with her credit card. Later that day, she used the same credit card issued by your institution to purchase a $70 purse online. Your corporate customer used a virtual debit card to purchase $200 of paper supplies. In this example, you would report 2 transactions for $320.

8.a In-person contactless card transactions

These are all cleared and settled, domestic and cross-border credit card transactions made via a contactless card.

Include:

- Transactions for which a physical card or token was "tapped" or "waved" to pay at the POS terminal

Do not include:

- Credit card-on-file e-commerce transactions (cardholder-initiated or merchant-initiated) (i.e., installment payment)
- Transactions made via digital wallets

► **Example:** Your customer bought lunch for $15 with his credit card. He physically tapped his card on the POS device to pay for lunch, using NFC technology. He then ordered a $30 dinner in a mobile application, paying with his credit card via his digital wallet (Apple Pay). In this example, you would report 1 transaction for $15.

8.b Digital wallet transactions = 8.b.1 + 8.b.2

These are all cleared and settled, domestic and cross-border credit card transactions made via a digital wallet, including tokenized digital wallet.

Include:

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

Do not include:

- Credit card-on-file e-commerce transactions (cardholder-initiated or merchant-initiated) (i.e., installment payment)
- Transactions made via contactless cards (i.e., "tap and pay")

► **Example:** Your customer bought lunch for $10 with his credit card, which was loaded into his digital wallet (Apple Pay). He physically tapped his phone on the POS device to pay for lunch, using NFC technology. He then ordered a $30 dinner in a mobile application, paying with his credit card via his digital wallet (Apple Pay). In this example, you would report 2 transactions for $40.

8.b.1 In-person

These include credit card transactions for which an electronic device, such as a smartphone, smart watch, or activity tracker, was "tapped" or "waved" to pay at the POS terminal (e.g., Apple Pay, Samsung Pay, Google Pay, Fitbit Pay). Such payments are considered contactless payments, but do not use a physical card or token

Include:

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

Do not include:

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

► **Example:** Your customer bought lunch for $15 with his credit card, which was loaded into his digital wallet (Apple Pay). He physically tapped his phone on the POS device to pay for lunch, using NFC technology. He then bought groceries for $100 with his credit card by tapping his card on the POS device. In this example, you would report 1 transaction for $15.

8.b.2 Remote

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

Include:

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

Do not include:

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

► **Example:** Your customer purchased a $500 item on an internet website with his credit card by entering his credit card number, name, and address. He then bought a $65 pair of shoes in a mobile application, paying with the same credit card via his digital wallet (Google Pay). In this example, you would report 1 transaction for $65.

8.c All other transactions

These are all cleared and settled, domestic and cross-border credit card transactions made without a contactless card or digital wallet. If your answer is "No" to item **1** above, please report "0" here.

Do not include:

- Transactions made via digital wallets
- Transactions for which a physical card or token was "tapped" to pay at the POS terminal

► **Example:** Your customer bought lunch for $10 with his credit card. He physically tapped his card on the POS device to pay for lunch, using NFC technology. He then ordered a $30 dinner in a mobile application, paying with his credit card via his digital wallet (Apple Pay). Your customer then bought dessert for $7 using the same credit card by inserting the card in the POS device. In this example, you would report 1 transaction for $7.

9. Third-party fraudulent general-purpose credit card network transactions = 9.a + 9.b

These include all cleared and settled third-party fraudulent network transactions made with general-purpose credit cards, charge cards, or co-branded cards (network volume), before any recoveries or chargebacks, issued by your institution. Please report any fraudulent third-party credit card transactions, regardless of whether the transaction resulted in a loss of funds. If your answer is "No" to item **1** above, please report "0" here.

Include:

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

Do not include:

- Fraud prevented by declining a transaction
- Fraud committed by a valid card user (first-party fraud)
- Fraudulent credit card non-network transactions (e.g., balance transfers, convenience checks),
- Fraudulent co-branded credit card "internal" closed-loop transactions
- Fraudulent credit card cash advances (e.g., ATM withdrawals, over-the-counter withdrawals)
- Fraudulent debit card transactions
- Fraudulent prepaid card transactions
- Credit card transactions authorized by a valid card user as part of a scam

► **Example 1:** Your accountholder 's credit card issued by your institution was stolen. The perpetrator used the card to make one purchase worth $1,000, which was authorized at the point of sale. The perpetrator attempted to make another purchase worth $500 the next day. Your accountholder had already alerted your institution to the previous fraudulent activity and a hold had been put on her account, so the perpetrator never received funds from the second attempt. In this example, you would report 1 transaction for $1,000.

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

9.a In-person transactions = 9.a.1 + 9.a.2

These include only third-party fraudulent general-purpose credit card transactions for which the card user is physically present with the card at the point of sale. Include digital wallet (e.g., Apple Pay, Samsung Pay) transactions at the point of sale only. Please report the total transactions using PIN, and without PIN.

Include:

- In-person fraudulent transactions
- Fraudulent in-person contactless credit card transactions (i.e., "tap and pay" with a credit card)
- Fraudulent in-person mobile transactions (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)
- Fraudulent in-person intermediated transactions (e.g., Square, Clover, Zettle)
- Fraudulent in-person card-not-present transactions (i.e., key-entered transactions)

Do not include:

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

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

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

9.a.1 With a PIN

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

Include:

- Fraudulent in-person transactions that were authenticated via PIN

Do not include:

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

► **Example:** Your accountholder 's credit card was stolen, and the perpetrator watched her enter her PIN at the point of sale before stealing the card. The perpetrator then used her card and PIN to buy a $200 watch at a jewelry store. He then used the card to buy dinner for $50 at a nearby restaurant by fraudulently signing the receipt. In this example, you would report 1 transaction of $200.

