Networks, Processors, and Issuers Payments Surveys (NPIPS)

Selected Glossary of Terms

Survey Period:
Calendar Year 2017

	General-Purpose Credit Card Network
Item	**Definition**
	United States: The states, territories, and possessions of the U.S., the District of Columbia, the Commonwealth of Puerto Rico, or any political subdivision of any of the foregoing.
1a	**Denials/declines:** Transaction attempts that receive a denial response by the host authorization system and do not result in an authorized transaction.
2a	**Pre-authorization only:** Transactions that are approved but not settled (e.g., the initial amount which a rental agency, hotel, or fuel dispenser operator receives authorization, but final payment and amount transfer is never made).
3	**Net, authorized & settled transactions:** Transactions initiated by the acquirer that are completed with the final payment amount transferred from the acquirer to the issuer. Such transactions include those that are subsequently reversed through a chargeback, or other adjustment or return.
3a	**Cash advances:** Transactions involving the provision of cash to the cardholder via an ATM or over the counter with the use of a credit or charge card, typically authenticated by entering a personal identification number (PIN). (Unlike debit or prepaid card cash-back transactions, cash advances are not combined with a purchase.)
3b.1	**Chargebacks:** Transactions initiated by the issuer that reverse a transaction, in whole or in part, and transfer value from the acquirer to the issuer (e.g., customer disputes, fraud, processing errors, authorization issues, or non-fulfillment of copy requests). A chargeback provides the issuer with a way to return a disputed transaction, typically on behalf of the cardholder.
3b.2	**Other adjustments and returns:** Transactions initiated by the acquirer that reverse a transaction, in whole or in part, and transfer value from the acquirer to the issuer (e.g., customer return of goods, complaints, merchant-identified fraud, duplicate transaction entry).
4	**Net, purchase transactions:** Transactions that have been authorized and settled. Exclude denials, transactions that are pre-authorization only, cash advances, chargebacks, and other adjustments and returns.
6a.1	**Chip:** Transactions for which account information taken from a computer microchip embedded in a card or mobile device that securely stores data to be read via contact or contactless/NFC communications with a merchant payment device or terminal. Include EMV and all other types of chip transactions with a card or mobile device. Report only in-person transactions.
6a.1.1	**EMV:** "Dipped" transactions are initiated by inserting a card with an embedded EMV microchip into a merchants chip-enabled terminal. Data are tokenized and processed using a unique one-time use code and can be authenticated with Chip-and-Signature and Chip-and-PIN.

	General-Purpose Credit Card Network
Item	**Definition**
6a.1.2	**RFID/NFC (including both mobile and card-based chips):** "Tap and Pay" contactless transactions use Radio Frequency Identification (RFID) and/or a specialized subset of Near-field Communications (NFC) standards to initiate a card-based payment. NFC is designed to be a secure form of data exchange and can support EMV transactions. Contactless authentication can utilize a physical card, fob, or sticker that is "tapped" to pay at a point-of-sale (POS) terminal. Examples include MasterCard Tap & Go®, Visa payWave and Exxon's SpeedPass.
6a.2	**Scanner (Barcode/QR code):** "Scanner" initiated transactions are when a merchant utilizes an optical Barcode reader to access cardholder data. Quick-response (QR) and other images can be used to provide required account information from a smartphone or printed image.
6a.3	**Magnetic stripe:** "Swipe" transactions where cardholder and account information contained in a magnetic stripe are read when a card passes through a reader. This would also include MIST technology used by Samsung Pay to spoof the swipe to transmit track data from magstripe cards to POS terminals.
6a.4	**Card number/cashier key entry:** "Keyed" transactions are initiated by a merchant when the POS terminal cannot read the magnetic-stripe of the card and the cashier must key in the cardholder data. Merchants that are not EMV chip-enabled may be required to support manual key entry as a method of backup acceptance should a magnetic-stripe read on a card fail.
6a.5	**Other:** Any other method used to provide customer card account information not listed above.
7a	**PIN (personal identification number):** In-person transactions where a cardholder enters their Personal Identification Number (PIN) to authenticate the card purchase. This would also include remote transactions where PINs are entered through secure methods like Acculynk.
7b	**Zip code:** Zip codes of cardholders' billing address are used with Address Verification Systems (AVS). AVS is often used as an anti-fraud method for unattended terminals like fuel dispensers. Address verification systems can also be used for remote purchases.
7c	**Card identification number:** A number (typically 3- or 4-digits) printed on the card that provides additional identification and verification of a cardholder for authenticating purchases. This includes a variety of codes supported by card networks such as CIN, CID, CVV, CVV2, or CSC.
7d	**Other/unknown:** All other transactions where one of the listed types of data was not recorded. Include transactions associated with no authentication or transactions using an unlisted/unmeasured type of authentication such as low-value transactions (e.g., under $50) where no signature or PIN entry is required at certain merchant classes such as Grocery or Quick Service Restaurants.

