

The Initial Effects of EMV Migration on Chargebacks in the United States

Fumiko Hayashi, Zach Markiewicz, and Sabrina Minhas

December 2018

RWP 18-10

<https://dx.doi.org/10.18651/RWP2018-10>

FEDERAL RESERVE BANK *of* KANSAS CITY



The Initial Effects of EMV Migration on Chargebacks in the United States*

Fumiko Hayashi, Zach Markiewicz and Sabrina Minhas[†]

December 2018

Abstract

To reduce counterfeit fraud in the card-present (CP) environment, the United States started migrating to EMV chip technology in the mid-2010s. Since October 2015, merchants have been liable for counterfeit fraud committed using EMV cards if the merchants have not adopted EMV chip-readable terminals. Merchants are held liable through chargebacks. This study examines the initial effects of the EMV liability shift on fraud chargeback and merchant loss rates using data from merchant processors and PIN debit networks. Combined with gross fraud rates—overall fraud rates regardless of who incurs fraud losses—estimated in other studies, the results of our study suggest that merchants have faced a significantly higher share of fraud losses since the shift; however, this spike will decline if merchants continue to adopt EMV. Merchant fraud loss rates for signature-based transactions in the CP channel increased sixfold, but the rates significantly vary between magnetic stripe (mag-stripe) and chip-to-chip transactions. The rates for mag-stripe transactions are over 9 basis points in value for all merchants combined, and vary across merchant categories, while the rates for chip-to-chip transactions are very low, around 0.02 basis points, across all merchant categories. Because the gross fraud rates of mag-stripe transactions did not increase in the same period, our results suggest that the higher merchant fraud loss rates for mag-stripe transactions after the liability shift is mainly due to the liability shift. Compared to signature-based transactions, fraud chargeback rates of PIN debit transactions in the CP channel are much lower. Our results suggest that both EMV and PIN are effective in reducing merchant fraud loss rates. However, we need detailed gross fraud rates to examine how effective EMV and PIN are in reducing fraud itself in the CP channel. Our results for card-not present (CNP) fraud chargeback and merchant loss rates are mixed. Both rates increased for some merchant categories, but the rates for all merchants combined actually declined in our data. This decline is likely due to the underrepresentation of signature-based CNP transactions in our data. The gross fraud rates for CNP transactions actually increased in the same period and merchants are generally liable for CNP fraud.

JEL Classification: E42, L81

Keywords: Chargebacks, fraud, EMV liability shift, authentication methods

* We thank merchant processors and debit card networks who participated in this study, the Merchant Advisory Group and the Debit Network Alliance for soliciting those processors and debit card networks, and participants at the Bank of Canada's Retail Payments Workshop and the Federal Reserve Bank of Kansas City seminar for their valuable comments. The views expressed herein are those of the authors and do not necessarily reflect the views of the Federal Reserve Bank of Kansas City, the Federal Reserve Bank of Chicago, or the Federal Reserve System.

[†] Fumiko Hayashi is a payments policy advisor and economist at the Federal Reserve Bank of Kansas City, Zach Markiewicz is a marketing research specialist at the Federal Reserve Bank of Chicago, and Sabrina Minhas is a research associate at the Federal Reserve Bank of Kansas City. Their email addresses are fumiko.hayashi@kc.frb.org, zach.markiewicz@chi.frb.org, and sabrina.minhas@kc.frb.org.

1. Introduction

After many other developed countries had already migrated to chip-card technology, the U.S. payment card industry started migrating to that technology in the mid-2010s. The chip-technology, which is also known as Europay, MasterCard, and Visa (EMV) technology, uses dynamic data to strongly authenticate each and every transaction, thereby mitigating counterfeit fraud in the card-present (CP) environment. Instead of mandating EMV migration, U.S. payment card networks changed CP fraud liability allocation between issuers and merchants to give both parties incentives to adopt EMV. Prior to the liability shift, issuers were generally liable for CP fraud. From October 1, 2015, however, the fraud liability for a CP transaction shifted to the merchant if the merchant has not adopted EMV, but the issuer has – in other words, if the merchant has not installed point-of-sale (POS) terminals that can accept chip cards, but the issuer has issued chip cards.¹ If neither or both parties have adopted EMV, then the issuer is generally liable for fraudulent transactions. Issuers' and merchants' EMV adoption does not affect card-not-present (CNP) fraud liability allocation, and merchants are generally liable for CNP fraud.

Chargebacks are used to assign fraud liability to merchants. A cardholder reports a fraudulent transaction to the card issuer when he finds a transaction he did not authorize on his payment card statement. If the issuer believes the merchant is liable for the fraudulent transaction according to rules set out by the card network, the issuer initiates a chargeback to the merchant. When the card issuer initiates a chargeback, the merchant processor, which is the entity that provides payment card processing services for the merchant, returns the funds to the issuer from the merchant's account. The funds may again be deposited to the merchant account if the merchant successfully reclaims the funds by disputing the chargeback. As a result, merchant

¹ For gas stations, the liability shift does not take effect until October 2020.

losses are a subset of chargebacks. While chargebacks are also used for other reasons, such as processing errors, problems related to authorization or cancelation, product quality, and non-receipt of goods and services, fraud is the most common reason for a chargeback, according to Hayashi, Markiewicz and Sullivan (2016).²

The purpose of this study is to examine the initial effects of EMV migration on chargebacks. Whether fraud chargeback rates for CP transactions, measured as the number or value of CP transactions charged back to merchants due to fraud relative to the number or value of CP (sales) transactions, increases or decreases depends on two factors. The first factor is how much lower chargeback rates are for CP chip-to-chip transactions relative to the rates for CP magnetic stripe (mag-stripe) transactions. A chip-to-chip transaction is initiated with a chip card and accepted by a chip readable POS terminal. In contrast, a mag-stripe transaction relies on information from the mag-stripe of a chip or non-chip card. The second factor is how CP transactions are distributed between chip-to-chip and mag-stripe transactions. If chargeback rates for CP chip-to-chip transactions are sufficiently low and the share of chip-to-chip transactions in the CP transactions is sufficiently large, then chargeback rates for CP transactions would decline; otherwise, the rates would increase. Although the EMV liability shift only applies to CP transactions, it may increase chargeback rates for CNP transactions if EMV migration has induced fraudsters to focus more on CNP transactions. Since merchants are generally liable for CNP fraud, an increase in CNP fraud rates implies an increase in chargeback rates for CNP transactions. In many other countries, CNP fraud increased after EMV migration (Hayashi, Moore and Sullivan 2015).

² For details about chargebacks, see Hayashi, Markiewicz and Sullivan (2016) and Appendix A.

This study also examines how the EMV liability shift has affected chargeback rates for different authentication methods – signature versus personal identification number (PIN).

Outside the United States, chip cards are often used with PIN for CP transactions, while in the United States, chip *credit* cards are used with signature, but chip *debit* cards are used with both signature and PIN.³ Chip cards with PIN can address counterfeit fraud as well as fraud due to lost or stolen cards because only the cardholders should know their PIN. In contrast, chip cards with signature (or no authentication) can address counterfeit fraud only.⁴

Combined with gross fraud rates—overall fraud rates regardless of who incurs fraud losses—estimated in other studies, the results of our study inform how card fraud losses are distributed between merchants and other parties, including card issuers and cardholders. Understanding the distribution of fraud losses allows us to examine the extent to which the current distribution properly incentivizes the parties who can address fraud to actually do so. If the liability is not properly allocated to the parties who can address fraud, their incentives may be insufficient to adequately secure payments (Hayashi, Moore and Sullivan 2015).

In this study, we use chargeback and sales data collected from merchant processors and PIN debit card networks. Two samples focusing on signature-based general-purpose card transactions are collected from merchant processors and one sample focusing on PIN-debit card transactions is from PIN debit card networks. The two samples on signature-based transactions differ in time periods: one is before the EMV liability shift and the other is immediately after the shift. The time period of the PIN-debit sample is immediately after the shift.

³ From April 2018, card networks dropped the signature requirement for credit and signature debit card transactions.

⁴ Authentication technologies such as biometrics may be stronger authentication method than static PIN and become increasingly available with mobile devices. However, those technologies have not been widely used for payments in the United States.

We find fraud chargeback rates for signature-based transactions have significantly increased since the EMV liability shift. The increase is associated with CP transactions rather than CNP transactions. While CNP fraud chargeback rates are still higher than CP fraud chargeback rates, the difference between the rates decreases. For some merchant categories, CNP fraud chargeback rates have increased since the liability shift, but the rates have declined for all merchants combined in our data. This decline is likely due to the underrepresentation of signature-based CNP transactions in our data. The gross fraud rates for CNP transactions have actually increased in the same period and merchants are generally liable for CNP fraud. The increase in the CP fraud chargeback rates may be mainly caused by the liability shift because the gross fraud rates for CP transactions have not increased in the same period. For at least some merchant categories, however, an increase in fraud itself may be another source. We observe an increase in the CP fraud chargeback rate at gas stations, for which the liability shift has not taken place. This likely implies that fraudsters have worked harder to exploit the weak security of mag-stripe before the U.S payment card industry fully migrates to EMV.

Among signature-based CP transactions, fraud chargeback rates for chip-to-chip transactions are significantly lower than those for mag-stripe transactions. Merchant fraud loss rates for chip-to-chip transactions are around 0.02 basis points (bps) in value across all merchant categories in our data. This result is expected as issuers, not merchants, are generally liable for chip-to-chip transaction fraud. In contrast, merchant fraud loss rates for mag-stripe transactions are over 9 bps for all merchants combined and vary by merchant category.

Compared to signature-based transactions, fraud chargeback rates for PIN-based transactions are much lower. This is partly due to the very small share of CNP transactions (which are more fraud prone) among PIN-based transactions. Even within CP transactions, fraud

chargeback rates for PIN-based transactions are much smaller. Within CP chip-to-chip transactions, chargeback rates for PIN-based transactions are still smaller than those for signature-based transactions.

Our results suggest that merchants have faced a significantly higher share of fraud losses since the EMV liability shift; however, this spike will decline if merchants continue to adopt EMV. The results also suggest that both EMV and PIN are effective in reducing merchant fraud loss rates. However, we need detailed gross fraud rates to examine how effective EMV and PIN are in reducing fraud itself in the card-present channel.

The rest of this paper is organized as follows. Section 2 explains the U.S. payment card industry's EMV migration. Section 3 describes our data. Section 4 provides our results and discusses their implications for merchants and policymakers. Section 5 concludes.

2. EMV migration in the United States

The United States is a late adopter of EMV technology: it waited until 2011 when a card network announced its EMV migration plan. In many other countries, the national level of EMV adoption started during the 2000s.⁵ European countries were the earliest adopters. The United Kingdom began EMV migration in 2002, reaching nearly full migration by 2006. In France, a national rollout of EMV chip-and-PIN cards was announced in 2003 and finalized by the end of 2006. In North America, Mexico began EMV migration in 2006, while Canada began a national rollout of EMV chip-and-PIN cards in 2008 (Simmons 2016).

EMV migration in the United States is different from other countries in part due to a lack of government initiative or mandate requiring the migration. Instead, the migration has been led

⁵ See King (2012) for detailed descriptions about EMV migration in other countries.

by industry members. Card networks, including Visa, MasterCard, American Express and Discover, announced in 2011 and 2012 that the liability shift would occur in October 2015. To support industry cooperation and the alignment of the move to EMV technology, the EMV Migration Forum, a cross-industry body including card networks, financial institutions, merchants, and other participants in the U.S. card industry, was formed in 2012.

Since then, the migration has faced several challenges. First, a slight variation in the liability shift across networks made EMV adoption more complex.⁶ While counterfeit fraud liability shift applies to all networks, lost-or-stolen fraud liability shift applies only to MasterCard, American Express and Discover. Once card issuers issue EMV cards, the liability for counterfeit fraud in the CP environment shifts to the merchant if the merchant has not adopted chip-readable POS terminals, but the liability remains with the issuer if the merchant has adopted chip-readable terminals. Visa and domestic PIN debit networks have not implemented the liability shift for lost-or-stolen fraud, while MasterCard, American Express and Discover have shifted lost-or-stolen fraud liability to the party with the higher risk environment. In a security hierarchy, these three card networks consider an EMV card used with PIN to be more secure than an EMV card used without PIN.⁷

Second, the U.S. debit card industry faced a unique challenge related to a routing requirement of Regulation II. According to Regulation II, debit cards must carry at least two unaffiliated card networks to process transactions on the cards (Hayashi 2012). EMV technology, however, is a standard developed by EMVCo, which is now owned by six major global card brands including Visa, MasterCard, American Express, Discover, JCB and UnionPay. Visa and

⁶ See US Payments Forum (2017) for detailed liability shifts by card network.

⁷ Issuers are generally liable for lost-or-stolen fraud if merchants adopt POS terminals that can read both chip and PIN.

MasterCard, which have the intellectual property right to EMV chips, could have met the Regulation II requirement by making their chips available only to each other or a subset of PIN debit networks selected by them. But such arrangements threaten the interoperability among PIN debit networks, resulting in a competitive advantage for Visa and MasterCard over domestic PIN debit networks.

After a long debate among card networks, Visa and MasterCard eventually made a series of bilateral agreements with domestic PIN debit networks starting in February 2014 (Digital Transactions News 2014). The two global card networks agreed to provide free license of their common application identifier (AID) technology to domestic debit networks, which enables merchants to route EMV debit transactions in compliance with regulatory requirements.

A third challenge was due to EMV terminal certification delays. For merchants, installing EMV chip-readable POS terminals is not sufficient to avoid liability. After installation, EMV terminals need to be certified before they can process EMV transactions. Some merchants, primarily mid- and small-sized, were unable to process chip-to-chip transactions in time for the liability shift due to EMV terminal certification delays. As a result, merchants who installed EMV terminals but were unable to receive the proper certification in time were still liable for losses from counterfeit or lost-or-stolen fraud on chip cards. Large merchants, however, may have been prioritized by merchant processors to receive the certification and be able to process EMV transactions earlier than mid- and small-sized merchants.

In response to the delayed certification process, card networks provided some relief to merchants. For example, Visa reduced merchants' liability for certain fraudulent transactions until April 2018 (PYMNTS 2016). Beginning in July 2016, counterfeit fraud would not be charged back to merchants if the value of such fraud is under \$25. As of October 2016, Visa also

limited the number of fraudulent transactions that could be charged back by issuers. After 10 fraudulent counterfeit transactions per account, the issuer assumed liability. The first limitation occurred during the time period of our data.

3. Data

In this study, we compare chargeback and merchant loss rates before and after the EMV liability shift for various types of card payments, such as CP versus CNP, chip-to-chip versus mag-stripe, PIN versus signature (or no authentication), and by merchant category. Chargeback rates in number or in value for a certain type of card payment are measured as the number or value of payments for that type of card payment that are charged back to merchants relative to the number or value of corresponding sales transactions. For example, a chargeback rate in value for CP chip-to-chip signature-based transactions at department stores is equal to the value of chargebacks made for CP chip-to-chip signature-based transactions at department stores divided by the value of CP chip-to-chip signature-based sales transactions at department stores. To this end, we use chargeback and sales data furnished by merchant processors and PIN debit networks.

Our data include three samples. From merchant processors, we collect two samples focusing on signature-based, general-purpose card transactions (i.e., general-purpose credit and signature debit or prepaid card transactions). The time period of the two samples is different. The first sample covers a one-year period before the EMV liability shift, from October 1, 2013 to September 30, 2014. This sample is the same one used in Hayashi, Markiewicz and Sullivan (2016). The second sample covers a one-year period immediately after the EMV liability shift, from October 1, 2015 to September 30, 2016. While these two samples include both four-party scheme (Visa and MasterCard) and three-party scheme (American Express and Discover)

signature-based transactions, we focus our analysis on four-party scheme transactions in this paper.⁸ A third sample is from PIN debit networks, which covers PIN-debit card transactions for one year immediately after the EMV liability shift, from October 1, 2015 to September 30, 2016. Although PIN debit networks do not typically have a chargeback process, funds of transactions can be reversed as adjustments.

To measure chargeback rates accurately, it is ideal to keep track of chargebacks for sales transactions made in a certain period of time (say, the calendar year 2016). However, this approach is very challenging in practice because some chargebacks take more than a year to resolve. Thus, we take an alternative approach: we collect data on chargebacks received by the processors' (or PIN debit networks') merchants and sales transactions made at these merchants for the same one-year period. As for the one-year period, we choose from the beginning of the fourth quarter 2013 or 2015 to the end of the third quarter 2014 or 2016, instead of the calendar year 2014 or 2016 for two reasons. The first reason is to avoid potentially biased chargeback statistics due to the holiday shopping season.⁹ The second reason is to align the time period of our two samples with the date of the EMV liability shift, which was the beginning of the fourth quarter 2015.

Our three samples do not include individual chargebacks or sales transactions; instead, chargebacks and sales transactions are aggregated by merchant processors and PIN debit

⁸ For three-party scheme chargebacks, merchant processors process transactions for small- and mid-sized merchants because large merchants often work directly with the card networks. To avoid potential bias in chargeback rates caused by differences in merchant size, this paper focuses on four-party scheme transactions.

⁹ Retail sales during the holiday shopping season typically account for 20 percent of retail sales during the entire year. Therefore, the treatment of holiday shopping sales and their chargebacks is important. Our chargeback and sales data exclude chargebacks and sales during the holiday shopping season in 2014 or in 2016 but include those in 2013 or in 2015. If we use the calendar year 2014 (or in 2016) as for the one-year period, many chargebacks for transactions made during the holiday shopping season in 2014 (or in 2016) would not be in the chargeback data, but those in 2013 would. On the other hand, sales transactions made during the holiday shopping season in 2014 (or in 2016) would be in the sales data but those in 2013 (or in 2015) would not. This may cause underestimation of chargeback rates because holiday sales in 2014 (or in 2016) increased from that in 2013 (or in 2015).

networks at our requested level. To examine chargeback and merchant loss rates, we asked merchant processors and PIN debit networks to provide the number and value of chargebacks their merchants received, as well as the number and value of chargebacks the merchants successfully disputed. The merchants' losses are calculated by subtracting the latter from the former.