9.a.2 Without a PIN

These include only third-party fraudulent general-purpose credit card transactions that are not authenticated using a PIN at the point of sale (single-message over the payment card network). These fraudulent transactions use zip code authentication, card identification number authentication, or other authentication method.

Include:

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

Do not include:

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

► **Example:** Your accountholder 's credit card was stolen, and the perpetrator watched her enter her PIN at the point of sale before stealing the card. The perpetrator then used her card and PIN to buy a $200 watch at a jewelry store. He then used the card to buy dinner for $50 at a nearby restaurant by fraudulently signing the receipt. In this example, you would report 1 transaction of $50.

9.b Remote transactions = 9.b.1 + 9.b.2

These include only third-party fraudulent general-purpose credit card transactions for which the card user does not physically present the card to authorize the transaction. Please report any fraudulent third-party credit card transactions, regardless of whether the transaction resulted in a loss of funds. Please report the total transactions with either a domestic or foreign payee.

Include:

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

Do not include:

- In-person fraudulent transactions
- Fraudulent in-person contactless credit card transactions (i.e., "tap and pay" with a credit card)
- Fraudulent in-person mobile transactions (i.e., digital wallet transactions at the point of sale using near-field communication, magnetic secure transmission, QR codes, or barcode technology)
- Fraudulent in-person intermediated transactions (e.g., Square, Clover, Zettle)
- Fraudulent in-person card-not-present transactions (i.e., key-entered transactions)

► **Example 1:** Your accountholder 's credit card was stolen. The perpetrator used the card to purchase a TV for $500 at a store by fraudulently signing the receipt. He then proceeded to use the stolen card to buy an item online for $250. Both transactions were authorized. In this example, you would report 1 transaction for $250.

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

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

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

Include:

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

Do not include:

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

► **Example:** Your accountholder 's credit card was stolen. The perpetrator used the card to buy a $250 coat online from a French retailer. He then used the card online to buy a $15 book from a U.S. bookstore. In this example, you would report 1 transaction for $15.

9.b.2 Foreign payee

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

Include:

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

Do not include:

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

► **Example:** Your accountholder 's credit card was stolen. The perpetrator used the card to buy a $250 coat online from a French retailer. He then used the card online to buy a $15 book from a U.S. bookstore. In this example, you would report 1 transaction for $250.

Cash Withdrawals and Deposits

GENERAL TERMINOLOGY

This section covers all cash deposits and withdrawals to and from circulation, including third-party fraudulent ATM cash withdrawal transactions. Cash, also called currency, includes paper banknotes and coin. Do not include banknotes and coin exchanged with the Federal Reserve or other supplier for maintaining cash inventory or any other exchanges on your institutions ' own account. Third-party fraudulent ATM cash withdrawal transactions are cleared and settled ATM cash withdrawal transactions that a third-party initiated without the authorization, agreement, or voluntary assistance of an authorized accountholder or cardholder with the intent to deceive for personal gain. All transactions are considered cleared and settled if cash was paid out.

Your institution

"Your institution" refers to the participating depository institution at its highest organizational level (i.e., holding company, if applicable), including all affiliates. Only report data associated with your institution 's U.S. domiciled accounts (i.e., those accounts located within the 50 U.S. states, D.C., or U.S. territories such as Guam, Puerto Rico, or U.S. Virgin Islands), including both domestic and cross-border transactions.

Cash withdrawals

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

Cash withdrawals include…	Cash Withdrawals do not include…
▪ All cash withdrawals by your accountholders (including, as appropriate for the particular survey question, withdrawals made in other countries) ▪ Cash paid out in exchange for a check, whether for an accountholder or not (in this case, whomever receives the cash is a customer) ▪ Credit card cash advances ▪ Prepaid card cash withdrawals	▪ Cash withdrawals or other transactions by individuals or businesses other than your accountholders ▪ Deposit transactions ▪ Inquiries ▪ Funds transfers ▪ Statement prints ▪ Purchases (e.g., stamps, tickets) ▪ Any other non-withdrawal transactions

Cash advances

A service that allows credit and charge card holders to withdraw cash using a credit card, either in-person through an ATM or over the counter at a bank or other financial agency. Credit card issuers reporting cash advances in this section should not include convenience checks or balance transfers in reported amounts.

ATM cash withdrawals

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

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

Cash deposits

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

Cash deposits include…	Cash deposits do not include…
▪ All cash deposits by your accountholders regardless of channel ▪ Prepaid card cash deposits	▪ Cash deposits or other transactions by individuals or businesses other than your accountholders ▪ Withdrawal transactions ▪ Inquiries ▪ Funds transfers ▪ Statement prints ▪ Purchases (e.g., stamps, tickets) ▪ Any other non-withdrawal transactions

Account type definitions

Consumer account

An account for personal use by an individual or household from which ATM withdrawals can be made and cash can be deposited.