	General-Purpose Credit Card Network
Item	Definition
9a	**Lost or stolen card:** Fraudulent transactions via a card reported as lost or stolen.
9b	**Card issued but not received:** Fraudulent transactions reported to be via an intercepted new or replacement card in transit that was activated by someone other than the cardholder.
9c	**Fraudulent application:** Fraudulent transactions reported to be via a new card that was issued to someone other than the cardholder using falsified information or a stolen identity.
9d	**Counterfeit card:** Fraudulent point-of-sale transactions via an altered or cloned card.
9e	**Fraudulent use of account number:** Fraudulent transactions using account number and other card and cardholder details, typically remotely.
9f	**Other (including account takeover):** All other fraudulent transactions not included the above categories. In particular, "other" covers account takeover, a form of identity theft whereby an unauthorized party gains access to and use of an existing card account.
17	**Transaction value distribution:** Your best estimate for the number and dollar value of transactions that fall within the "dollar size bands" requested.
18	**Total cards:** All issued, activated, and unexpired general-purpose credit or charge cards (linked to U.S.-domiciled accounts).
18	**Active cards:** Cards outstanding with a minimum level of purchase activity according to your organization's definition.

	Private-Label Credit Card Merchant Issuer
Item	Definition
	United States: The states, territories, and possessions of the U.S., the District of Columbia, the Commonwealth of Puerto Rico, or any political subdivision of any of the foregoing.
3a	**Denials/declines:** Transaction attempts that receive a denial response by the host authorization system and do not result in an authorized transaction.
4a	**Pre-authorization only:** Transactions that are temporarily authorized but not completed or posted, or the portion of authorized amounts that are not included in a final posting.
5	**Completed transactions (posted to card accounts):** Purchase or cash advance transactions that are completed and posted to the private-label card account for payment. Such transactions include those that are subsequently reversed in an adjustment or return requested by the merchant or cardholder, defined below.