To generate detailed chargeback and merchant loss rates, we asked merchant processors and PIN debit networks to divide the numbers and values of chargebacks merchants received and the numbers and values of chargebacks merchants successfully disputed into different groups. Six criteria are used to create the different groups. First, those numbers and values are divided by card network. Merchant processors divide their chargebacks for signature-based transactions into four-party schemes (Visa and MasterCard) and three-party schemes (American Express and Discover).¹⁰ PIN-debit networks provide the number and value of chargebacks/adjustments in their own network. Second, the numbers and values by card network are separated into two transaction channels – CP and CNP.¹¹ CP chargebacks and chargebacks disputed by merchants are further separated into two transaction types – whether a chargeback is for a chip-to-chip or mag-stripe transaction. PIN networks further divide CP chip-to-chip or mag-stripe chargebacks based on authentication method – with or without PIN.

These detailed numbers and values of chargebacks and chargebacks disputed by merchants are also divided into seven reason code categories for signature-based transactions. The seven reason code categories are fraud, non-receipt goods and services, product quality, cancellation, non-receipt information, processing errors, and authorization issues.¹² For PIN-

¹⁰ In this study, we use transactions of four-party schemes. See footnote 8 for our reason.

¹¹ The numbers and values of CNP chargebacks are further divided into e-Commerce and other CNP, such as telephone and mail orders.

¹² See Appendix B for reason codes.

debit transactions, the detailed numbers and values of chargebacks are divided into two – whether a chargeback is due to fraud or not.

Finally, we asked merchant processors and PIN debit networks to provide the detailed numbers and values of chargebacks and chargebacks disputed by merchants not only for all merchants they process but also by merchant category. Five major categories are selected. The first includes department, big box, and apparel stores. The second includes grocery, food, and drug stores. The third is gas stations. The fourth includes restaurants, drinking places and caterers. The fifth category covers the travel industry, including airlines, car rentals and hotels.

To calculate detailed chargeback and merchant loss rates, detailed sales data are essential. We asked merchant processors and PIN debit networks to provide the number and value of sales transactions that are divided in the same way as the number and value of chargebacks, except for the reason code categories.

Several merchant processors and PIN debit networks participated in our study and provided detailed chargebacks (or adjustments) and sales data. Processors and networks are assured anonymity in order to encourage participation and detailed responses. The PIN debit networks who participated in this study, altogether, processed approximately 20 percent of PIN-debit purchase transactions in 2016.¹³ The merchant processors who provided data for our two samples do not completely overlap. The merchant processors for our first sample, from October 2013 to September 2014, altogether processed a little over 20 percent of signature-based, general-purpose, four-party scheme transactions in 2014. The processors for our second sample,

¹³ PIN-debit ATM transactions are excluded.

from October 2015 to September 2016, altogether processed about 30 percent of transactions in 2016.¹⁴

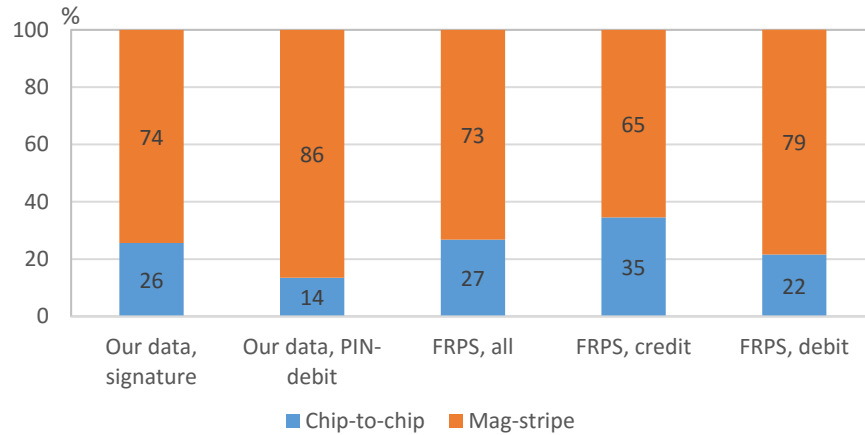
Although our data include 20 to 30 percent of card transactions, our data are not representative of all signature-based, general-purpose, four-party scheme transactions or all PIN-debit transactions. Our data underrepresent signature-based CNP transactions and potentially over-represent PIN-debit CNP transactions. The Federal Reserve Payment Study 2017 Supplement (FRPS 2017) reports that 44 percent of general-purpose card transactions in terms of value are CNP, but the CNP share in our signature-based data is 25 percent. Conversely, the Federal Reserve Board of Governors (FR BOG 2016) reports that the CNP share of PIN-debit transactions is 3.3 percent in 2015, while the share in our data is 9 percent.

Within signature-based CP transactions, the distribution between chip-to-chip and mag-stripe transactions in our data, however, is similar to the distribution reported in FRPS (2017): the chip-to-chip share in terms of value is 26 percent in our data and 27 percent in FRPS (Chart 1). In contrast, the chip-to-chip share in CP transactions is only 14 percent in our PIN-debit data, suggesting that our PIN-debit data are likely to underrepresent merchants who have adopted chip-readable terminals. According to FRPS (2017), the chip-to-chip share in combined signature- and PIN-debit transactions in terms of value is 22 percent. According to the Pulse debit issuer study in 2017, 59 percent of chip-to-chip transactions are PIN-debit transactions in terms of number while 41 percent of them are signature-debit transactions. If the average transaction size of chip-to-chip debit transactions is similar between PIN and signature

¹⁴ Merchant processors that provided data for the October 2015–September 2016 period, altogether, processed more than 50 percent of signature-based, general-purpose, four-party scheme transactions in 2016. However, about 20 percent of transactions are not used in our analysis due to insufficient information.

transactions, then these findings suggest the chip-to-chip share in PIN-debit is greater than 22 percent.

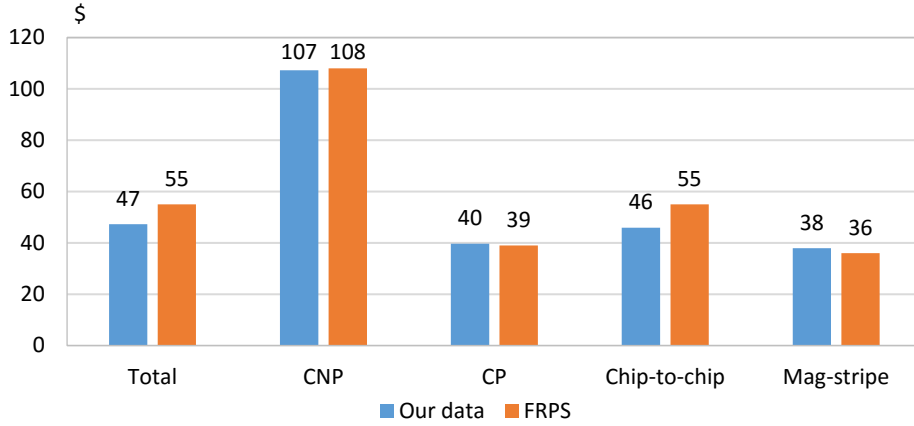
Chart 1: Distribution between chip-to-chip and mag-stripe transactions in CP transaction value: our data vs. FRPS



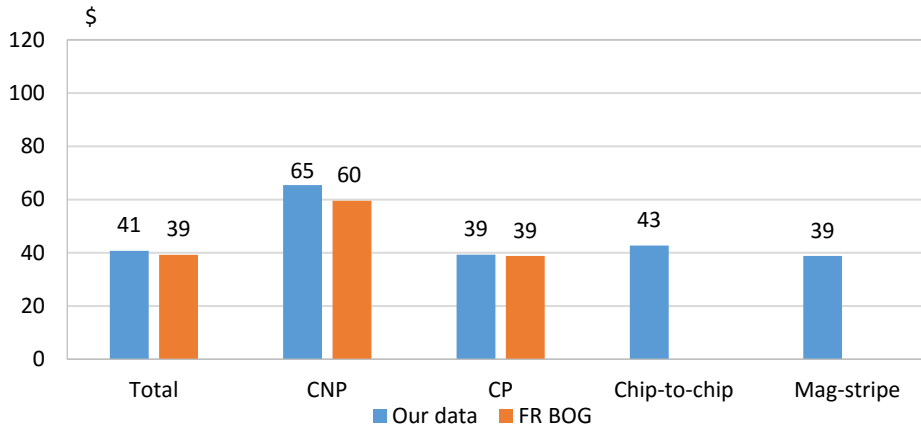
Although there are differences between our data and the nationally representative data of FRPS (2017) or FR BOG (2016) in terms of transaction shares by channel, our data show similarity with those data in terms of the average transaction size (Chart 2). We compare our signature-based data against FRPS data, which include signature-based and PIN-debit. While the average transaction size for all transactions differs between our data and FRPS, the two data have almost identical average transaction size for CNP and CP transactions. Our PIN-debit data and FR BOG data have similar average transaction size for all transactions and for CP transactions.

Chart 2: Average transactions size: our data vs. FRPS or FR BOG

A: Signature-based



B: PIN-debit



4. Results

This section provides various statistics related to total chargeback (or adjustment) rates, which include all chargebacks regardless of reason, and statistics related to fraud chargeback rates. These statistics are weighted averages calculated using the number or value of sales transactions and the number or value of chargebacks each of the processors’ and PIN debit networks’ merchants received. Because merchants successfully dispute some of the chargebacks

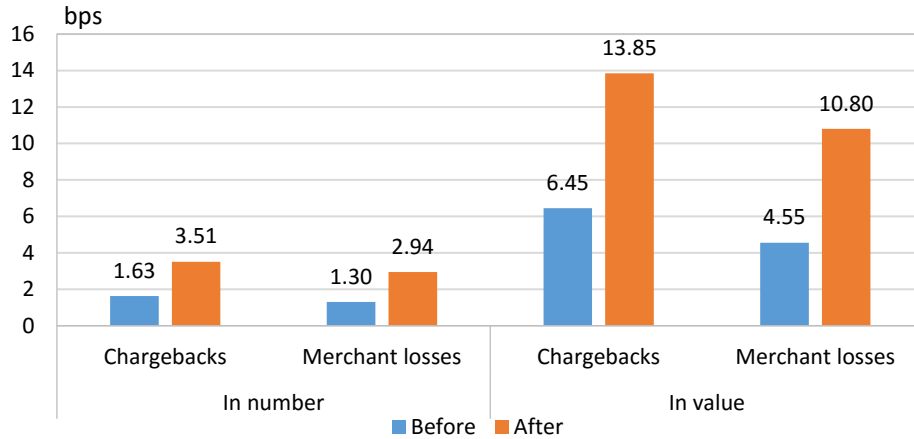
requested by issuers, we show both chargeback rates and merchant loss rates. Chargeback rates measure the number or value of chargebacks relative to the number or value of sales transactions, while merchant loss rates measure the number or value of transactions for which merchants ultimately lost funds via the chargeback process, relative to the number or value of sales transactions.

In this section, we first compare chargeback rates for signature-based transactions before and after the EMV liability shift. Second, we focus on chargebacks for CP transactions and compare chip-to-chip and mag-stripe chargeback rates. Third, we compare chargeback/adjustment rates for signature-based and PIN-debit transactions.

4.1 Chargeback rates for signature-based transactions: before and after the EMV migration

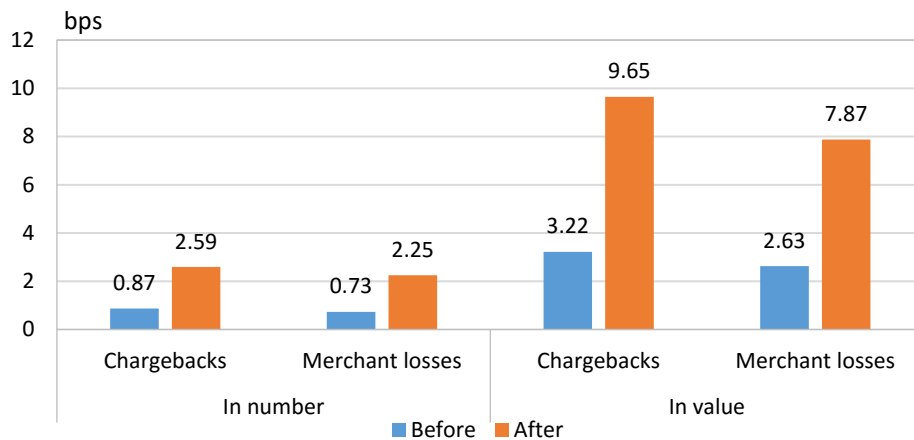
After the EMV liability shift took place in October 2015, the total chargeback and merchant loss rates, which combine all reason codes, increased. Chart 3 presents the weighted average total chargeback and merchant loss rates for all merchants, regardless of their merchant category and transaction channels. Both the total chargeback and merchant loss rates increased more than twofold after the EMV liability shift.

Chart 3: Total chargeback and merchant loss rates for all merchants



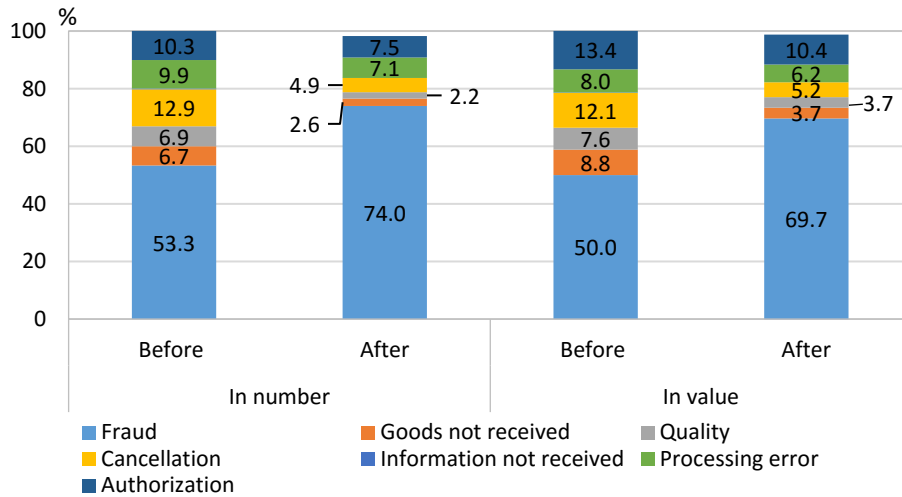
The increases in the total chargeback and merchant loss rates are mainly explained by the increases in the fraud chargeback and merchant loss rates. Fraud chargeback and merchant loss rates for all merchants combined have nearly tripled since the liability shift (Chart 4). The fraud merchant loss rate in terms of value, for example, has increased from 2.63 bps before the shift to 7.87 bps after the shift. The share of chargebacks attributable to fraud significantly increased from 53 to 74 percent in number and from 50 to 70 percent in value (Chart 5). The shares of all other reason codes declined after the liability shift.¹⁵

Chart 4: Fraud chargeback and merchant loss rates for all merchants



¹⁵ To a much lesser extent, chargeback rates for processing error and authorization reasons have also increased.

Chart 5: Reason code shares in chargebacks



The increases in fraud chargeback and merchant loss rates are mostly associated with the CP channel, rather than the CNP channel. While the CP share in sales transactions declined after the EMV liability shift in our data, the CP share in fraud chargebacks increased (Chart 6). The opposite trends in sales and fraud chargebacks suggest a significant increase in the CP fraud chargeback rate. In fact, the fraud chargeback and merchant loss rates for CP transactions have increased six-fold since the liability shift (Chart 7). All of the five merchant categories for which we collected data have experienced increases in the fraud chargeback and merchant loss rates for CP transactions. The size of the increases, however, vary significantly across the categories: For department and grocery stores, the increase in the merchant loss rate in value is more than tenfold, while for restaurants and travel industries, the increase is less than threefold (Chart 8).