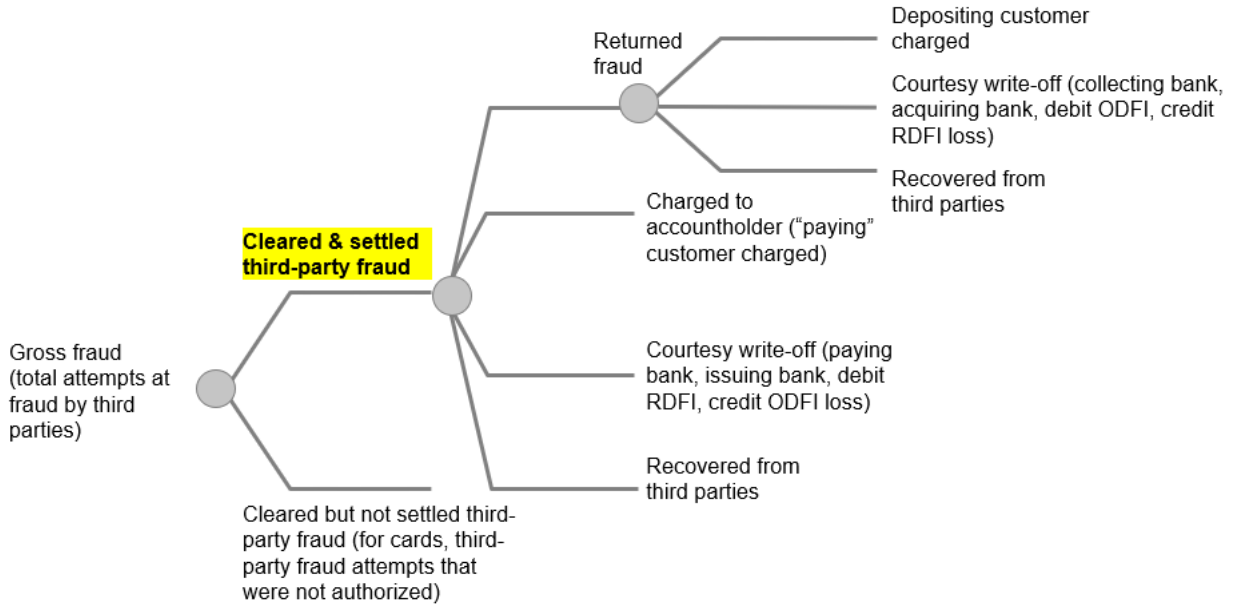
Business/government account

An account owned by an organization (i.e., business, government, non-depository financial institution, or not-for-profit organization) from which ATM withdrawals can be made and cash can be deposited

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

Third-party fraud

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



SURVEY ITEMS

CASH WITHDRAWALS

1. Total cash withdrawals from your institution = 1.a + 1.b + 1.c

These include all cleared and settled, domestic and cross-border cash withdrawals made from accounts at your institution.

Include:

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

Do not include:

- Noncash withdrawal transactions made from accounts at your institution
- Withdrawals made from accounts at another institution
- Deposit transactions
- Teller vault activity
- Convenience checks
- Balance transfers
- Other non-withdrawal transactions (e.g., inquiries, statement print-outs, purchases of stamps, tickets)

1.a Over-the-counter cash withdrawals

These include all cash withdrawals made by your institution 's accountholders at bank lobby teller window or drive-through teller.

Note: Please count only over-the-counter cash withdrawals made at your institution 's branch locations from accounts at your institution.

Include:

- Cash withdrawn by a third party that is not paid out on behalf of another depository institution (e.g. via a "check cashing" service)
- Withdrawal transactions initiated via a withdrawal slip or via the deposit of any negotiable or nonnegotiable instrument
- Over-the-counter cash withdrawals made using your accountholder 's debit, prepaid or credit card linked to the account
- Over-the-counter check cashing (only include the portion of the check that was received in cash)

Do not include:

- Cash paid out to a third-party on behalf of another depository institution (e.g. an over-the-counter cash advance from a credit card issued by another institution)
- Cash withdrawals at ATM terminals including those located at your institution 's branch locations

► **Example:** Your accountholder withdrew $100 in cash over the counter from a teller at one of your institution 's branch locations. In this example, you would report 1 transaction of $100.

1.b Cash orders at wholesale vaults and RCMTs

These include all cash withdrawals handled through armored couriers including vaults operated by your institution or outsourced to armored couriers or other third-party vault operators or made at remote currency management terminals (RCMTs) at merchant customer locations. These RCMT (e.g., "smart safes" and "cash recyclers") cash withdrawals are those that were deployed by your institution and resided at a client site (e.g., gas station, restaurant). Also include all cash (notes and coin) withdrawals made at wholesale vaults from accounts at your institution.

Note: Please count only cash withdrawals made from accounts at your institution at wholesale vaults.

Include:

- Cash withdrawals at outsourced wholesale vaults made from accounts at your institution
- All cash withdrawals at RCMTs

Do not include:

- Banknotes and coin exchanged with the Federal Reserve or other supplier for maintaining cash inventory or any other exchanges on your institution 's own account
- Cash withdrawals at ATM terminals
- Cash deposits made at remote currency management terminals
- Transactions that involved armored couriers withdrawing cash from these terminals or replenishing cash in cash recyclers

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

► **Example 2:** Your customer, a gas station, has installed a cash recycler provided by your institution at one of its stores. In the evening, a gas station clerk deposited $500 in the cash recycler. The next morning, another clerk withdrew $1,000 from the same recycler. In this example, you would report 1 withdrawal for $1,000.

1.c Total ATM cash withdrawals (your institution 's accountholder, any ATM) = 1.c.1 + 1.c.2

These include 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.