	Private-Label Credit Card Merchant Issuer
Item	**Definition**
5a	**Cash advances:** Transactions involving the provision of cash to the cardholder. Credit card cash advances are typically counted separately from any purchase transaction.
5b	**Adjustments and returns:** Completed and posted transactions that are subsequently reversed, in whole or in part, and that transfer value back to the card account (e.g., customer return of goods, complaints, disputed charges, fraud, duplicate transaction entry).
6	**Net, purchase transactions:** Completed purchase transactions that have not been reversed. Exclude denials, transactions that are pre-authorization only, cash advances, and adjustments and returns defined above.
7a.1	**Transactions initiated with a mobile device:** Transactions initiated on a smart device in person with NFC using a "digital wallet".
8a	**Lost or stolen card:** Fraudulent transactions via a card reported as lost or stolen.
8b	**Card issued but not received:** Fraudulent transactions reported to be via an intercepted new or replacement card in transit that was activated by someone other than the cardholder.
8c	**Fraudulent application:** Fraudulent transactions reported to be via a new card that was issued to someone other than the cardholder using falsified information or a stolen identity.
8d	**Counterfeit card:** Fraudulent point-of-sale transactions via an altered or cloned card.
8e	**Fraudulent use of account number:** Fraudulent transactions using account number and other card and cardholder details, typically remotely.
8f	**Other (including account takeover):** All other fraudulent transactions not included the above categories. In particular, "other" covers account takeover, a form of identity theft whereby an unauthorized party gains access to and use of an existing card account.
11	**Transaction value distribution:** Your best estimate for the number and dollar value of transactions that fall within the "dollar size bands" requested.
12	**Total cards outstanding:** All issued, activated, and unexpired private-label credit cards (linked to U.S.-domiciled accounts).
12	**Active cards:** Cards outstanding with a minimum level of purchase activity according to your organization's definition.

	Private-Label Credit Card Processor
Item	**Definition**
	United States: The states, territories, and possessions of the U.S., the District of Columbia, the Commonwealth of Puerto Rico, or any political subdivision of any of the foregoing.
3a	**Denials/declines:** Transaction attempts that receive a denial response by the host authorization system and do not result in an authorized transaction.
4a	**Pre-authorization only:** Transactions that are temporarily authorized but not completed or posted, or the portion of authorized amounts that are not included in a final posting.
5	**Completed transactions (posted to card accounts):** Purchase or cash advance transactions that are completed and posted to the private-label card account for payment. Such transactions include those that are subsequently reversed in an adjustment or return requested by the merchant or cardholder, defined below.
5a	**Cash advances:** Transactions involving the provision of cash to the cardholder. Credit card cash advances are typically counted separately from any purchase transaction.
5b	**Adjustments and returns:** Completed and posted transactions that are subsequently reversed, in whole or in part, and that transfer value back to the card account (e.g., customer return of goods, complaints, disputed charges, fraud, duplicate transaction entry).
6	**Net, purchase transactions:** Completed purchase transactions that have not been reversed. Exclude denials, transactions that are pre-authorization only, cash advances, and adjustments and returns defined above.
7a.1	**Transactions initiated with a mobile device:** Transactions initiated on a smart device in person with NFC using a "digital wallet".
8a	**Lost or stolen card:** Fraudulent transactions via a card reported as lost or stolen.
8b	**Card issued but not received:** Fraudulent transactions reported to be via an intercepted new or replacement card in transit that was activated by someone other than the cardholder.
8c	**Fraudulent application:** Fraudulent transactions reported to be via a new card that was issued to someone other than the cardholder using falsified information or a stolen identity.
8d	**Counterfeit card:** Fraudulent point-of-sale transactions via an altered or cloned card.
8e	**Fraudulent use of account number:** Fraudulent transactions using account number and other card and cardholder details, typically remotely.

	Private-Label Credit Card Processor
Item	**Definition**
8f	**Other (including account takeover):** All other fraudulent transactions not included the above categories. In particular, "other" covers account takeover, a form of identity theft whereby an unauthorized party gains access to and use of an existing card account.
11	**Transaction value distribution:** Your best estimate for the number and dollar value of transactions that fall within the "dollar size bands" requested.
12	**Total cards outstanding:** All issued, activated, and unexpired private-label credit cards (linked to U.S.-domiciled accounts).
12	**Active cards:** Cards outstanding with a minimum level of purchase activity according to your organization's definition.