Chart 6: CP channel share

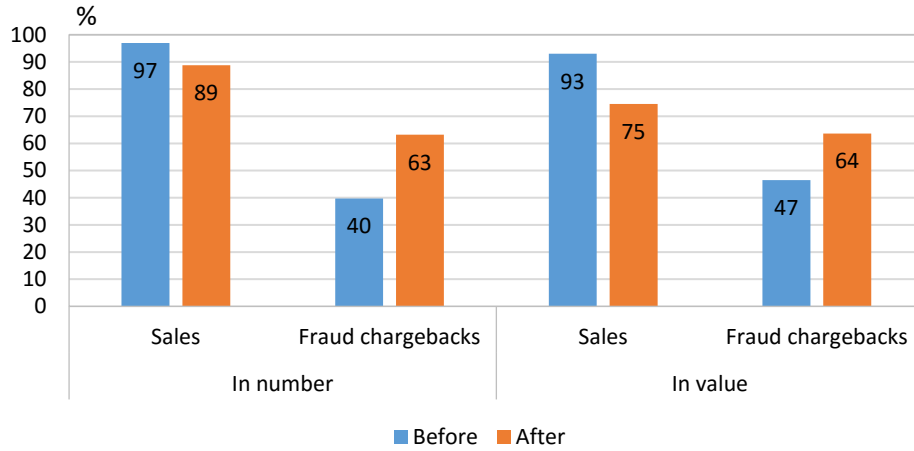


Chart 7: Fraud chargeback and merchant loss rates for CP transactions

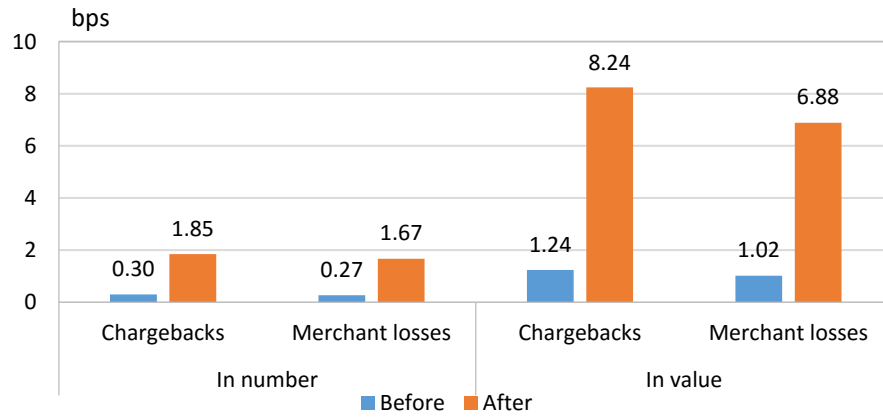
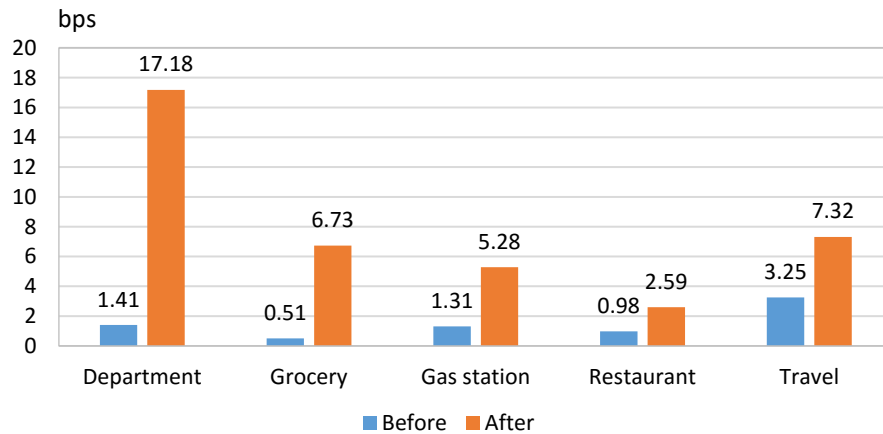
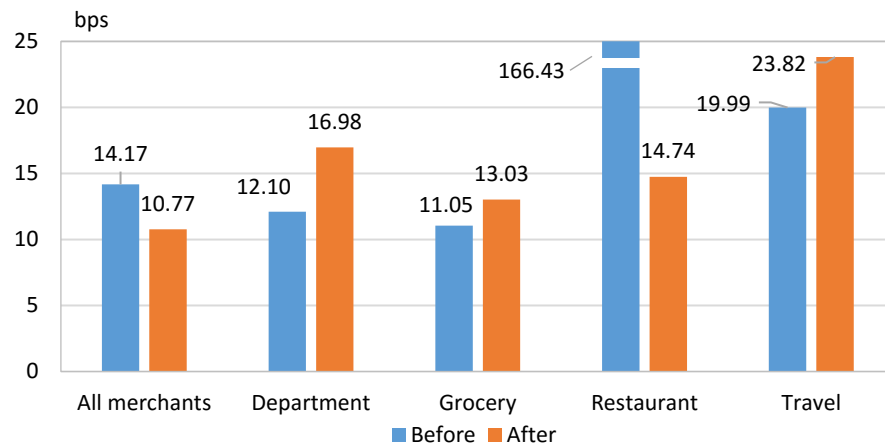


Chart 8: Fraud merchant loss rates for CP in value by merchant category



Our results for CNP transactions are mixed. For department and grocery stores, CNP fraud chargeback and merchant loss rates have increased, but for restaurants and all merchants combined, these rates have declined. For example, the CNP fraud merchant loss rate in terms of value has increased from 12.1 to 17.0 bps for department stores and from 11.1 to 13.0 bps for grocery stores, but the rate has decreased from 14.2 to 10.8 bps for all merchants combined (Chart 9). Two reports by FR BOG (FR BOG 2014 and 2016) indicate that the merchant fraud loss rate for signature-debit CNP transactions has increased from 10.2 bps in 2013 to 11.9 bps in 2015.¹⁶ According to another report by FR BOG (FR BOG 2018), the gross fraud rate for credit CNP transactions increased from 15.5 bps in 2015 to 18.7 bps in 2016, and the gross fraud rate for debit CNP transactions also increased from 14.7 bps in 2015 to 17.8 bps in 2016.¹⁷ These suggest that CNP fraud merchant loss rates increased for all merchants combined because merchants are generally liable for CNP fraud.

Chart 9: Fraud merchant loss rates by merchant category and for all merchants combined



The declines in the CNP fraud chargeback and merchant loss rates for all merchants combined in our data are likely due to the underrepresentation of signature-based CNP

¹⁶ Merchant fraud loss rates are based on the authors' calculation using the information shown in the FR BOG (2014 and 2016).

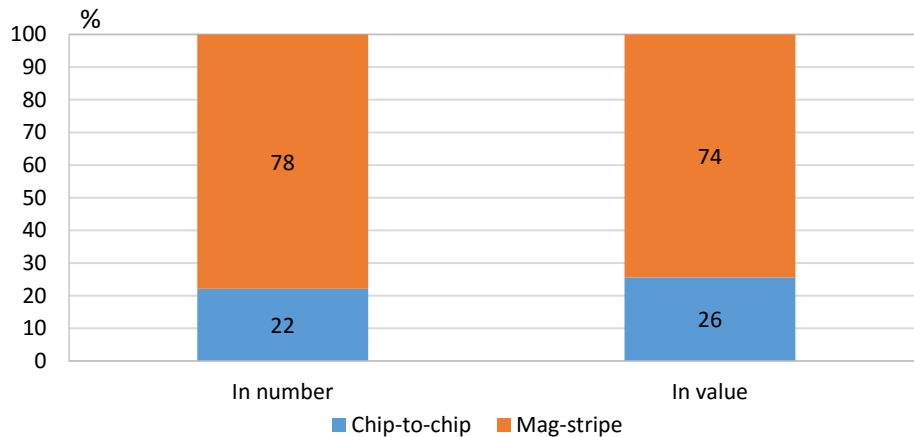
¹⁷ FR BOG (2018) divides card payments into in-person and remote channels, instead of CP and CNP channels.

transactions in our data. As Chart 6 indicates, the share of CNP transactions in value is only 7 percent for the period before the liability shift in our data, which is significantly smaller than the 36 percent share of CNP in signature-debit transaction value in 2013. In our sample for the period after the liability shift, the CNP share increased to 25 percent; nevertheless, the share is still much smaller than the 44 percent share of CNP in signature-based transaction value in 2016.

4.2 Chargeback rates for signature-based CP transactions: chip-to-chip versus mag-stripe

Although the EMV liability shift took place in October 2015, the majority of transactions were still non-chip (either a non-chip card was used or a chip card was used at a non-chip readable POS terminal), and thus information on the mag-stripe was read to process transactions. In our data, the share of chip-to-chip transactions is only 22 percent of CP transactions in terms of number when all merchants are combined (Chart 10).

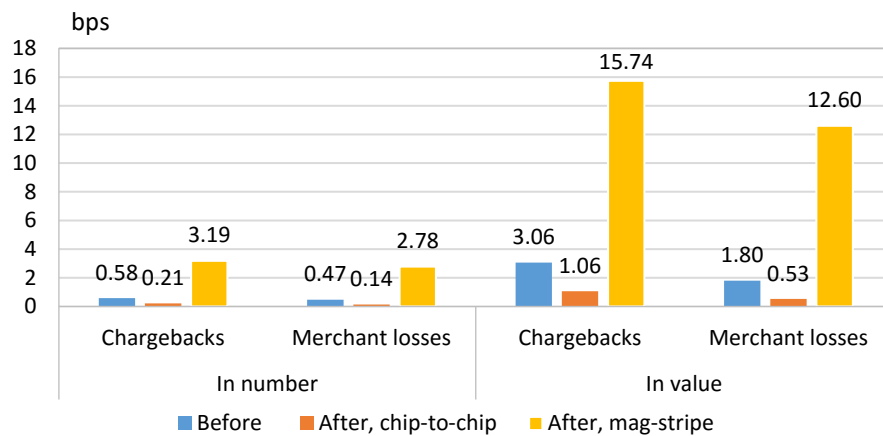
Chart 10: Distribution between chip-to-chip and mag-stripe transactions in CP



The total chargeback and merchant loss rates are significantly higher for mag-stripe transactions than for chip-to-chip transactions. For example, the merchant loss rate for mag-stripe transactions is higher by more than 2 bps in number and by about 12 bps in value than that for chip-to-chip transactions for all merchants combined (Chart 11). Compared to the total

chargeback and merchant loss rates for CP transactions before the liability shift, the rates for chip-to-chip transactions are lower, but the rates for mag-stripe transactions are significantly higher. The differences in total chargeback and merchant loss rates are associated with three reason codes – fraud, authorization and processing errors – and the other four reason codes have little effect.¹⁸

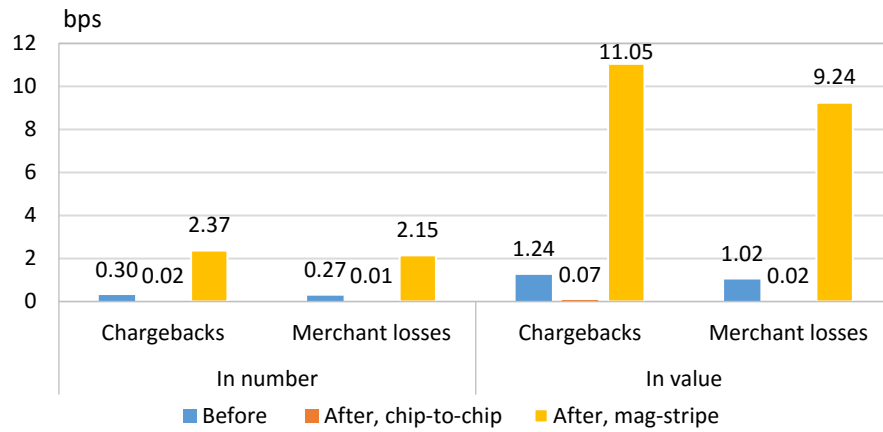
Chart 11: Total chargeback and merchant loss rates for all merchants: chip-to-chip vs. mag-stripe



The fraud chargeback and merchant loss rates are significantly higher for mag-stripe transactions than for chip-to-chip transactions. Since issuers are generally liable for fraud losses with chip-to-chip transactions, the merchant fraud loss rate is very low: 0.01 bps in number and 0.02 bps in value (Chart 12). In contrast, the merchant fraud loss rate for mag-stripe transactions is very high: 11.05 bps in number and 9.24 bps in value. Compared to the merchant fraud loss rate for CP transactions before the liability shift, the majority of which are mag-stripe transactions, the rate for mag-stripe transactions after the liability shift is almost 10 times higher.

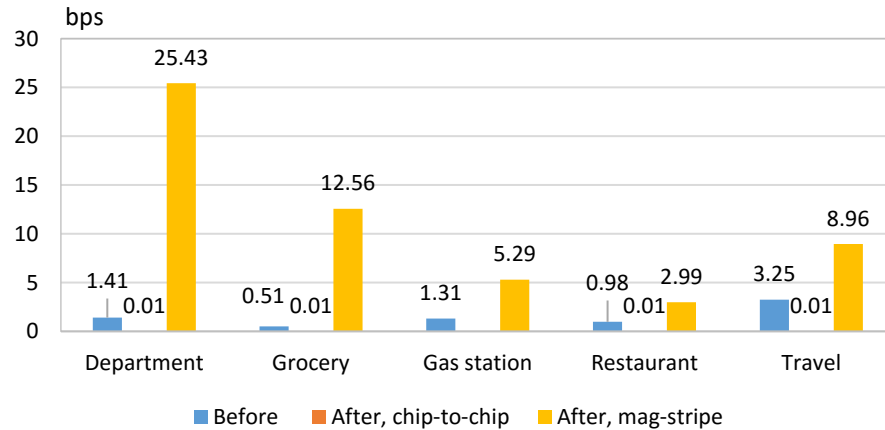
¹⁸ The four reason codes are non-receipt of goods or services; quality of service or merchandise, cancellation and return, and non-receipt of information.

Chart 12: Fraud chargeback and merchant loss rates for all merchants: chip-to-chip vs. mag-stripe



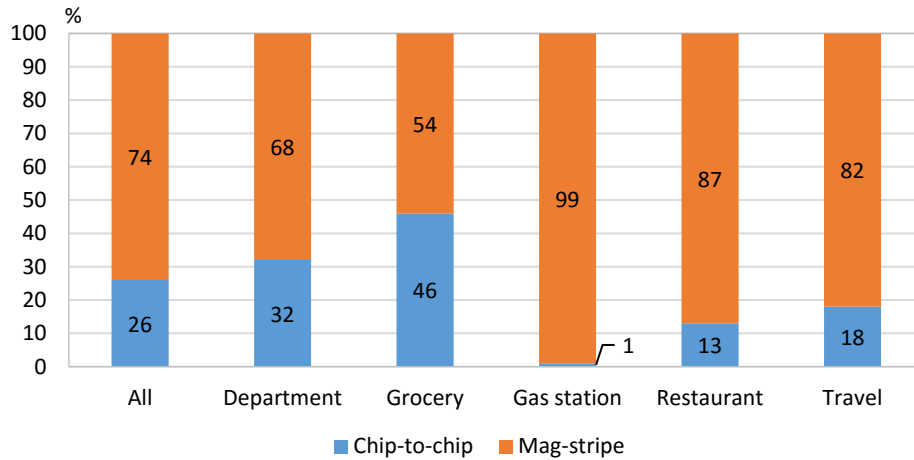
The higher merchant fraud loss rate for mag-stripe transactions after the liability shift may be mainly explained by the liability shift because the gross fraud rates for mag-stripe transactions did not increase in the same period (FR BOG 2018). For at least some merchants, however, the fraud rate itself may have increased for mag-stripe transactions, as fraudsters may have intensified their attacks on such transactions knowing that the EMV migration will eventually deplete their ability to exploit the weak security of mag-stripe. Distinguishing between these two causes is difficult, but our results from gas stations provide potential insights. For gas stations, the liability shift will not take effect until 2020; nevertheless, gas stations' fraud loss rate increased from 1.31 to 5.29 bps after *the other* merchants' liability shift took place, suggesting an increase in the fraud rate itself for mag-stripe transactions for at least some merchant categories (Chart 13).

Chart 13: Merchant fraud loss rates by merchant category: chip-to-chip vs. mag-stripe



There is an additional finding from Chart 13. While merchant fraud loss rates for chip-to-chip transactions are almost constant around 0.01 bps across merchant categories, those for mag-stripe transactions significantly vary by merchant category. Department and grocery stores have much higher merchant fraud loss rates for mag-stripe transactions (25.43 and 12.56 bps, respectively) than restaurants and the travel industry (2.99 and 8.96 bps, respectively). Interestingly, merchant categories with higher fraud loss rates for mag-stripe transactions have a larger share of chip-to-chip transactions in CP transactions (Chart 14). The chip-to-chip share is much larger for department and grocery stores (32 and 46 percent, respectively) than for restaurants and the travel industry (13 and 18 percent, respectively). These results suggest that EMV migration has progressed more rapidly among merchants who are more vulnerable to mag-stripe fraud and thus can greatly reduce fraud losses by adopting chip-readable POS terminals.

Chart 14: Distribution between chip-to-chip and mag-stripe transactions in CP in value by merchant category



When all merchants are combined, chargeback and merchant loss rates due to authorization problems show similar results, albeit to a much lesser extent, to fraud chargeback and merchant loss rates (Chart 15). The rates for chip-to-chip transactions are lower, and the rates for mag-stripe transactions are generally higher, than those for CP transactions before the liability shift. However, these results are not common across all merchant categories. At grocery stores and gas stations, the rates for mag-stripe transactions are slightly *lower* after the liability shift than before (Chart 16). The results imply that chip-to-chip transactions can also reduce chargebacks and merchant losses due to authorization problems. The reason why mag-stripe transactions have higher chargeback rates due to authorization problems after the liability shift than before for some merchant categories, however, is unclear and requires further investigation.