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

Include:

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

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

1.c.1 "On-us" ATM cash withdrawals (your institution 's accountholder, your institution 's ATM)

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

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

Include:

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

Do not include:

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

► **Example:** Your customer used her Visa debit card to withdraw $200 from an ATM located in a grocery store. The ATM is owned and operated by your institution. In this example, you would report 1 transaction for $200.

1.c.2 "Foreign" ATM cash withdrawals (your institution 's accountholder, "foreign" ATM)

A "foreign" ATM is any ATM not owned or operated by your institution.

These are all cash withdrawals made at other institutions ' ATMs from accounts at your institution.

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

Include:

- Your institution 's prepaid, debit, and credit card accountholders ' ATM cash withdrawals at "foreign" ATMs (include cash advances from credit card accountholders)
- Both domestic and cross-border transactions at ATM terminals operated by other depository institutions or by ATM operators that are not sponsored by your institution

Do not include:

- Any transactions at your institution 's ATM terminals, regardless of who made them (whether they hold an account at your institution)
- Over-the-counter cash withdrawals
- Non-withdrawal transactions

► **Example:** Your customer used her Visa debit card to withdraw $50 from an ATM located in a grocery store. The ATM is owned and operated by another institution. In this example, you would report 1 transaction for $50.

2. Total cash withdrawals from your institution (repeat item 1) = 2.a + 2.b

Repeat item **1** above. These include all cleared and settled, domestic and cross-border cash withdrawals made from accounts at your institution.

Include:

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

Do not include:

- Noncash withdrawal transactions made from accounts at your institution
- Withdrawals made from accounts at another institution
- Deposit transactions
- Teller vault activity
- Convenience checks
- Balance transfers
- Other non-withdrawal transactions (e.g., inquiries, statement print-outs, purchases of stamps, tickets)

2.a From consumer accounts

These include all consumer deposit account cash withdrawals. Please refer to the **GENERAL TERMINOLOGY** section above for the definition of consumer accounts.

Include:

- Consumer or prepaid account withdrawals
- Consumer credit card cash advances

Do not include:

- Business/government account withdrawals

► **Example:** Your consumer accountholder withdrew $250 in cash at an ATM. In this example, you would report 1 withdrawal of $250.

2.b From business/government accounts

These include all business/government account cash withdrawals. Please include small business accounts under business/government accounts. Please refer to the **GENERAL TERMINOLOGY** section above for the definition of business/government accounts.

Include:

- Cash withdrawals made on a debit or prepaid card linked to a business/government account
- Business/government credit card cash advances

Do not include:

- Consumer account withdrawals

► **Example:** Your small business accountholder, a restaurant owner, withdrew $500 in cash over the counter at one of your institution 's branches. In this example, you would report 1 withdrawal of $500.

3. Total ATM cash withdrawals (your institution 's accountholder, any ATM) (repeat item 1.c) = 3.a + 3.b

Repeat item **1.c** above. These are cash withdrawals made from accounts at your institution from any ATM, including those at your institution 's ATM terminals or "foreign" ATMs. A "foreign" ATM is an ATM operated by an unaffiliated depository institution or ATM operator that is not sponsored by your institution.

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

Include:

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

Do not include:

- Withdrawals by another institution 's accountholders at your institution 's ATMs
- Deposit transactions
- RCMT withdrawals
- Teller vault activity
- Over-the-counter cash withdrawals
- Other non-withdrawal transactions (e.g., inquiries, statement print-outs, purchases of stamps, tickets)

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

3.a Domestic ATM cash withdrawals (your institution 's accountholder, any ATM in the U.S.)

These are cash withdrawals made from accounts at your institution from any ATM located in the U.S. (i.e., ATMs located in the 50 U.S. states, D.C., or U.S. territories).

Include:

- All cash withdrawals on your institution 's accounts from any ATM located in the U.S.

Do not include:

- Cash withdrawals on your institution 's accounts from any ATM located outside the U.S.

► **Example:** Sam, John, and Jenny are checking accountholders at your institution. Sam withdrew $100 in cash at one of your institution 's ATMs located in New York. John withdrew $150 in cash at another institution 's ATM located in Chicago. Jenny withdrew $200 in cash at another institution 's ATM located in Canada. In this example, you would report 2 withdrawals for a total of $250.

3.b Cross-border ATM cash withdrawals (your institution 's accountholder, any ATM outside the U.S.)

These are cash withdrawals made from accounts at your institution from any ATM located outside the U.S.

Include:

- All cash withdrawals on your institution 's accounts from any ATM located outside the U.S.

Do not include:

- Cash withdrawals on your institution 's accounts from any ATM located in the U.S.

► **Example:** Sam, John, and Jenny are checking accountholders at your institution. Sam withdrew $100 in cash at one of your institution 's ATMs located in New York. John withdrew $150 in cash at another institution 's ATM located in Chicago. Jenny withdrew $200 in cash at another institution 's ATM located in Canada. In this example, you would report 1 withdrawal for $200.

4. Third-party fraudulent ATM cash withdrawals (your institution 's accountholder, any ATM) = 4.a + 4.b

These are all cleared and settled ATM cash withdrawals that were not authorized by your institution 's accountholders (third-party fraud).