	General-Purpose Debit Card Network
Item	**Definition**
	United States: The states, territories, and possessions of the U.S., the District of Columbia, the Commonwealth of Puerto Rico, or any political subdivision of any of the foregoing.
2a	**Denials/declines:** Transaction attempts that receive a denial response by the host authorization system and do not result in an authorized transaction.
3a	**Pre-authorization only:** Transactions that are approved but not settled (e.g., the initial amount which a rental agency, hotel, or fuel dispenser operator receives authorization, but final payment and amount transfer is never made).
4	**Net, authorized & settled transactions:** Transactions initiated by the acquirer that are completed with the final payment amount transferred from the acquirer to the issuer. Such transactions include those that are subsequently reversed through a chargeback, or other adjustment or return.
4a	**Cash-back at the point of sale:** Purchase transactions that include an amount of cash given back to the card user. A point-of-sale (POS) purchase transaction with cash back is counted as one transaction.
4b.1	**Chargebacks:** Transactions initiated by the issuer that reverse a transaction, in whole or in part, and transfer value from the acquirer to the issuer (e.g., customer disputes, fraud, processing errors, authorization issues, or non-fulfillment of copy requests). A chargeback provides the issuer with a way to return a disputed transaction, typically on behalf of the cardholder.
4b.2	**Other adjustments and returns:** Transactions initiated by the acquirer that reverse a transaction, in whole or in part, and transfer value from the acquirer to the issuer (e.g., customer return of goods, complaints, merchant-identified fraud, duplicate transaction entry).

	General-Purpose Debit Card Network
Item	**Definition**
5	**Net, purchase transactions:** Transactions that have been authorized and settled. Exclude denials, transactions that are pre-authorization only, cash advances, chargebacks, and other adjustments and returns.
7a.1	**Chip:** Transactions for which account information taken from a computer microchip embedded in a card or mobile device that securely stores data to be read via contact or contactless/NFC communications with a merchant payment device or terminal. Include EMV and all other types of chip transactions with a card or mobile device. Report only in-person transactions.
7a.1.1	**EMV:** "Dipped" transactions are initiated by inserting a card with an embedded EMV microchip into a merchants chip-enabled terminal. Data are tokenized and processed using a unique one-time use code and can be authenticated with Chip-and-Signature and Chip-and-PIN.
7a.1.2	**RFID/NFC (including both mobile and card-based chips):** "Tap and Pay" contactless transactions use Radio Frequency Identification (RFID) and/or a specialized subset of Near-field Communications (NFC) standards to initiate a card-based payment. NFC is designed to be a secure form of data exchange and can support EMV transactions. Contactless authentication can utilize a physical card, fob, or sticker that is “tapped” to pay at a POS terminal. Examples include MasterCard Tap & Go®, Visa payWave and Exxon's SpeedPass.
7a.2	**Scanner (Barcode/QR code):** "Scanner" initiated transactions are when a merchant utilizes an optical Barcode reader to access cardholder data. Quick-response (QR) and other images can be used to provide required account information from a smartphone or printed image.
7a.3	**Magnetic stripe:** "Swipe" transactions where cardholder and account information contained in a magnetic stripe are read when a card passes through a reader. This would also include MIST technology used by Samsung Pay to spoof the swipe to transmit track data from magstripe cards to POS terminals.
7a.4	**Card number/cashier key entry:** "Keyed" transactions are initiated by a merchant when the POS terminal cannot read the magnetic-stripe of the card and the cashier must key in the cardholder data. Merchants that are not EMV chip-enabled may be required to support manual key entry as a method of backup acceptance should a magnetic-stripe read on a card fail.
7a.5	**Other:** Any other method used to provide customer card account information not listed above.
8a	**PIN (personal identification number):** In-person transactions where a cardholder enters their Personal Identification Number (PIN) to authenticate the card purchase. This would also include remote transactions where PINs are entered through secure methods like Acculynk.