Chart 15: Chargeback and merchant loss rates due to authorization problems for all merchants: chip-to-chip vs. mag-stripe

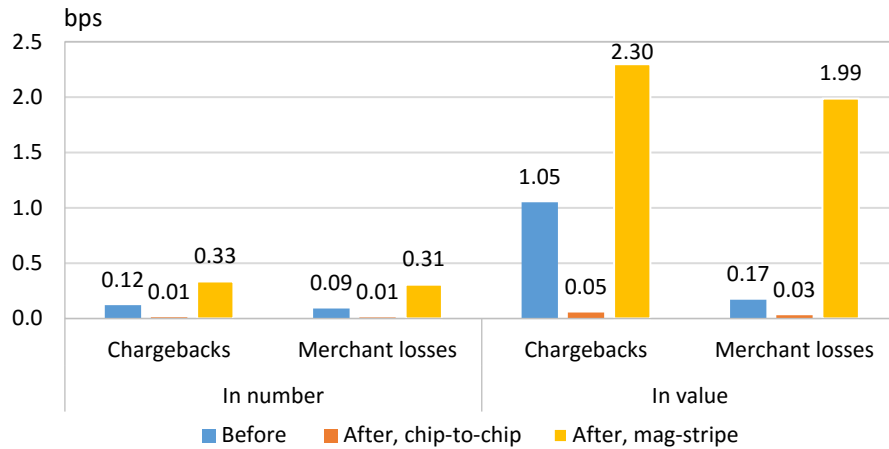
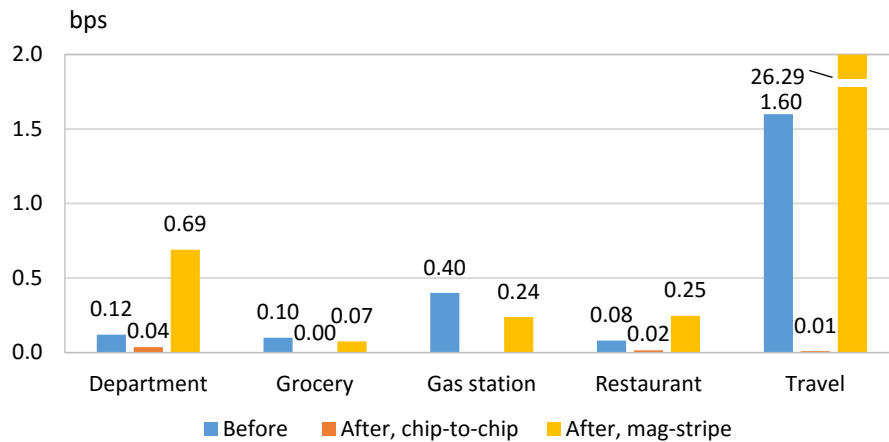


Chart 16: Merchant loss rates due to authorization problems in value by merchant category: chip-to-chip vs. mag-stripe



In contrast to fraud and authorization reasons, chargeback and merchant loss rates due to processing errors increased after the liability shift for both chip-to-chip and mag-stripe transactions when all merchants are combined (Chart 17). Mag-stripe transactions have higher rates after the liability shift than before across all five merchant categories, but whether chip-to-chip transactions have higher rate than CP transactions before the liability shift varies by merchant category. Chip-to-chip transactions have higher rates at department and grocery stores, but have lower rates at restaurants and the travel industry (Chart 18). When all merchants are

combined, as well as across all merchant categories from which we collected data, processing errors are the top reason for chip-to-chip transaction chargebacks, while they are a distant second or third reason for mag-stripe transaction chargebacks. It is unclear if relatively high chargeback rates for chip-to-chip transaction processing errors are a temporary issue during the transition period or a permanent issue inherent in chip-to-chip transactions. To examine it, more recent data would need to be collected.

Chart 17: Chargeback and merchant loss rates due to processing errors for all merchants: chip-to-chip vs. mag-stripe

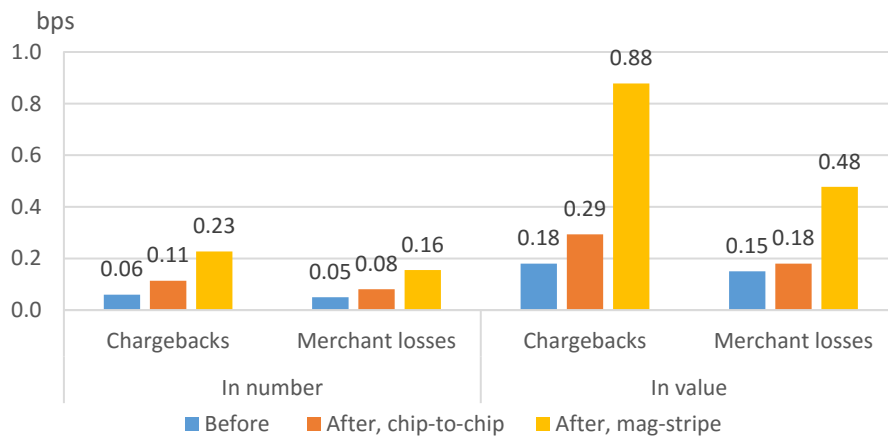
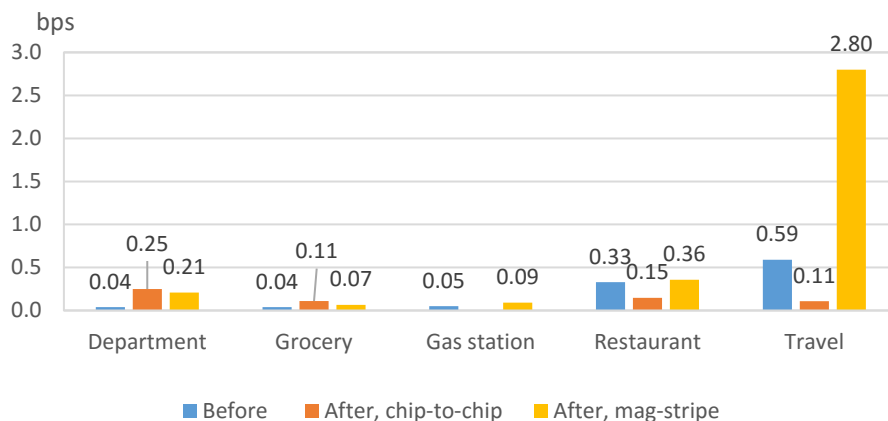


Chart 18: Merchant loss rates due to processing errors in value by merchant category: chip-to-chip vs. mag-stripe



4.3 Chargeback rates for PIN-based transactions

Unlike signature-based chargebacks, we cannot calculate weighted average chargeback (or adjustment) rates or report merchant loss rates for PIN-debit transactions due to missing information in our data. In this section, we present chargeback rates and other statistics in the general range derived from reported statistics of individual networks, rather than the weighted averages.

Compared to signature-based transactions, which include credit and signature-debit transactions, PIN-debit transactions have significantly lower chargeback rates. The total chargeback rate, which include both fraud and non-fraud reasons, is lower than 1 bps in number and 1.5 bps in value. Unlike signature-based transactions, the vast majority of chargebacks for PIN-debit transactions are not due to fraud. Although the share of fraud chargebacks in the total chargebacks varies by network, the share is no more than 30 percent. The fraud chargeback rate is lower than 0.05 bps in number and 0.15 bps in value (Table 1).

Table 1: Fraud chargeback rates for all merchants: PIN vs. signature (bps)

	PIN-debit		Signature-based	
	In number	In value	In number	In value
All	<0.05	<0.15	2.59	9.65
CNP	<0.50	<1.50	8.50	13.76
CP	~0.01	<0.02	1.85	8.24
Chip-to-chip	<0.01	<0.01	0.02	0.07
PIN	<0.01	<0.01	-	-
PIN-less	<0.01	<0.01	-	-
Mag-stripe	<0.02	<0.03	2.37	11.05
PIN	<0.01	<0.02	-	-
PIN-less	<0.20	<0.20	-	-

-: not applicable

Similar to signature-based transactions, the fraud chargeback rate for CNP transactions is higher than that for CP transactions. Fraud chargeback rate for CNP transactions is lower than 0.5 bps in number and 1.5 bps in value, while the rate for CP transactions is around 0.01 bps in

number and lower than 0.02 bps in value (Table 1). The vast majority of CNP transactions processed by PIN debit networks are PIN-less transactions; nevertheless, the fraud chargeback rate of PIN-less CNP transactions is significantly lower than that of signature-based CNP transactions. The difference in the fraud chargeback rate may be explained by the difference in use cases. It is anecdotally reported that a major use case of PIN-less CNP transactions is bill payments, for which payers (cardholders) and payees have pre-existing relationship. In contrast, many signature-based CNP transactions are made for one-time, ad-hoc payments.

CP transactions processed by PIN debit networks are divided into four groups based on two factors: whether the transactions are chip-to-chip or mag-stripe and whether the transactions are with PIN or without PIN. PIN-less CP transactions are generally small-value transactions: the average size of PIN-less transactions is around \$20, while that of PIN transactions is around \$40. The share of PIN-less transactions in CP transactions is also small, about 10 percent in number and 5 percent in value.

As expected, mag-stripe, PIN-less transactions have the highest fraud chargeback rate among the four groups: the rate is lower than 0.2 bps in both number and value (Table 1). The three other groups have much lower chargeback rates. With chip-to-chip transactions, the rate is lower than 0.01 bps in both number and value, regardless of whether PIN was used. Mag-stripe, PIN transactions have a slightly higher chargeback rate, which is still lower than 0.01 bps in number and 0.02 bps in value.

4.4 Implications of our results

Our results provide interesting implications. Without PIN, either PIN-less or signature-based, chip-to-chip transactions are highly effective in reducing fraud chargeback rates;

however, once PIN is used, the incremental reduction of chargeback rates with chip-to-chip transactions is marginal. Fraud chargeback rates for chip-to-chip transactions are slightly lower when those transactions are made with PIN than with signature. These results suggest that both EMV and PIN are effective in reducing chargeback rates. To examine how effective EMV and PIN (or alternative stronger method of) authentication are in reducing fraud itself in the CP environment, detailed data on issuers' fraud losses or on gross fraud for all parties are needed.¹⁹

Although fraud chargeback rates for CNP transactions have not increased in our data, other available data suggest these rates have increased. Moreover, merchants incur fraud losses not only via chargebacks but also by issuing direct credits to their customers when the merchants receive a fraud claim directly from their customers. According to CyberSource (2016), the share of direct credits as a percentage of all e-Commerce fraud losses increased from 57 percent in 2012 to 72 percent in 2015. Thus, merchant fraud loss rates, including both chargebacks and direct credits, could have increased more than what is reported. Uncovering actual fraud losses for CNP transactions would help show the true trend and loss allocation of CNP fraud, which, in turn, would help address CNP fraud more effectively.

5. Conclusion

This study has examined the initial effects of the EMV liability shift on chargeback rates in the United States. Chargeback and merchant loss rates for general-purpose, four-party scheme, signature-based transactions significantly increased immediately after the EMV liability shift.

¹⁹ According to Pulse (2017), fraud loss rates for debit card issuers increased from 2014 to 2015, but declined from 2015 to 2016 for both PIN- and signature-based transactions. These transactions include CP and CNP transactions. According to FR BOG (2018), the gross fraud rates in value for CP chip-to-chip transaction are lower than those for CP mag-stripe transactions for both credit cards (12.2 bps vs. 16.0 bps) and debit cards (2.71 bps vs. 5.86 bps) in 2016. The gross fraud rates for CP PIN and CP signature (or no authentication) are not available in FR BOG (2018).

Changes are most evident in the CP channel, where fraud chargeback and merchant loss rates have increased roughly sixfold since the liability shift; however, fraud chargeback and merchant loss rates significantly vary between chip-to-chip and mag-stripe transactions. Merchant fraud loss rates for CP chip-to-chip transactions are very low, around 0.02 bps in value, across merchant categories. In contrast, merchant fraud loss rates for CP mag-stripe transactions are much higher and vary across merchant categories: over 9 bps for all merchants combined, over 25 bps for department stores and over 12 bps for grocery stores.

The higher fraud merchant loss rates for mag-stripe transactions after the liability shift may be mostly associated with the liability shift, as the gross fraud rates of mag-stripe transactions did not increase in the same period. Our results from gas stations, however, suggest that fraud itself for mag-stripe transactions also increased for at least some merchant categories. The high merchant fraud loss rates in the CP channel will be temporary if merchants continue to adopt EMV.

Compared to signature-based transactions, PIN-debit transactions have much lower chargeback rates. Fraud chargeback rates of PIN-debit in the CP channel are lower than 0.02 bps. While mag-stripe PIN-less transactions have slightly higher fraud chargeback rates, chip-to-chip PIN, chip-to-chip PIN-less, and mag-stripe PIN transactions have chargeback rates lower than 0.02 bps. Our results suggest both EMV and PIN authentication are effective in reducing chargeback rates, but detailed gross fraud rates are needed to examine how effective EMV and PIN are in reducing fraud itself in the CP channel.

Our results for CNP fraud chargeback and merchant loss rates are mixed. Immediately following the liability shift, both rates increased for department and grocery stores, while they declined for restaurants and all merchants combined in our data. The rate decline for all

merchants combined in our data is likely due to the underrepresentation of signature-based CNP transactions in our data. The gross fraud rates for CNP transactions actually increased in the same period and merchants are generally liable for CNP fraud.

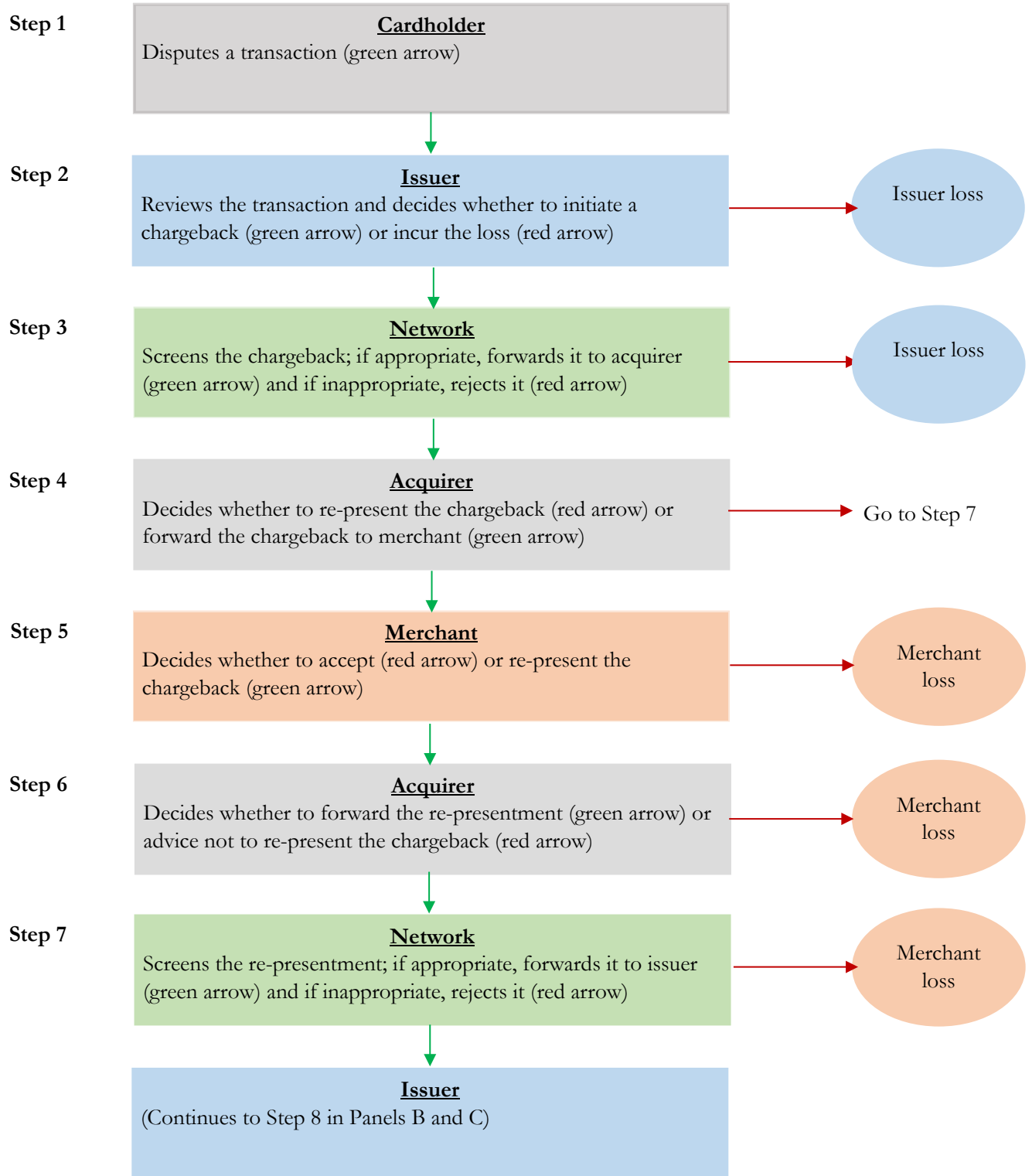
References

- CyberSource. 2015. "Annual Fraud Benchmark Report: A Balancing Act."
- Digital Transactions News. 2014. "Following Star, Accel, and Pulse, NYCE Selects Visa's EMV Debit Technology," April 1.
- Federal Reserve Board of Governors. 2014. "2013 Interchange Revenue, Covered Issuer Cost, and Covered Issuer and Merchant Fraud Loss Related to Debit Card Transactions."
- _____. 2016. "2015 Interchange Revenue, Covered Issuer Cost, and Covered Issuer and Merchant Fraud Loss Related to Debit Card Transactions."
- _____. 2018. "Changes in U.S. Payments Fraud from 2012 to 2016: Evidence from the Federal Reserve Payments Study."
- Federal Reserve System. 2017. "The Federal Reserve Payments Study: 2017 Annual Supplement."
- Hayashi, Fumiko. 2012. "The New Debit Card Regulations: Initial Effects on Networks and Banks," Federal Reserve Bank of Kansas City, *Economic Review*, vol. 95, no. 4, pp. 79-115.
- _____, Zach Markiewicz, and Richard J. Sullivan. 2016. "Chargebacks: Another Payment Card Acceptance Cost for Merchants," Federal Reserve Bank of Kansas City, Research Working Paper 16-01.
- _____, Taylor Moore, and Richard J. Sullivan. 2015. "The Economics of Retail Payments Security," *The Conference Proceedings of the Puzzle of Payments Security: Fitting the Pieces Together to Protect Retail Payments System*. Federal Reserve Bank of Kansas City. pp. 21-68.
- King, Douglas. 2012. "Chip-and-PIN: Success and Challenges in Reducing Fraud," Federal Reserve Bank of Atlanta, Retail Payments Risk Forum Working Paper.
- Pulse. 2017. "2017 Debit Issuer Study," August.
- PYMNTS.com. 2016. "Visa's Merchant-Friendly EMV Moves," June 17.
- Simmons, Kaleigh. 2016. "Card Fraud Instances Rising, Even in Countries with EMV," Rippleshort Blog, July 14.
- US Payments Forum. 2017. "Understanding the U.S. EMV Liability Shifts. Version 2.0," July.