Include:

- All cleared and settled third-party fraudulent ATM withdrawal transactions before any recoveries or chargebacks (debit, prepaid ATM cash withdrawals and credit card cash advances) (i.e. regardless of whether a loss is incurred)

Do not include:

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

► **Example 1:** Your accountholder 's debit card was stolen by a perpetrator who watched her enter her PIN at the point of sale. The perpetrator used the card and PIN to make a one-time $200 ATM withdrawal. The next day, the perpetrator tried to withdraw $500 from another ATM. Your accountholder had already reported the previous fraudulent activity and a hold had been put on their account, so the perpetrator was not able to withdraw any funds. In this example, you would report 1 transaction for $200.

► **Example 2:** Your accountholder claimed that a perpetrator stole her debit card and used it to withdraw $100 from an ATM. However, an investigation by your institution determined the claim to be false, as the money was actually withdrawn by your accountholder. Since this transaction is an example of first-party fraud (false claim of fraud), you would not include it in item **4** above.

4.a Domestic ATM cash withdrawals (your institution 's accountholder, any ATM in the U.S.)

These include all cash withdrawals from ATMs located in the U.S. (i.e., ATMs located in the 50 U.S. states, D.C., or U.S. territories), that were not authorized by your institution 's accountholders (third-party fraud)

Include:

- All third-party fraudulent ATM withdrawal transactions before any recoveries or chargebacks from ATMs located in the U.S., regardless of whether those funds were subsequently recovered

Do not include:

- Any third-party, fraudulent cash withdrawal from any ATM located outside the U.S.

► **Example:** Jen and Kate are accountholders at your institution. Both of their debit cards were stolen by perpetrators who watched them enter their PINs at the point-of-sale. Jen 's perpetrator used her card and PIN to make a one-time $300 ATM withdrawal in Atlanta. Kate 's perpetrator used her card and PIN to make a one-time $400 ATM withdrawal in Italy. In this example, you would report 1 transaction for $300.

4.b Cross-border ATM cash withdrawals (your institution 's accountholder, any ATM outside the U.S.)

These include all cash withdrawals from ATMs located outside the U.S., that were not authorized by your institution 's accountholders (third-party fraud)

Include:

- All third-party fraudulent ATM withdrawal transactions before any recoveries or chargebacks from ATMs located outside the U.S., regardless of whether those funds were subsequently recovered

Do not include:

- Any third-party, fraudulent cash from any ATM located in the U.S.

► **Example:** Jen and Kate are accountholders at your institution. Both of their debit cards were stolen by perpetrators who watched them enter their PINs at the point-of-sale. Jen 's perpetrator used her card and PIN to make a one-time $300 ATM withdrawal in Atlanta. Kate 's perpetrator used her card and PIN to make a one-time $400 ATM withdrawal in Italy. In this example, you would report 1 transaction for $400.

CASH DEPOSITS

5. Total cash deposited at your institution = 5.a + 5.b + 5.c

These are the total cash deposits made into accounts at your institution. Include cash deposits that were made over the counter at your institution 's bank branches, cash deposits at ATMs, cash deposits at wholesale vaults and RCMTs.

Include:

- Cash deposits into both deposit accounts as well as into prepaid card program accounts

Do not include:

- Noncash deposit transactions made to accounts at your institution
- Teller vault activity
- Withdrawal transactions
- Other non-deposit transactions (i.e., inquiries, statement print-outs, purchases of stamps, tickets)

5.a Over-the-counter cash deposits

These are the cash deposits made at bank lobby teller window or drive through teller.

Include:

- Over-the-counter cash deposits made at your institution 's branch locations to accounts at your institution

Do not include:

- Cash deposits at ATM terminals located in your institution 's branch locations
- Noncash deposit transactions made to accounts at your institution

► **Example:** Your accountholder deposited $600 in cash into his account over the counter through a teller at one of your institution 's branch locations. In this example, you would report 1 deposit of $600.

5.b Cash deposits at wholesale vaults and RCMTs

These are the cash deposits handled through armored couriers including vaults operated by your institution or outsourced to an armored courier or other third-party vault operator. These also include deposits made at RCMTs at merchant customer locations (i.e., "smart safes" and "cash recyclers") that were deployed by your institution and resided at a client site (e.g., gas station, restaurant).

Include:

- Cash deposits made to accounts at your institution at wholesale vaults
- All cash deposits made at RMCTs

Do not include:

- Banknotes and coin exchanged with the Federal Reserve or other supplier for maintaining cash inventory or any other exchanges on your institutions ' own account
- Noncash deposit transactions made to accounts at your institution
- Teller vault activity
- Cash withdrawals made at remote currency management terminals
- Transactions that involved armored couriers depositing cash from these terminals or replenishing cash in cash recyclers

► **Example 1:** A local retailer for which your institution provides banking services used an armored courier service to deposit $5,000 in cash and coin at your cash vault and to order $1,500 in various denominations of cash straps and coin rolls to make change available in its store(s). In this example, you would report 1 cash deposit for $5,000.

► **Example 2:** Your customer, a gas station, has installed a cash recycler provided by your institution at one of its stores. In the evening, a gas station clerk deposited $500 in the cash recycler. The next morning, another clerk withdrew $700 from the same recycler. In this example, you would report 1 deposit for $500.

5.c ATM cash deposits (your institution 's accountholder, any ATM) = 5.c.1 + 5.c.2

These are all cash deposits made to accounts at your institution at any ATM, including those at your institution 's ATM terminals (item **5.c.1** or "foreign" ATMs (item **5.c.2** below. A "foreign" ATM is an ATM operated by an unaffiliated depository institution or ATM operator.