	General-Purpose Debit Card Network
Item	**Definition**
8b	**Zip code:** Zip codes of cardholders' billing address are used with Address Verification Systems (AVS). AVS is often used as an anti-fraud method for unattended terminals like fuel dispensers. Address verification systems can also be used for remote purchases.
8c	**Card identification number:** A number (typically 3- or 4-digits) printed on the card that provides additional identification and verification of a cardholder for authenticating purchases. This includes a variety of codes supported by card networks such as CIN, CID, CVV, CVV2, or CSC.
8d	**Other/unknown:** All other transactions where one of the listed types of data was not recorded. Include transactions associated with no authentication or transactions using an unlisted/unmeasured type of authentication such as low-value transactions (e.g. under $50) where no signature or PIN entry is required at certain merchant classes such as Grocery or Quick Service Restaurants.
10a	**Lost or stolen card:** Fraudulent transactions via a card reported as lost or stolen.
10b	**Card issued but not received:** Fraudulent transactions reported to be via an intercepted new or replacement card in transit that was activated by someone other than the cardholder.
10c	**Fraudulent application:** Fraudulent transactions reported to be via a new card that was issued to someone other than the cardholder using falsified information or a stolen identity.
10d	**Counterfeit card:** Fraudulent point-of-sale transactions via an altered or cloned card.
10e	**Fraudulent use of account number:** Fraudulent transactions using account number and other card and cardholder details, typically remotely.
10f	**Other (including account takeover):** All other fraudulent transactions not included the above categories. In particular, "other" covers account takeover, a form of identity theft whereby an unauthorized party gains access to and use of an existing card account.
18	**Transaction value distribution:** Your best estimate for the number and dollar value of transactions that fall within the "dollar size bands" requested.
19	**Total cards:** All issued, activated, and unexpired general-purpose debit cards (linked to U.S.-domiciled accounts).
19	**Active cards:** Cards outstanding with a minimum level of purchase activity according to your organization's definition.

	General-Purpose Prepaid Card Network
Item	Definition
	United States: The states, territories, and possessions of the U.S., the District of Columbia, the Commonwealth of Puerto Rico, or any political subdivision of any of the foregoing.
1a	**Denials/declines:** Transaction attempts that receive a denial response by the host authorization system and do not result in an authorized transaction.
2a	**Pre-authorization only:** Transactions that are approved but not settled (e.g., the initial amount which a rental agency, hotel, or fuel dispenser operator receives authorization, but final payment and amount transfer is never made).
3	**Net, authorized & settled transactions:** Transactions initiated by the acquirer that are completed with the final payment amount transferred from the acquirer to the issuer. Such transactions include those that are subsequently reversed through a chargeback, or other adjustment or return.
3a	**Cash-back at the point of sale:** Purchase transactions that include an amount of cash given back to the card user. A point-of-sale (POS) purchase transaction with cash back is counted as one transaction.
3.b.1	**Chargebacks:** Transactions initiated by the issuer that reverse a transaction, in whole or in part, and transfer value from the acquirer to the issuer (e.g., customer disputes, fraud, processing errors, authorization issues, or non-fulfillment of copy requests). A chargeback provides the issuer with a way to return a disputed transaction, typically on behalf of the cardholder.
3b.2	**Other adjustments and returns:** Transactions initiated by the acquirer that reverse a transaction, in whole or in part, and transfer value from the acquirer to the issuer (e.g., customer return of goods, complaints, merchant-identified fraud, duplicate transaction entry).
4	**Net, purchase transactions:** Transactions that have been authorized and settled. Exclude denials, transactions that are pre-authorization only, cash advances, chargebacks, and other adjustments and returns.
6a.1	**Chip:** Transactions for which account information taken from a computer microchip embedded in a card or mobile device that securely stores data to be read via contact or contactless/NFC communications with a merchant payment device or terminal. Include EMV and all other types of chip transactions with a card or mobile device. Report only in-person transactions.
6a.1.1	**EMV:** "Dipped" transactions are initiated by inserting a card with an embedded EMV microchip into a merchants chip-enabled terminal. Data are tokenized and processed using a unique one-time use code and can be authenticated with Chip-and-Signature and Chip-and-PIN.
6a.1.2	**RFID/NFC (including both mobile and card-based chips):** "Tap and Pay" contactless transactions use Radio Frequency Identification (RFID) and/or a specialized subset of Near-field Communications (NFC) standards to initiate a card-based payment. NFC is designed to be a secure form of data exchange and can support EMV transactions. Contactless authentication can utilize a physical card, fob, or sticker that is “tapped” to pay at a point-of-sale (POS) terminal. Examples include MasterCard Tap & Go®, Visa payWave and Exxon's SpeedPass.