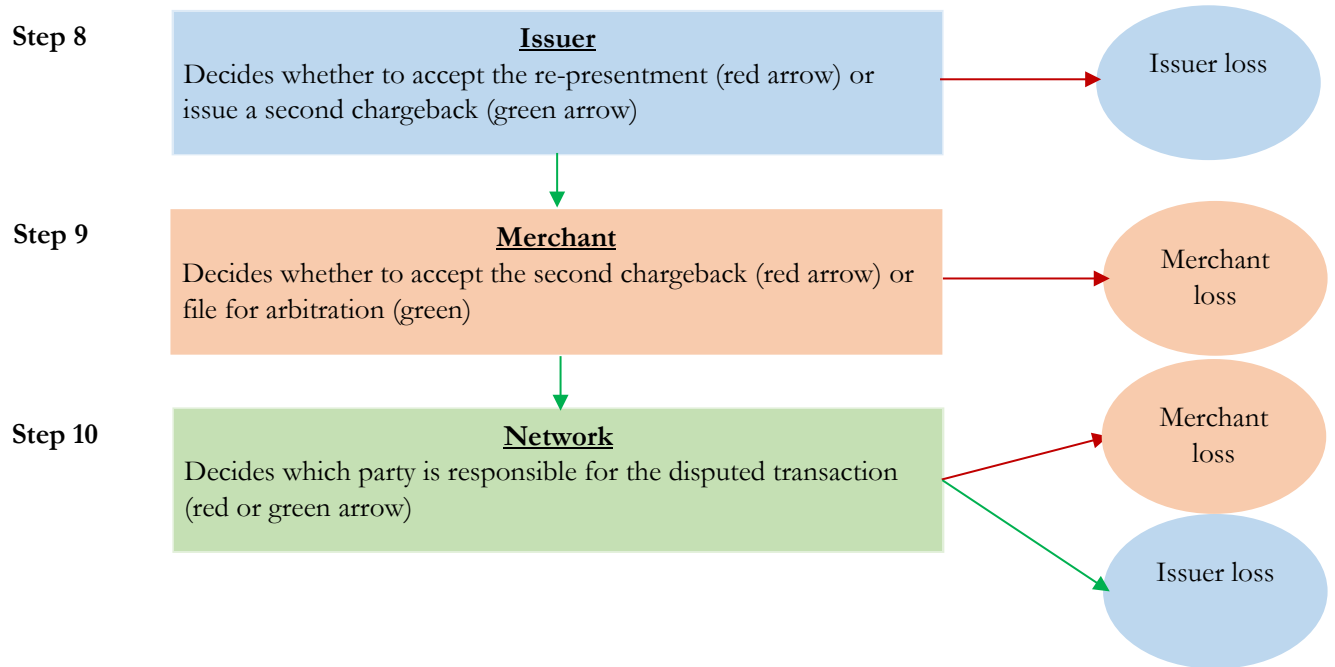
Appendix A: Chargeback lifecycle

Figure A1: Chargeback lifecycle

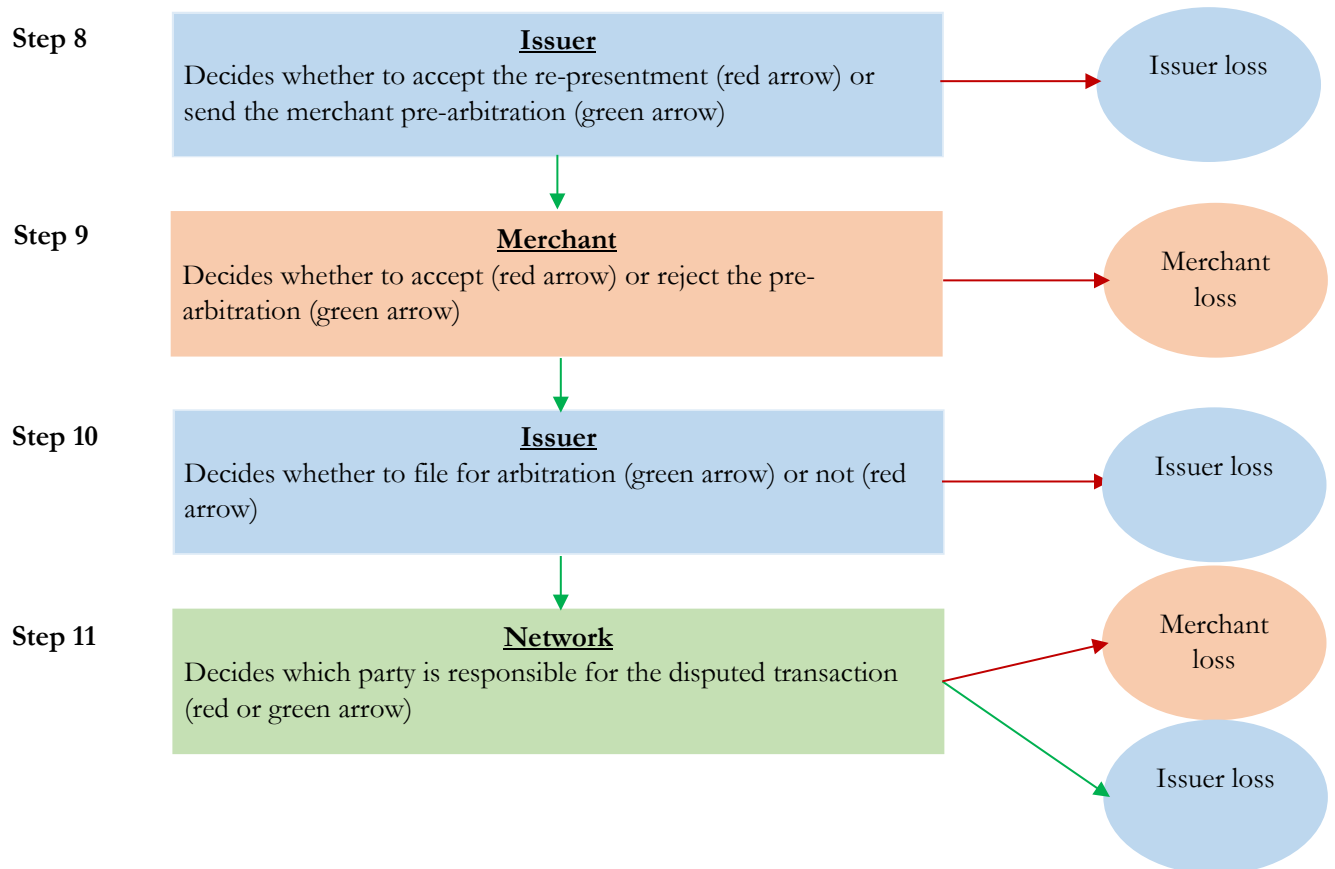
Panel A: Steps 1 through 7



Panel B: Steps 8 through 10 for MasterCard



Panel C: Steps 8 through 11 for Visa



Appendix B: Chargeback reason code categories and corresponding reason codes

Category	Visa	MasterCard
Fraud	57, 62, 75, 81, 83, 93	4837, 4840, 4863, 4870, 4871, 4849, 4847, 4862, 4857
Non-Receipt of Goods/Services	30, 90	4855, 4859
Quality of Service/Merchandise	53	4853, 4854, 4899
Cancellation and Return	41, 85	4841, 4860
Non-Receipt of Information	60, 79	4801, 4802
Processing Error	74, 76, 80, 82, 86, 96	4831, 4834, 4842, 4846, 4850
Authorization Issues	70, 71, 72, 73, 77, 78	4807, 4808, 4812, 4835

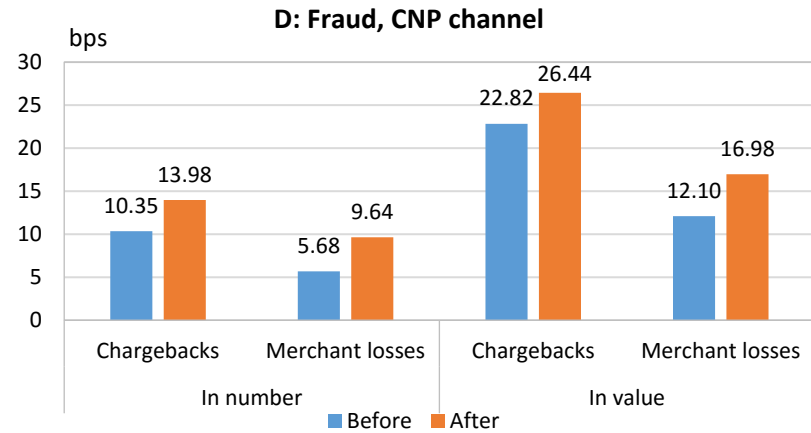
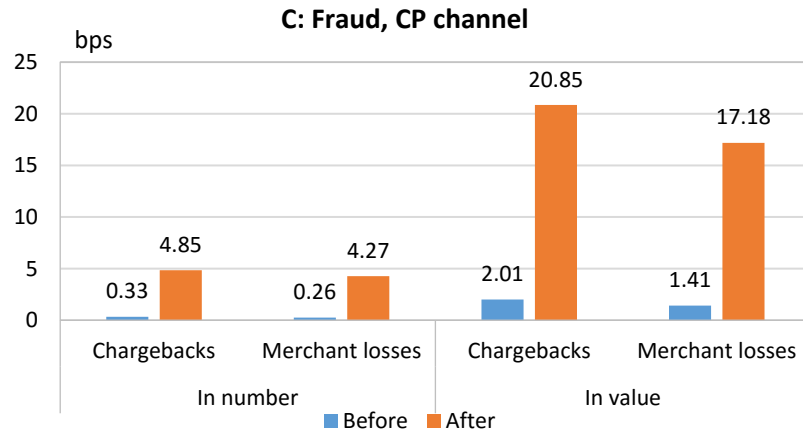
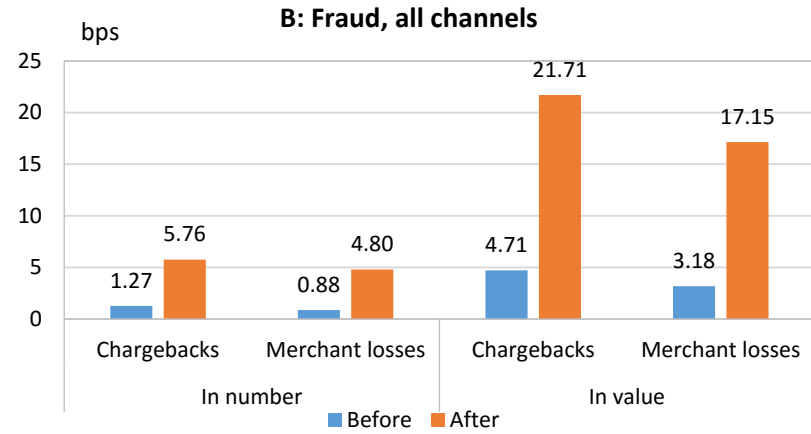
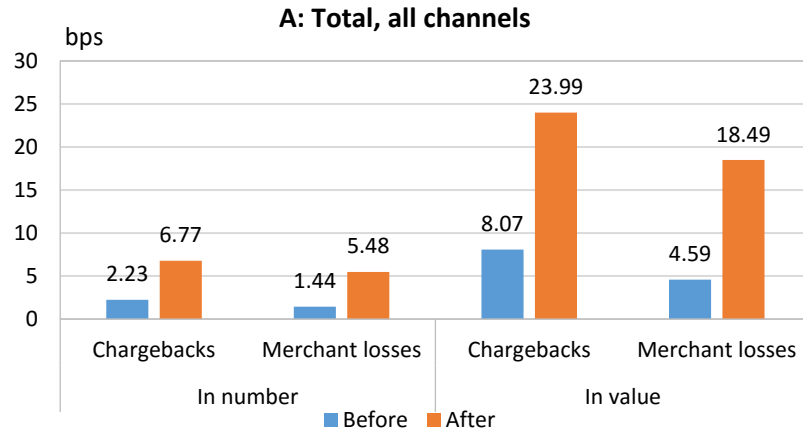
Appendix C: Merchant categories and corresponding merchant category codes (MCCs)

Category	MCC	Description
Travel	3000-3299	Airlines
	3351-3441	Car Rental
	3501-3790	Hotels/Motels/Inns/Resorts
Department, Big Box, and Apparel	5300	Wholesale Clubs
	5310	Discount Stores
	5311	Department Stores
	5331	Variety Stores
	5399	Misc. General Merchandise
	5611	Men's and Boy's Clothing and Accessories Stores
	5621	Women's Ready-To-Wear Stores
	5631	Women's Accessory and Specialty Shops
	5641	Children's and Infant's Wear Stores
	5651	Family Clothing Stores
	5655	Sports and Riding Apparel Stores
	5661	Shoe Stores
	5681	Furriers and Fur Shops
	5691	Men's, Women's Clothing Stores
	5697	Tailors, Alterations
	5698	Wig and Toupee Stores
	5699	Misc. Apparel and Accessory Shops
Grocery, Food, and Drug	5999	Misc. and Specialty Retail
	5411	Grocery Stores, Supermarkets
	5422	Meat Provisioners – Freezer and Locker
	5441	Candy, Nut, and Confectionery Stores
	5451	Dairy Products Stores
	5499	Misc. Food Stores
Gas station	5912	Drug Stores and Pharmacies
	5541	Service Stations (with or without ancillary services)
Restaurant	5542	Automated Fuel Dispensers
	5812	Eating places and Restaurants
	5814	Fast Food Restaurants
	5813	Drinking Places, Bars, Taverns, Cocktail lounges
	5811	Caterers
Travel	5462	Bakeries
	3000-3299	Airlines
	3351-3441	Car Rental
	3501-3790	Hotels/Motels/Inns/Resorts

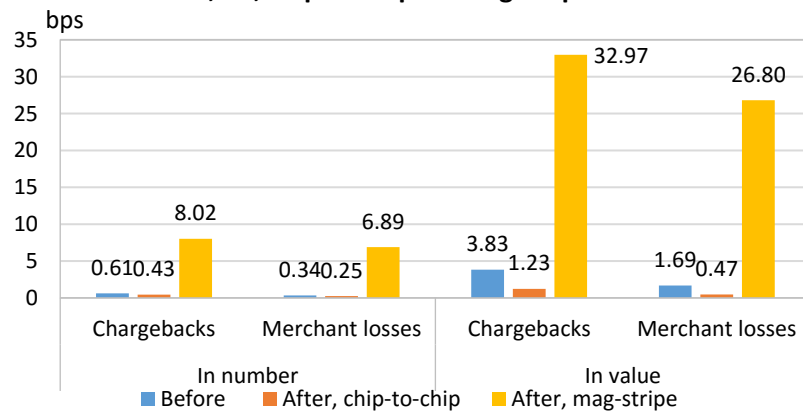
Appendix D: Detailed chargeback statistics

Department Category

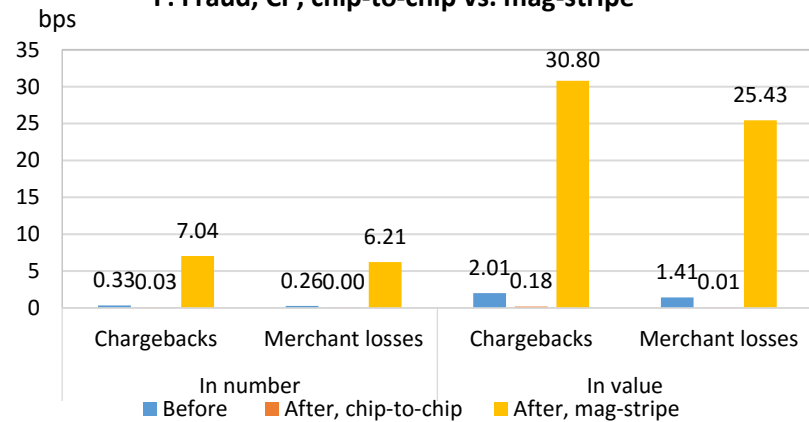
Chart D1: Chargeback and merchant loss rates



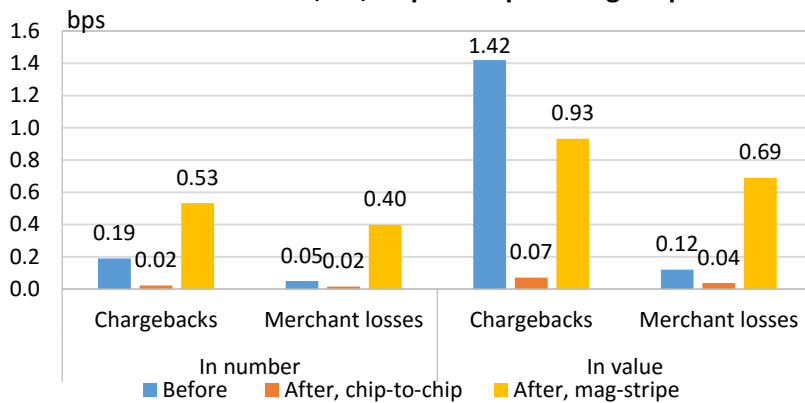
E: Total, CP, chip-to-chip vs. mag-stripe