Include:

- Cash deposits made to your institution on any ATM

Do not include:

- Deposits made to accounts at another institution
- Withdrawal transactions
- Other non-deposit transactions (i.e., inquiries, statement print-outs, purchases of stamps, tickets)

► **Example:** On Monday your accountholder deposited $250 cash into his checking account via an ATM. On Tuesday he deposited $500 in checks at the same ATM. In this example, you would report 1 cash deposit for $250.

5.c.1 "On-us" ATM cash deposits (your institution 's accountholder, your institution 's ATM)

These are all cash deposits made to accounts at your institution at your institution 's ATM terminals. An "on-us" ATM is any ATM owned or operated by your institution.

Include:

- Deposits made to accounts at your institution at fee-free ATM networks in which it participates

Do not include:

- Deposits by cardholders other than your institution 's accountholders, deposits made to accounts at your institution at "foreign" ATMs, or non-deposit transactions made to accounts at your institution

► **Example:** On Monday your accountholder deposited $250 cash into his checking account via an ATM owned by your institution. On Tuesday he deposited $500 in checks at the same ATM. In this example, you would report 1 cash deposit for $250.

5.c.2 "Foreign" ATM cash deposits (your institution 's accountholder, "foreign" ATM)

These are all cash deposits made to accounts at your institution at "foreign" ATMs. A "foreign" ATM is any ATM not owned or operated by your institution.

Alternative Payment Initiation Methods

This section covers all cleared and settled domestic and cross-border online or mobile bill payments and person-to-person (P2P) transfers originated by your institution 's consumer accountholders, including third-party fraudulent P2P transfer originations. Third-party fraudulent P2P transfer originations are cleared and settled P2P transfer originations that a third-party originated without the authorization, agreement, or voluntary assistance of an authorized accountholder or cardholder with the intent to deceive for personal gain.

GENERAL TERMINOLOGY

Your institution

"Your institution" refers to the participating depository institution at its highest organizational level (i.e., holding company, if applicable), including all affiliates. Only report data associated with your institution 's U.S. domiciled accounts (i.e., those accounts located within the 50 U.S. states, D.C., or U.S. territories such as Guam, Puerto Rico, or U.S. Virgin Islands), including both domestic and cross-border transactions.

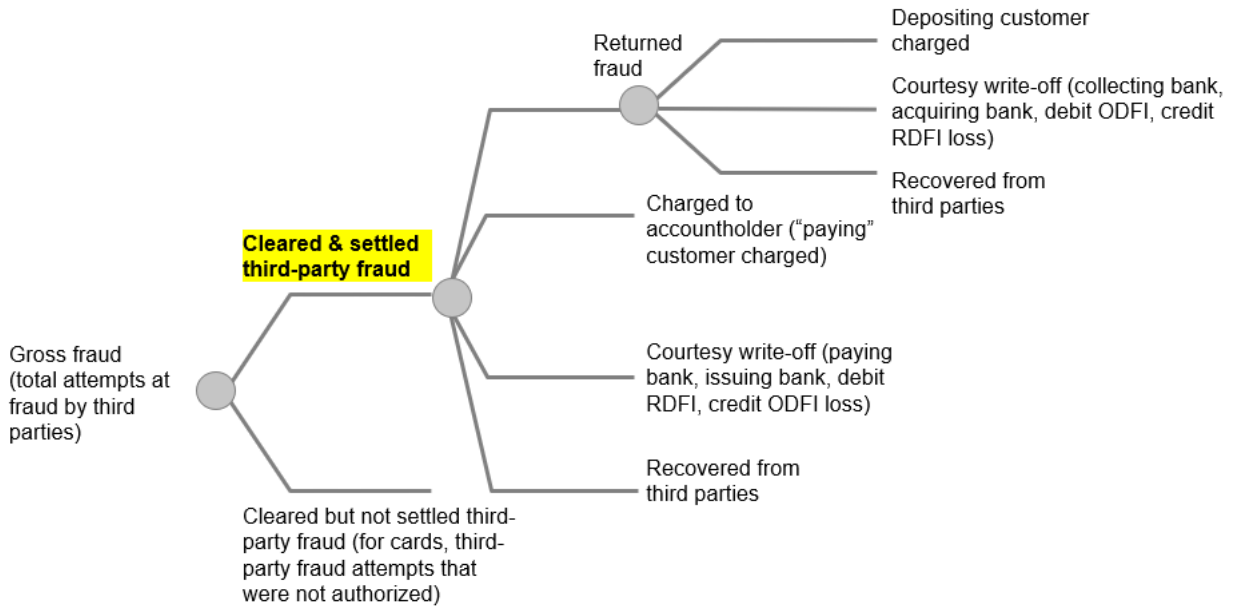
Average of Monthly Totals

For the average of monthly totals calculations, please sum the number or balance of accounts at the end of each month and then divide by 12.