	General-Purpose Prepaid Card Network
Item	**Definition**
6a.2	**Scanner (Barcode/QR code):** "Scanner" initiated transactions are when a merchant utilizes an optical Barcode reader to access cardholder data. Quick-response (QR) and other images can be used to provide required account information from a smartphone or printed image.
6a.3	**Magnetic stripe:** "Swipe" transactions where cardholder and account information contained in a magnetic stripe are read when a card passes through a reader. This would also include MIST technology used by Samsung Pay to spoof the swipe to transmit track data from magstripe cards to POS terminals.
6a.4	**Card number/cashier key entry:** "Keyed" transactions are initiated by a merchant when the POS terminal cannot read the magnetic-stripe of the card and the cashier must key in the cardholder data. Merchants that are not EMV chip-enabled may be required to support manual key entry as a method of backup acceptance should a magnetic-stripe read on a card fail.
6a.5	**Other:** Any other method used to provide customer card account information not listed above.
7a	**PIN (personal identification number):** In-person transactions where a cardholder enters their Personal Identification Number (PIN) to authenticate the card purchase. This would also include remote transactions where PINs are entered through secure methods like Acculynk.
7b	**Zip code:** Zip codes of cardholders' billing address are used with Address Verification Systems (AVS). AVS is often used as an anti-fraud method for unattended terminals like fuel dispensers. Address verification systems can also be used for remote purchases.
7c	**Card identification number:** A number (typically 3- or 4-digits) printed on the card that provides additional identification and verification of a cardholder for authenticating purchases. This includes a variety of codes supported by card networks such as CID, CIN, CVV, CVV2, or CSC.
7d	**Other/unknown:** All other transactions where one of the listed types of data was not recorded. Include transactions associated with no authentication or transactions using an unlisted/unmeasured type of authentication such as low-value transactions (e.g. under $50) where no signature or PIN entry is required at certain merchant classes such as Grocery or Quick Service Restaurants.
9a	**Lost or stolen card:** Fraudulent transactions via a card reported as lost or stolen.
9b	**Card issued but not received:** Fraudulent transactions reported to be via an intercepted new or replacement card in transit that was activated by someone other than the cardholder.
9c	**Fraudulent application:** Fraudulent transactions reported to be via a new card that was issued to someone other than the cardholder using falsified information or a stolen identity.

	General-Purpose Prepaid Card Network
Item	**Definition**
9d	**Counterfeit card:** Fraudulent point-of-sale transactions via an altered or cloned card.
9e	**Fraudulent use of account number:** Fraudulent transactions using account number and other card and cardholder details, typically remotely.
9f	**Other (including account takeover):** All other fraudulent transactions not included the above categories. In particular, "other" covers account takeover, a form of identity theft whereby an unauthorized party gains access to and use of an existing card account.
17	**Transaction value distribution:** Your best estimate for the number and dollar value of transactions that fall within the "dollar size bands" requested.
18	**Total cards:** All issued, activated, and unexpired general-purpose prepaid cards (linked to U.S.-domiciled accounts).
18	**Active cards:** Cards outstanding with a minimum level of purchase activity according to your organization's definition.