F: Fraud, CP, chip-to-chip vs. mag-stripe



G: Authorization, CP, chip-to-chip vs. mag-stripe



H: Processing error, CP, chip-to-chip vs. mag-stripe

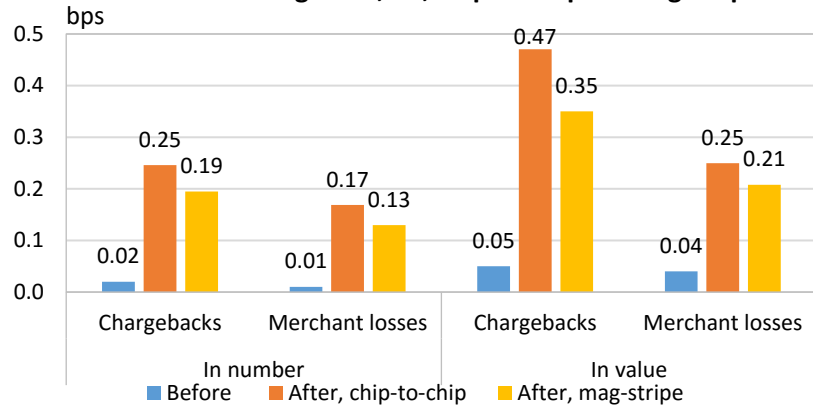


Chart D2: Reason code shares in chargebacks, all channels

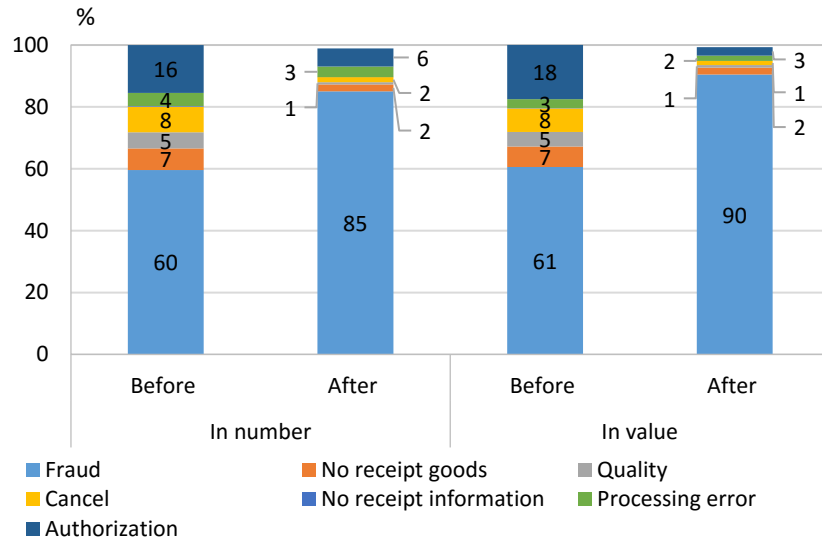


Chart D3: Card present channel share

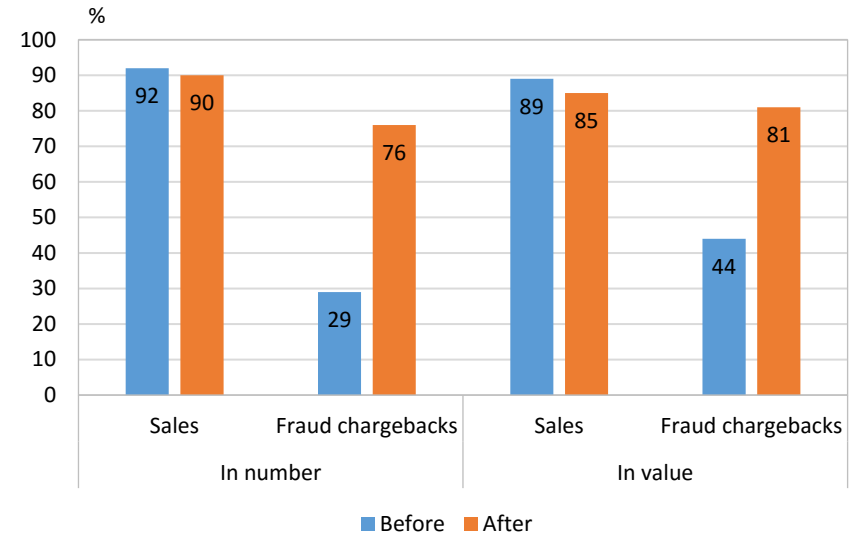
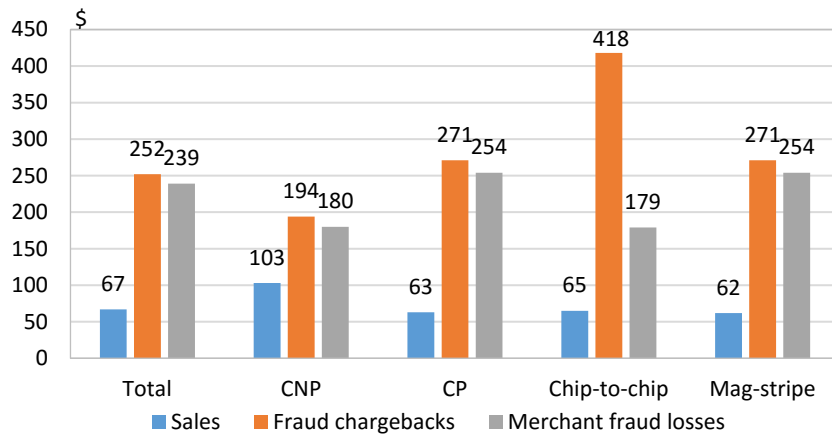
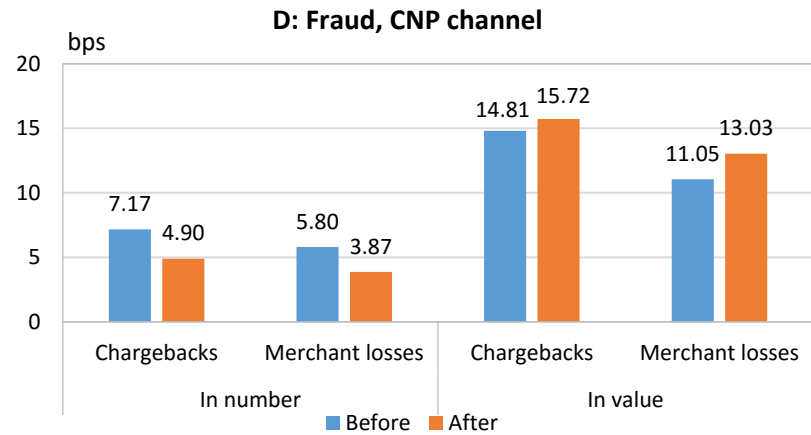
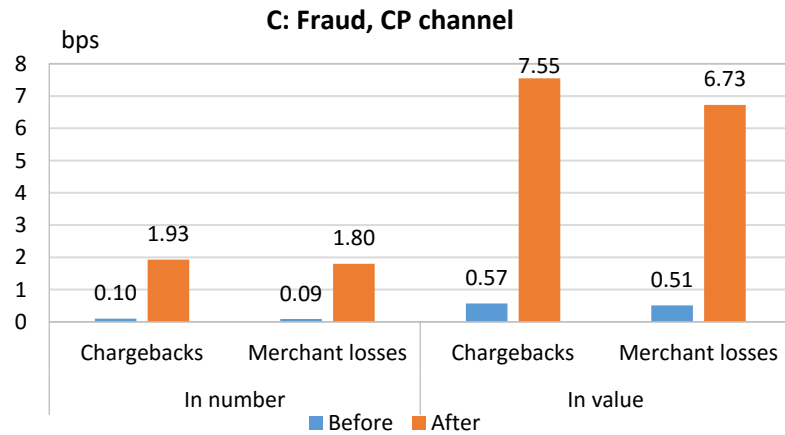
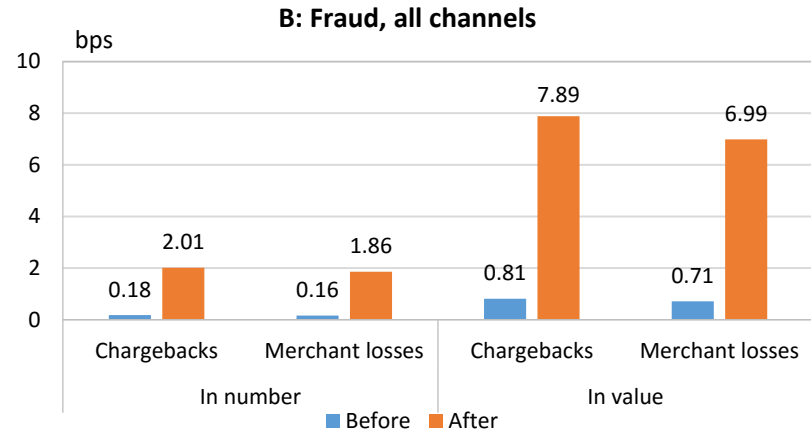
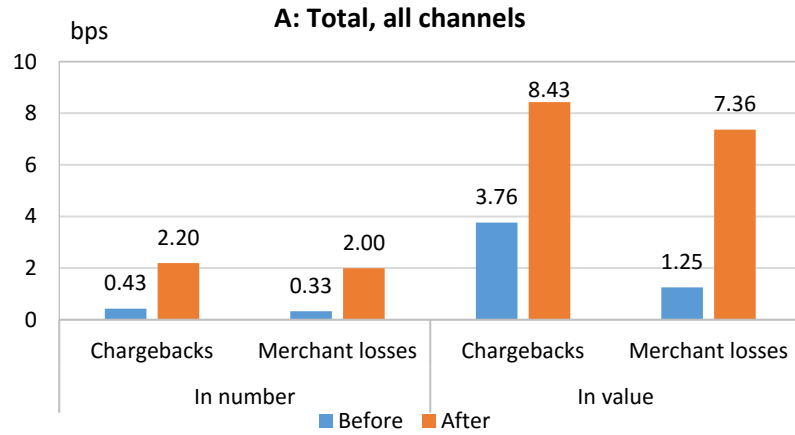


Chart D4: Average value per transaction for signature-based transactions



Grocery Category

Chart D5: Chargeback and merchant loss rates



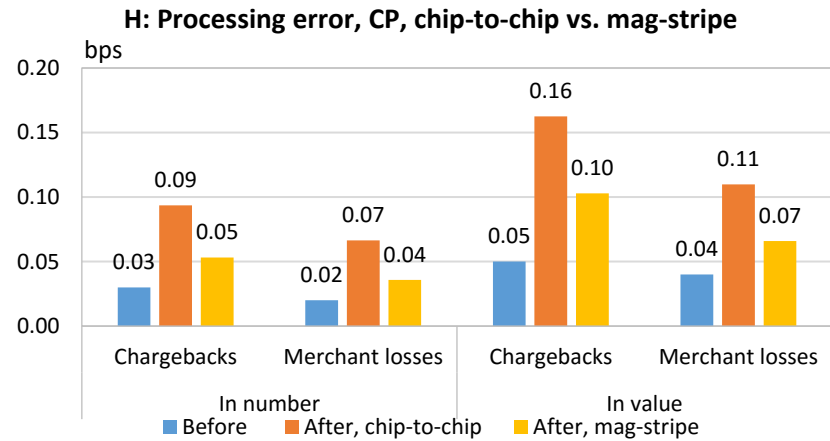
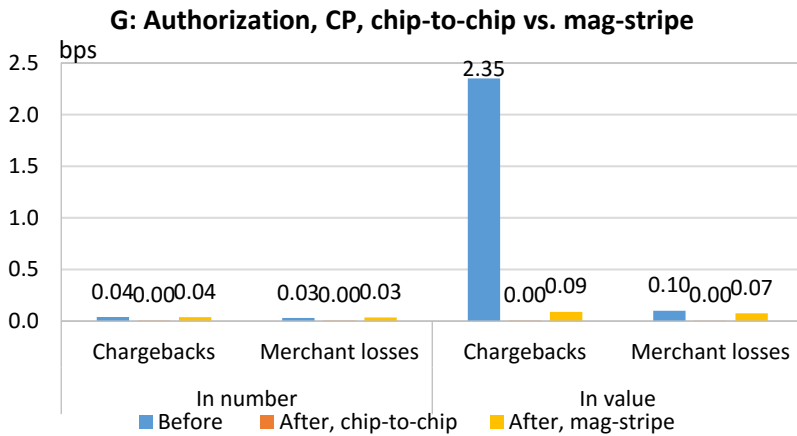
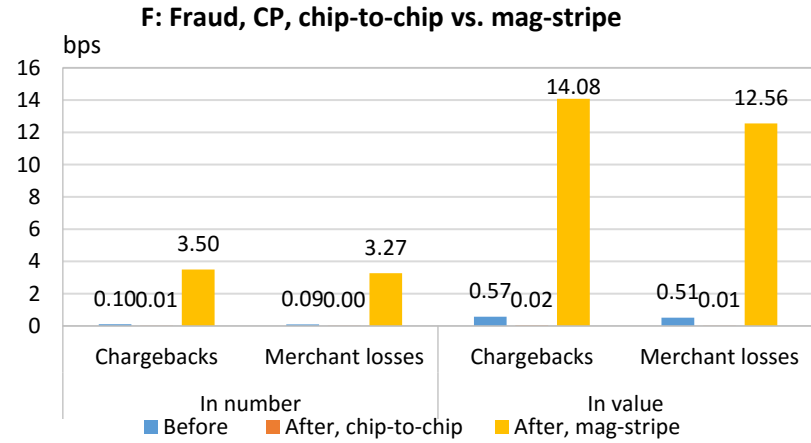
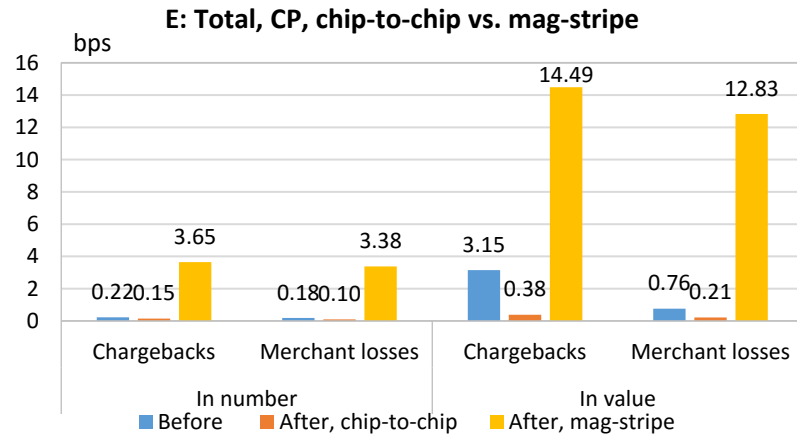