	Account 1		Account 2		Account 3		Sum	
	Account Open	End-of-Month Balance	Account Open	End-of-Month Balance	Account Open	End-of-Month Balance	Number of Open Accounts	Sum of End-of-Month Balances
Jan	Yes	$2,726	Yes	$497	No	Not Applicable	2	$3,223
Feb	Yes	$2,196	Yes	$418	No	Not Applicable	2	$2,614
Mar	Yes	$2,706	Yes	$226	No	Not Applicable	2	$2,932
Apr	Yes	$1,553	Yes	$267	No	Not Applicable	2	$1,820
May	Yes	$2,735	Yes	$397	No	Not Applicable	2	$3,132
Jun	Yes	$2,899	Yes	$550	No	Not Applicable	2	$3,449
Jul	Yes	$2,213	Yes	$176	No	Not Applicable	2	$2,389
Aug	Yes	$2,933	Yes	$685	No	Not Applicable	2	$3,618
Sep	Yes	$2,853	Yes	$723	Yes	$8,660	3	$12,236
Oct	Yes	$2,352	Yes	$704	Yes	$9,329	3	$12,385
Nov	Yes	$2,730	Yes	$0	Yes	$9,994	3	$12,724
Dec	Yes	$1,664	Yes	$0	Yes	$9,015	3	$10,679
						Sum	28	$71,201
							Divide by 12 months and round to nearest whole number	Divide by 12
						Report Average	**2 accounts**	**$5,933 in balances**

Third-party fraud

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



SURVEY ITEMS

1. Did your institution offer online or mobile consumer bill payments during calendar year 2021?

These include online and mobile bill payment transactions initiated through your institution 's bill payment platform. If your answer to this question is "No," please report "0" for item **2** below.

Include:

- All online and mobile bill payment transactions paid from consumer accounts at your institution and initiated through your institution 's website (including mobile browser), mobile application, or an SMS/text message

Do not include:

- Payments made through a biller 's website
- Person-to-person transfers (e.g., Zelle) reported in items **3.a** and **5** below
- All online and mobile bill payment transactions paid from business/government accounts at your institution and initiated through a web browser (including a mobile browser), a mobile application, or an SMS/text message

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

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

These include all cleared and settled, domestic and cross-border online and mobile consumer bill payment transactions initiated through your institution 's bill payment platform. If your answer is "No" to item **1** above, please report "0" here.

Include:

- All online and mobile bill payment transactions paid from consumer accounts at your institution and initiated through your institution 's website (including mobile browser), mobile application, or an SMS/text message

Do not include:

- Payments made through a biller 's website
- Person-to-person transfers (e.g., Zelle) reported in items **3.a** and **5** below
- All online and mobile bill payment transactions paid from business/government accounts at your institution and initiated through a web browser (including a mobile browser), a mobile application, or an SMS/text message

► **Example:** Your accountholder paid her $50 utility bill through her PC by initiating a payment from her account via your institution 's website. Another accountholder paid his rent of $1,500 by initiating a payment from his account via your institution 's website using his smartphone. A third accountholder paid his rent of $2,000 by initiating a payment via your institution 's mobile application rather than your institution 's website. In this example you would report 3 transactions for $3,550.

3. Did your institution offer an online or mobile person-to-person (P2P) funds transfer system during calendar year 2021?

These include all online, mobile, and SMS/text message funds transfer transactions from person to person (P2P). If your answer is "No," please report "Not applicable" for item **3.a** and "0" for items **4**, **5,** and **6** below.

Include:

- Person-to-person transfers initiated through your institution 's website (including mobile browser), mobile application, or an SMS/text message. Include Zelle and Popmoney P2P transfers if they are initiated through your institution 's online application

Do not include:

- Business/government-to-person
- Transfers made from an external party 's website including Venmo, Popmoney, and Zelle P2P transfers if they are initiated through an external party 's online application
- Transfers from small business accounts to consumer accounts
- Online and mobile bill payment transactions initiated through your institution 's bill payment platform
- P2P transfers received from an accountholder at another institution

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

3.a If the answer is "Yes" to item 3 above did your institution offer an immediate payments option via an online or mobile person-to-person (P2P) funds transfer system during calendar year 2021?

Immediate payments are funds transfers sent with real-time or near-real-time availability to the recipient (30 minutes or less). If the answer to this question is "No," please enter "0" for number and value in your answer to items **5.a** and **6.a** below.

4. Number of active online or mobile person-to-person (P2P) transfer accounts

Average of monthly totals means the average of end-of-month totals for each of the months in 2021.

New active P2P transfer accounts are accounts from which at least one payment was sent via your institution 's P2P transfer platform for the first time within a month.

All active P2P transfer accounts are accounts from which at least one payment was sent via your institution 's P2P transfer platform within a month.

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

► **Example:** Your institution had 100 P2P transfer accounts in January from which at least one value transaction was completed. For 10 of these accounts, the accountholder completed a transaction via your institution 's P2P transfer platform for the first time. In this example, you would report 10 new active P2P transfer accounts, and 100 active P2P transfer accounts in January. To calculate the active users for calendar year 2021, repeat this calculation with the average of all 12 months.

5. Total online or mobile person-to-person (P2P) transfer originations = 5.a + 5.b

These include all cleared and settled, domestic and cross-border person-to-person transfers originated by your institution 's consumer accountholders and initiated via your institution 's website, mobile application, or an SMS/text message to another consumer account. If your answer is "No" to item **3** above, please report "0" here.

Include:

- P2P transfer originations made from consumer accounts at your institution and initiated via your institution 's website or mobile application (include transfer originations made through digital payments network partners, e.g., Zelle, Visa Direct, or Mastercard Send, if applicable).