	Automated Teller Machine Card Network
Item	**Definition**
	United States: The states, territories, and possessions of the U.S., the District of Columbia, the Commonwealth of Puerto Rico, or any political subdivision of any of the foregoing.
1a	**Denials/declines:** Transaction attempts that receive a denial response by the host authorization system and do not result in an authorized transaction.
1c.2.1	**Government-administered general-purpose prepaid cards:** Cash withdrawals made with cards (including virtual cards) issued to a consumer for the purpose of providing government benefits. Include state and federal programs with cash benefits such as unemployment, TANF, or Social Security.
2a	**Lost or stolen card:** Fraudulent transact-ions via a card reported as lost or stolen.
2b	**Card issued but not received:** Fraudulent transactions reported to be via an intercepted new or replacement card in transit that was activated by someone other than the cardholder.
2c	**Fraudulent application:** Fraudulent transactions reported to be via a new card that was issued to someone other than the cardholder using falsified information or a stolen identity.
2d	**Counterfeit card:** Fraudulent point-of-sale transactions via an altered or cloned card.

	Automated Teller Machine Card Network
Item	**Definition**
2e	**Other (including account takeover):** All other fraudulent transactions not included the above categories. In particular, "other" covers account takeover, a form of identity theft whereby an unauthorized party gains access to and use of an existing card account.
3a	**Chip-accepted terminals:** An ATM terminal that accepts card with a computer microchip (including EMV and other types of chip cards) that securely stores the card data that currently resides on the magnetic stripe. These can also include terminals that accept contactless NFC transactions from a mobile phone or other device.

	Private-Label Prepaid Card Issuer and Processor
Item	**Definition**
	United States: The states, territories, and possessions of the U.S., the District of Columbia, the Commonwealth of Puerto Rico, or any political subdivision of any of the foregoing
1a	**Denials/declines:** Transaction attempts that receive a denial response by the host authorization system and do not result in an authorized transaction.
2a	**Pre-authorization only:** Transactions that are temporarily authorized but not completed or posted, or the portion of authorized amounts that are not included in a final posting.
3	**Completed transactions (posted to card accounts):** Purchase transactions (including any cash-back) that are completed and posted to the private-label card account for payment. Such transactions include those that are subsequently reversed in an adjustment or return requested by the merchant or cardholder, defined below.
3a	**Cash-back at the point of sale:** Purchase transactions that include an amount of cash given back to the card user. A point-of-sale (POS) purchase transaction with cash back is counted as one transaction.
3b	**Adjustments and returns:** Completed and posted transactions that are subsequently reversed, in whole or in part, and that transfer value back to the card account (e.g., customer return of goods, complaints, disputed charges, fraud, duplicate transaction entry).
4	**Net, purchase transactions:** Completed purchase transactions that have not been reversed. Exclude denials, transactions that are pre-authorization only, and adjustments and returns defined above. For value, also exclude the dollar amount of the cash-back at the point of sale.
5a.1	**Transactions initiated with a mobile device:** Transactions initiated on a smart device in person with NFC using a "digital wallet".

	Private-Label Prepaid Card Issuer and Processor
Item	**Definition**
6a	**Lost or stolen card:** Fraudulent transactions via a card reported as lost or stolen.
6b	**Card issued but not received:** Fraudulent transactions reported to be via an intercepted new or replacement card in transit that was activated by someone other than the cardholder.
6c	**Fraudulent application:** Fraudulent transactions reported to be via a new card that was issued to someone other than the cardholder using falsified information or a stolen identity.
6d	**Counterfeit card:** Fraudulent point-of-sale transactions via an altered or cloned card.
6e	**Fraudulent use of account number:** Fraudulent transactions using account number and other card and cardholder details, typically remotely.
6f	**Other (including account takeover):** All other fraudulent transactions not included the above categories. In particular, "other" covers account takeover, a form of identity theft whereby an unauthorized party gains access to and use of an existing card account.
11	**Total cards:** All issued, activated, and unexpired private-label prepaid cards (linked to U.S.-domiciled accounts).
11	**Active cards:** Cards outstanding with a minimum level of purchase activity according to your organization's definition.