Chart D6: Reason code shares in chargebacks, all channels

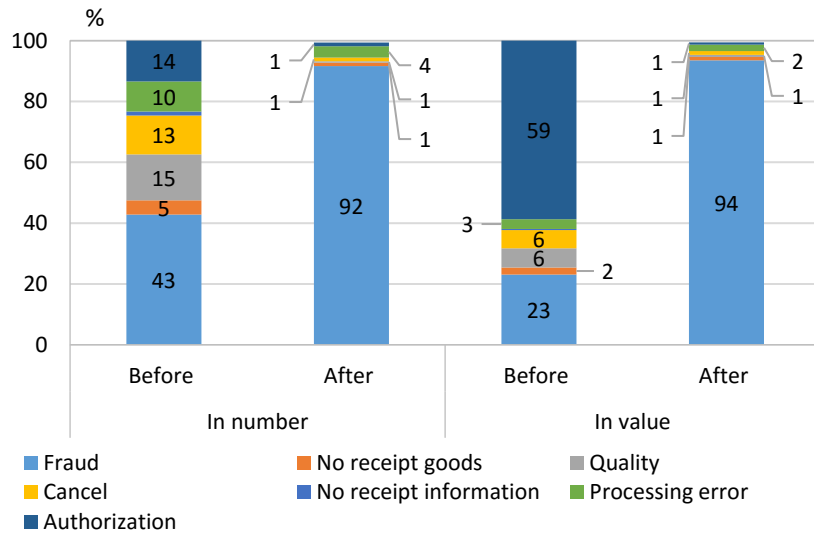


Chart D7: Card present channel share

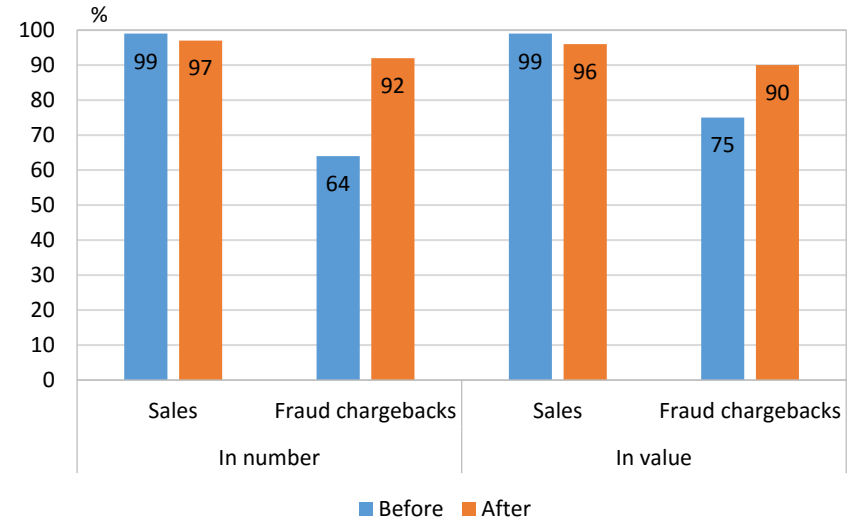
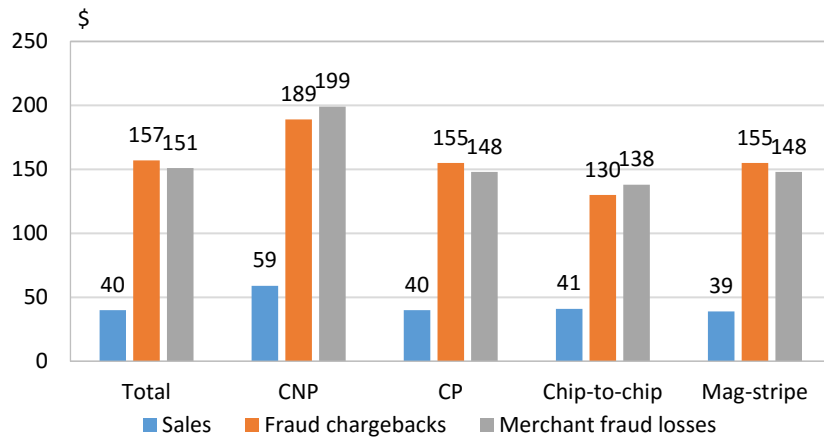
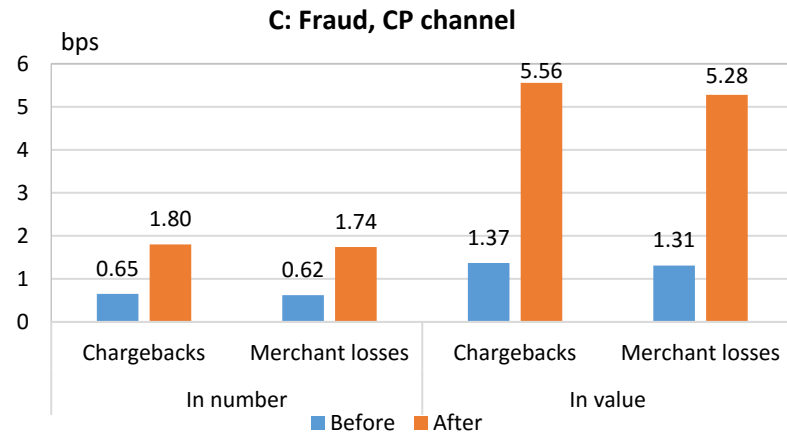
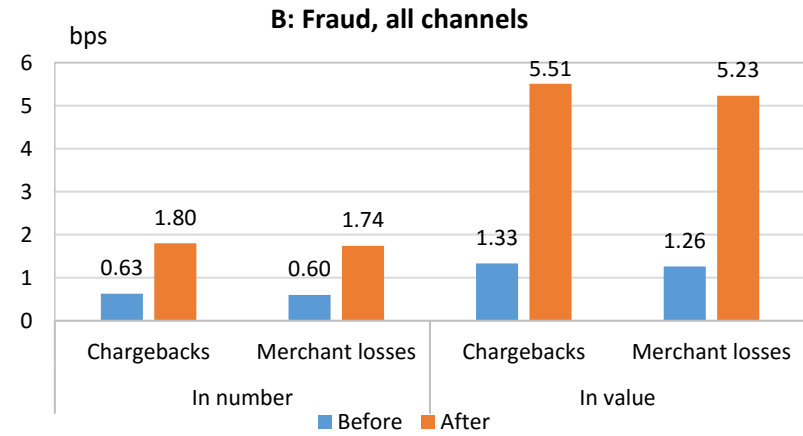
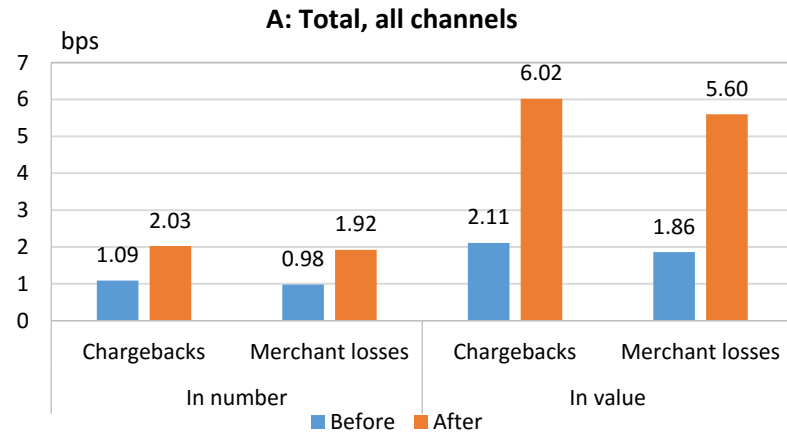


Chart D8: Average value per transaction for signature-based transactions

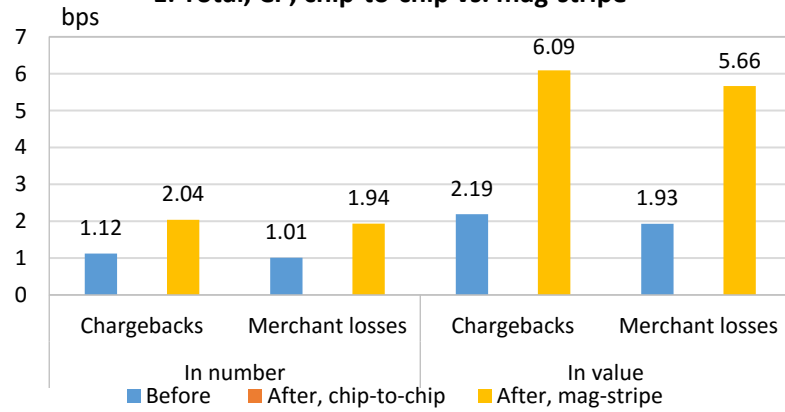


Gas stations

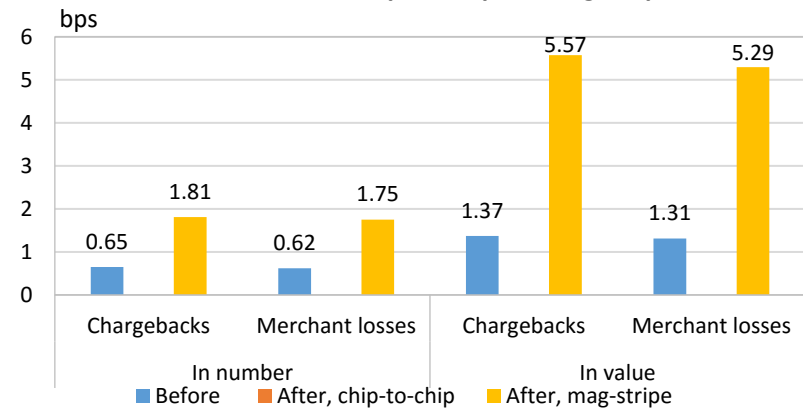
Chart D9: Chargeback and merchant loss rates



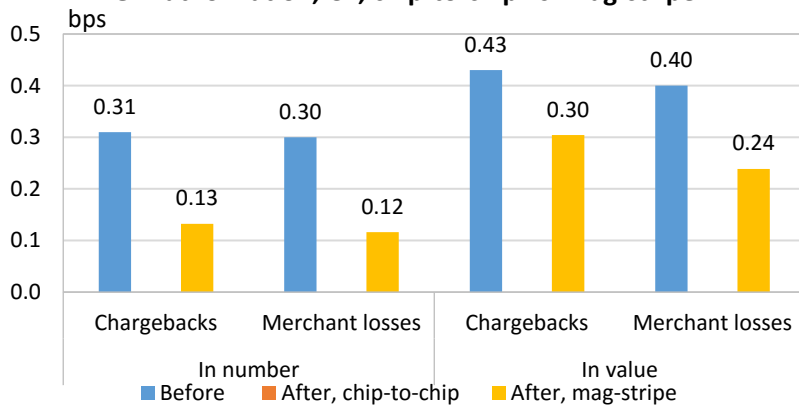
E: Total, CP, chip-to-chip vs. mag-stripe



F: Fraud, CP, chip-to-chip vs. mag-stripe



G: Authorization, CP, chip-to-chip vs. mag-stripe



H: Processing error, CP, chip-to-chip vs. mag-stripe

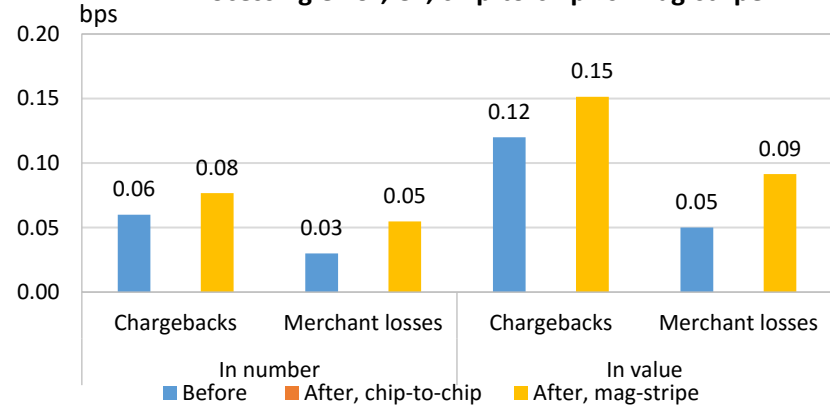


Chart D10: Reason code shares in chargebacks, all channels

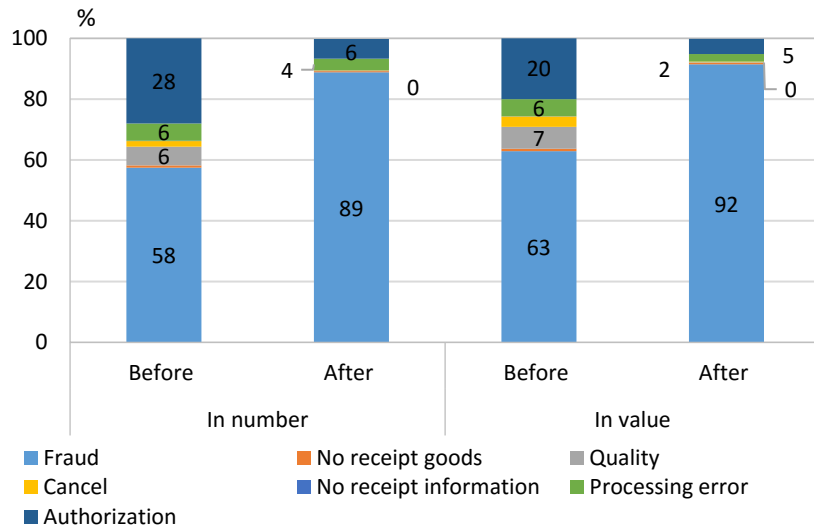
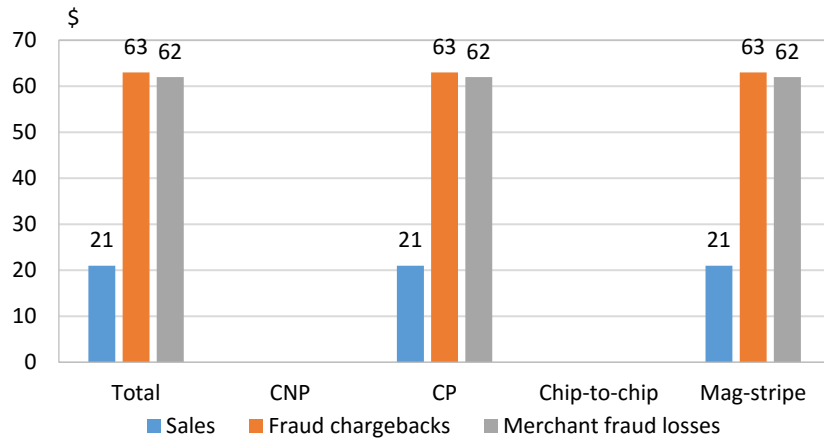


Chart D11: Card present channel share

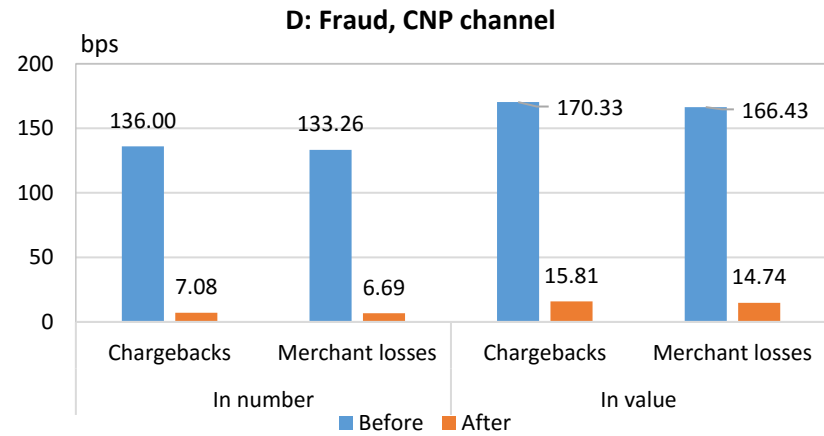
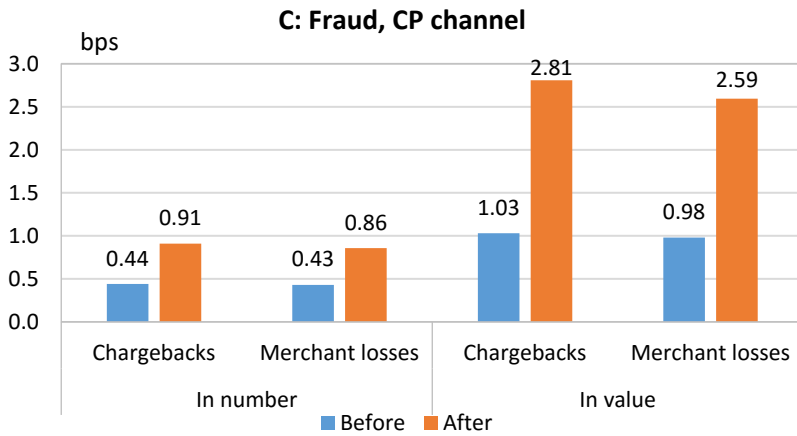
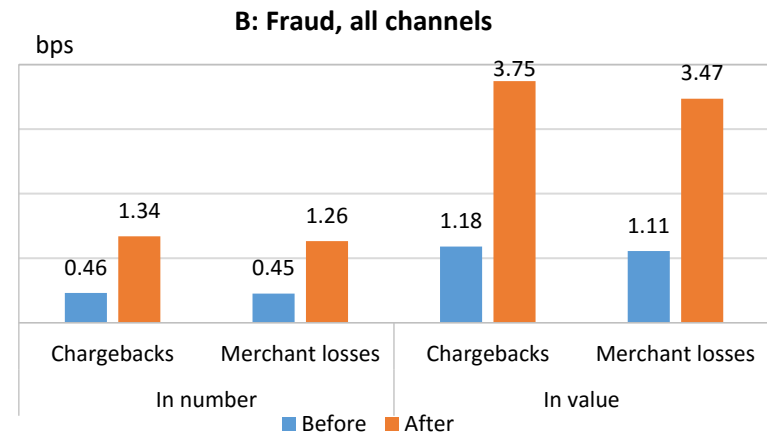
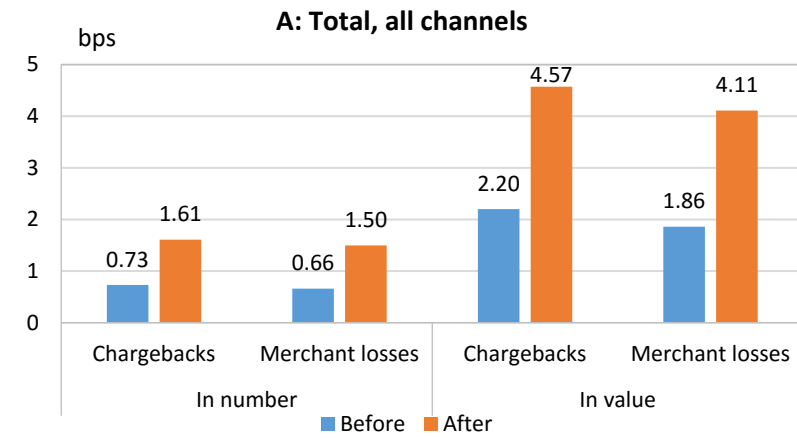