Do not include:

- Business/government-to-person
- Transfers made from an external party 's website (e.g., PayPal, Venmo, or Popmoney)
- Transfers from small business accounts to consumer accounts
- Online and mobile bill payment transactions initiated through your institution 's bill payment platform
- P2P transfers received from an accountholder at another institution

► **Example:** Your accountholder, Jenny, initiated a $200 payment from her account to another person 's account at another institution through your institution 's mobile application on her tablet by entering the recipient 's phone number or e-mail address. Jenny then initiated another payment for $50 from her account to another person 's account at your institution through your institution 's mobile application. Jenny then initiated a payment of $75 to another friend via Venmo. In this example, you would report 2 transactions for $250.

5.a Immediate payments

These include all P2P transactions in which funds are sent with real-time or near-real-time availability to the recipient (30 minutes or less).

Include:

- Payments using a funds transfer method, system, and internal policy that supports immediate funds availability to the beneficiary (end user or final payee). E.g., include Zelle, internal book transfers, or Mastercard Send/Visa Direct under a policy of immediate funds availability to recipient.

Do not include:

- P2P transfers in which funds are typically not available to recipient within 30 minutes
- Transfers made from an external party 's website such as Venmo or Popmoney
- Business/government-to-person
- Transfers from small business accounts to consumer accounts
- Online and mobile bill payment transactions initiated through your institution 's bill payment platform

► **Example:** Your accountholder paid his friend $50 using Zelle on your institution 's mobile application. The same accountholder then paid his brother $100 using the Automated Clearinghouse and the funds were available the next day. In this example, you would report 1 transaction for $50.

5.b All other

These include all P2P transfers in which funds are sent without real-time or near-real-time availability to the recipient (later than 30 minutes and, typically 1 or more days after payment was initiated).

Include:

- Payments using a funds transfer method, system, and internal policy that do not support immediate payments. E.g. Automated Clearinghouse (settled same-day or later), or Visa Direct/Mastercard Send under a policy of funds availability to recipient later than 30 minutes.

Do not include:

- P2P transfers in which funds are typically available to recipient within 30 minutes
- Business/government-to-person
- Transfers from small business accounts to consumer accounts
- Online and mobile bill payment transactions initiated through your institution 's bill payment platform

► **Example 1:** Your accountholder paid his friend $50 using Zelle on your institution 's mobile application. The same accountholder then paid his brother $100 using the Automated Clearinghouse and the funds were available the next day. In this example, you would report 1 transaction for $100.

6. Third-party fraudulent online or mobile person-to-person (P2P) transfer originations = 6.a + 6.b

These include all cleared and settled third-party fraudulent person-to-person transfers originated from your institution 's consumer account and initiated via your institution 's website, mobile application, or an SMS/text message to another consumer account. If your answer is "No" to item **3** above, please report "0" here.

Include:

- Cleared and settled third-party fraudulent person-to-person transfers initiated through your institution 's website (including a mobile browser), mobile application, or an SMS/text message (i.e., regardless of whether a loss is incurred). Include fraudulent Zelle and Popmoney P2P transfers if they are initiated through your institution 's online application

Do not include:

- Fraudulent business/government-to-person
- Fraudulent transfers made from an external party 's website, including Venmo, Popmoney, and Zelle P2P transfers if they are initiated through an external party 's online application
- Fraudulent transfers from small business accounts to consumer accounts
- Any fraudulent bill payment transactions initiated through your institution 's bill payment platform
- Fraudulent P2P transfers received from an accountholder at another institution

► **Example:** John is an accountholder at your institution. His account was hacked. The perpetrator used Zelle through your institution 's mobile application and paid his own account, also at your institution, $100. He then initiated a second payment of $200 from John 's account to pay another person 's account at another institution using Zelle as before. The next day, the perpetrator attempted to initiate a third payment of $300 from John 's account to pay his own account at your institution via Zelle on your institution 's mobile application. However, John had already alerted your institution to the previous fraudulent activity and a hold had been put on his account, so the funds were never made available to the perpetrator. In this example you would report 2 transactions for $300.

6.a Immediate payments

These include all fraudulent P2P transactions in which funds are sent with real-time or near-real-time availability to the recipient (30 minutes or less).

Include:

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

Do not include:

- Fraudulent P2P transfers in which funds are typically not available to recipient within 30 minutes
- Fraudulent business/government-to-person
- Fraudulent transfers from small business accounts to consumer accounts

► **Example:** Your customer 's account at your institution was hacked. The perpetrator paid his own account, also at your institution, $100 using Zelle on your institution 's mobile application. The perpetrator then paid another fraud originator 's account $200 using the Automated Clearinghouse and the funds were available the next day. In this example, you would report 1 transaction for $100.

6.b All other

These include all fraudulent P2P transfers in which funds are sent without real-time or near-real-time availability to the recipient (later than 30 minutes and, typically 1 or more days after payment was initiated).

Include:

- Fraudulent payments using a funds transfer method, system, and internal policy that do not support immediate payments. E.g. Automated Clearinghouse (settled same-day or later), or Visa Direct/Mastercard Send under a policy of funds availability to recipient later than 30 minutes.

Do not include:

- Fraudulent P2P transfers in which funds are typically available to recipient within 30 minutes
- Fraudulent business/government-to-person
- Fraudulent transfers from small business accounts to consumer accounts
- Fraudulent received P2P transfers from an accountholder at another institution

► **Example:** Your customer 's account at your institution was hacked. The perpetrator paid his own account, also at your institution, $100 using Zelle on your institution 's mobile application. The perpetrator then paid another fraud originator 's account $200 using the Automated Clearinghouse and the funds were available the next day. In this example, you would report 1 transaction for $200.