Chart D12: Average value per transaction for signature-based transactions



Restaurant Category

Chart D13: Chargeback and merchant loss rates



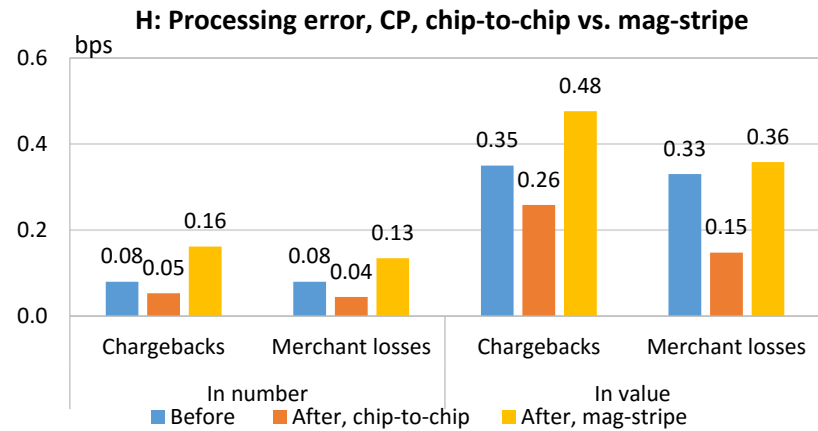
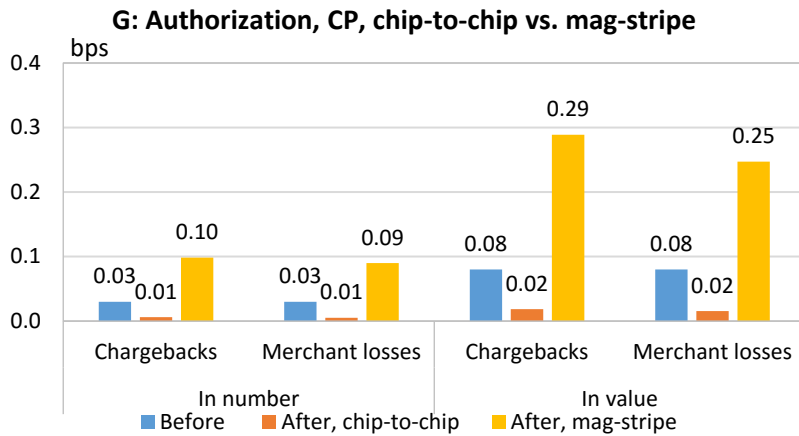
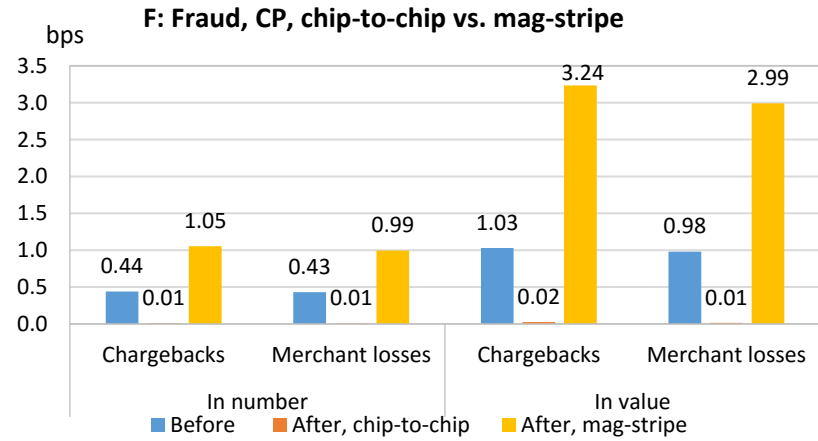
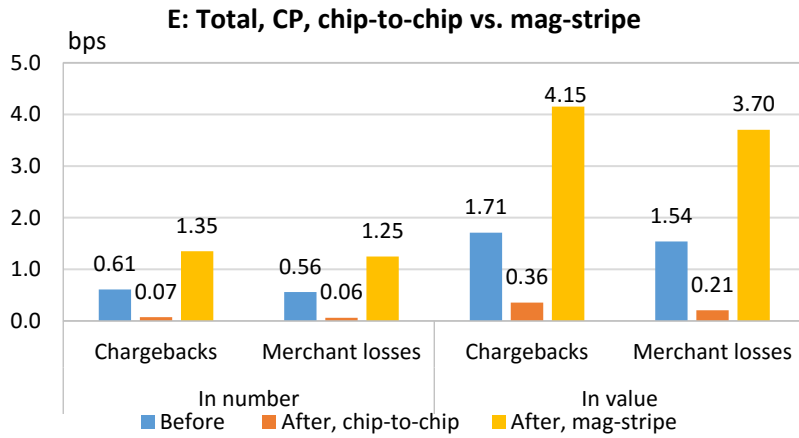


Chart D14: Reason code shares in chargebacks, all channels

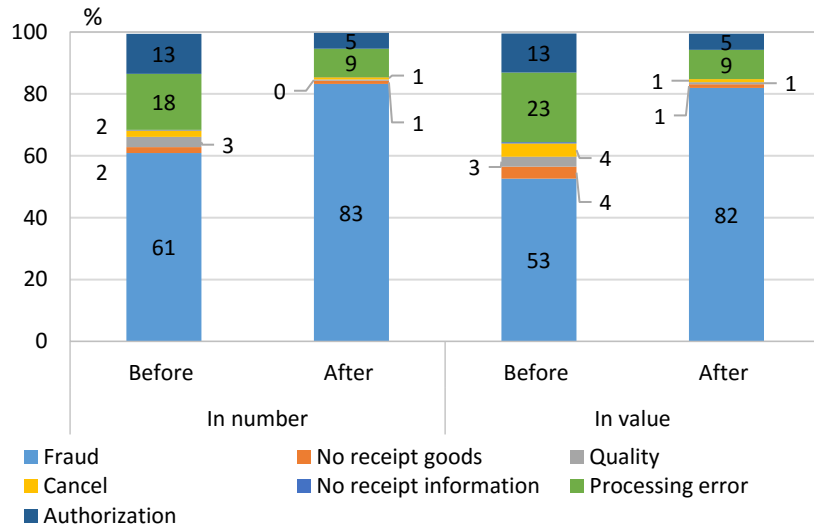


Chart D15: Card present channel share

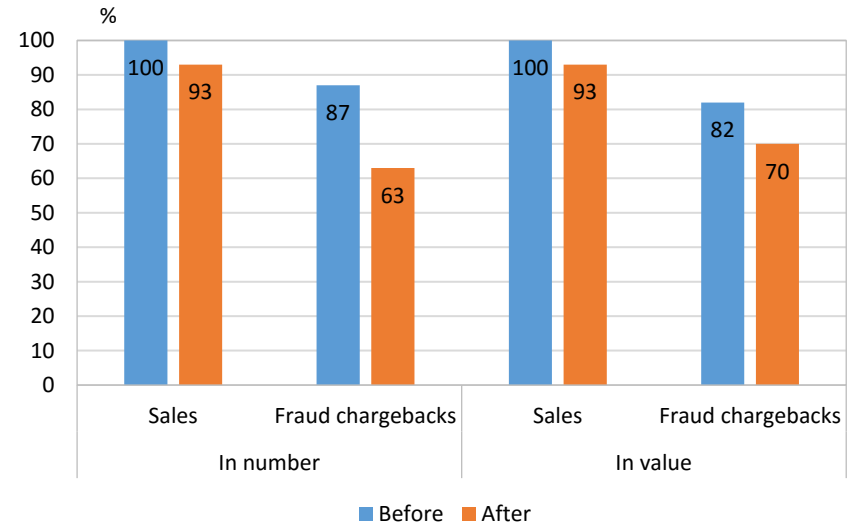
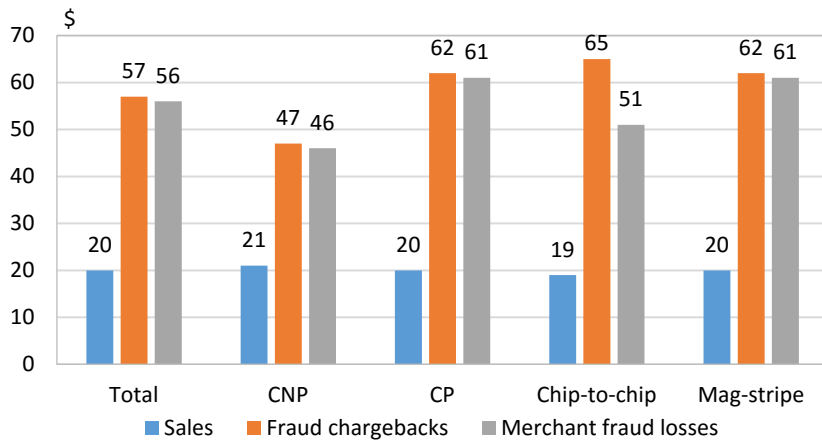
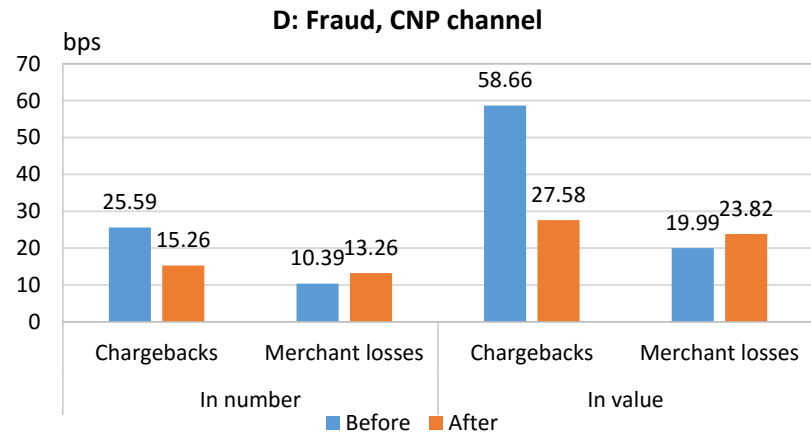
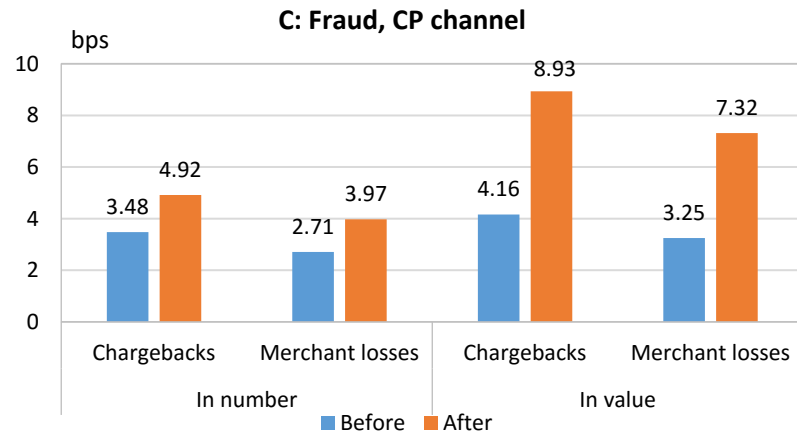
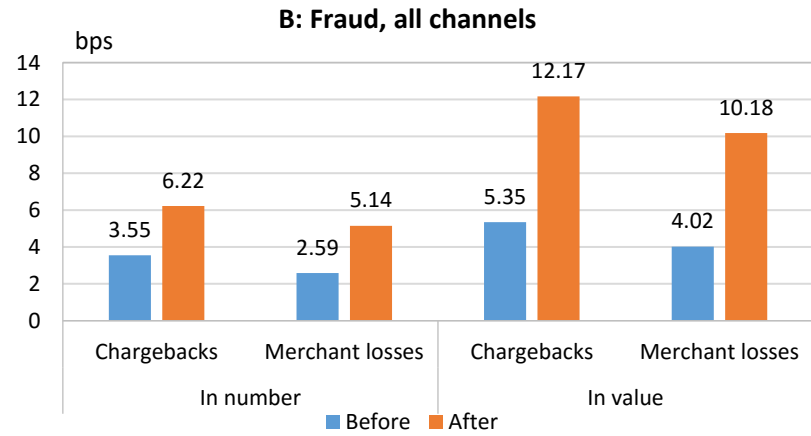
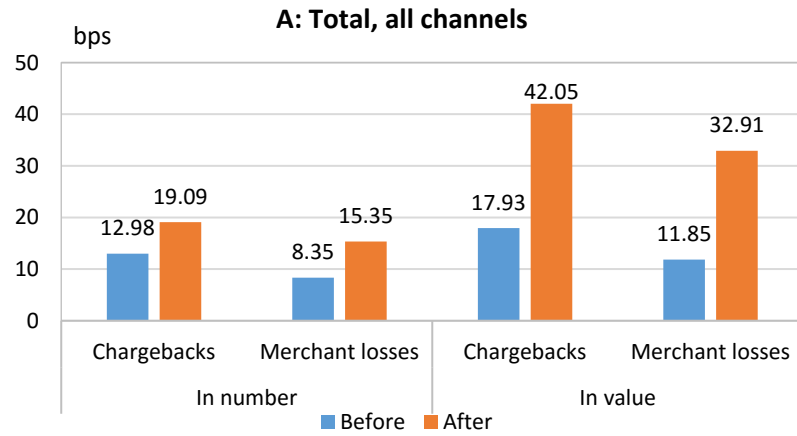


Chart D16: Average value per transaction for signature-based transactions



Travel Category

Chart D17: Chargeback and merchant loss rates



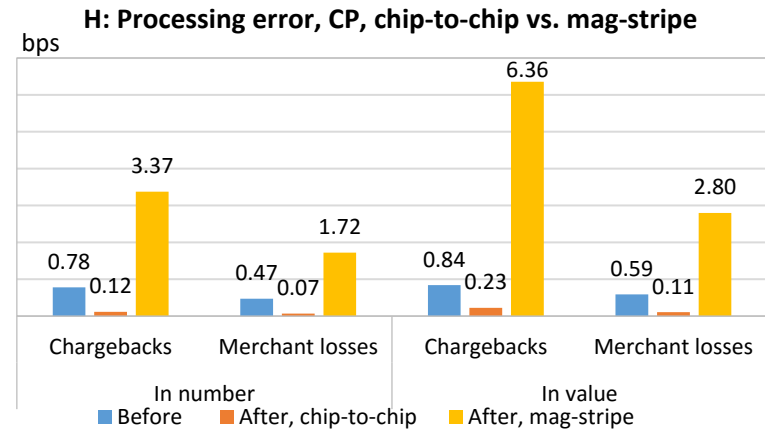
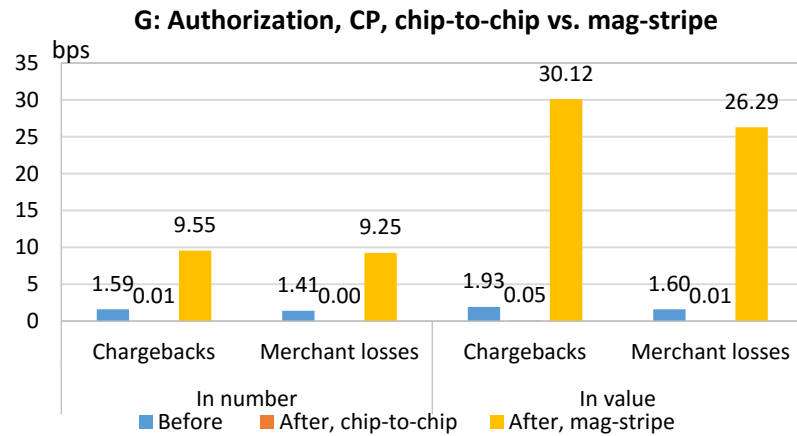
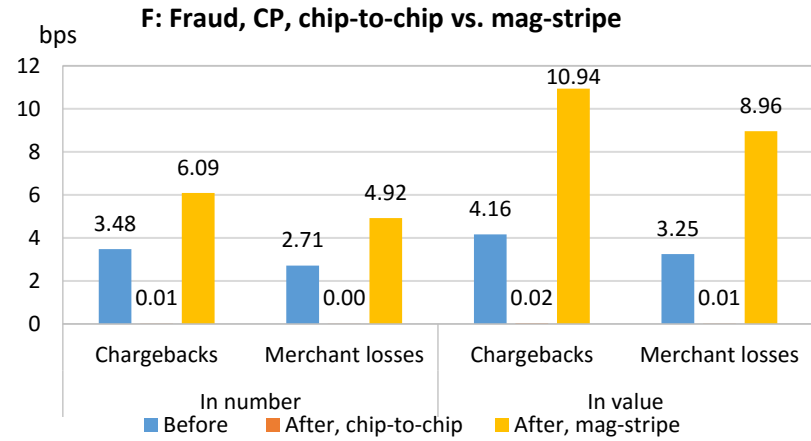
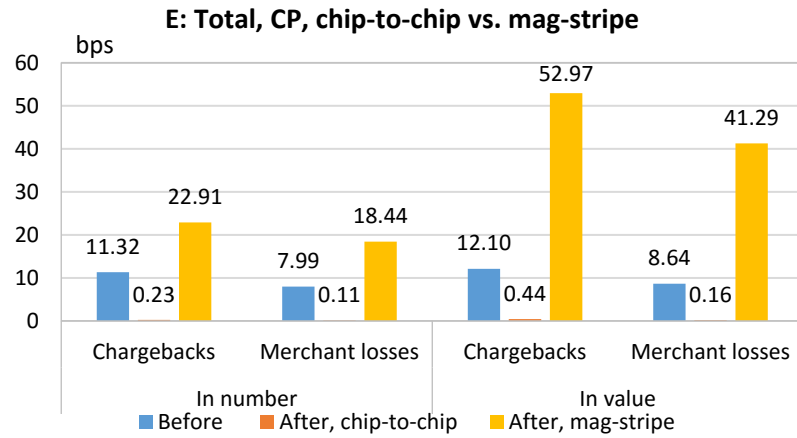


Chart D18: Reason code shares in chargebacks, all channels

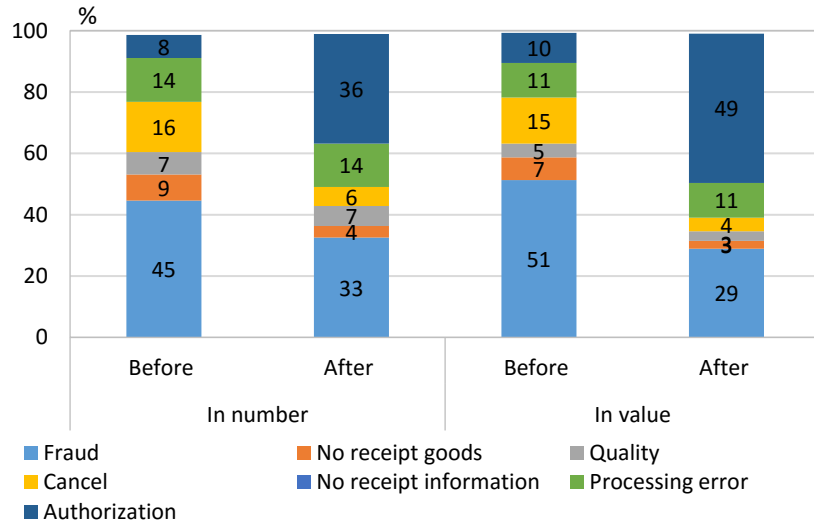


Chart D19: Card present channel share

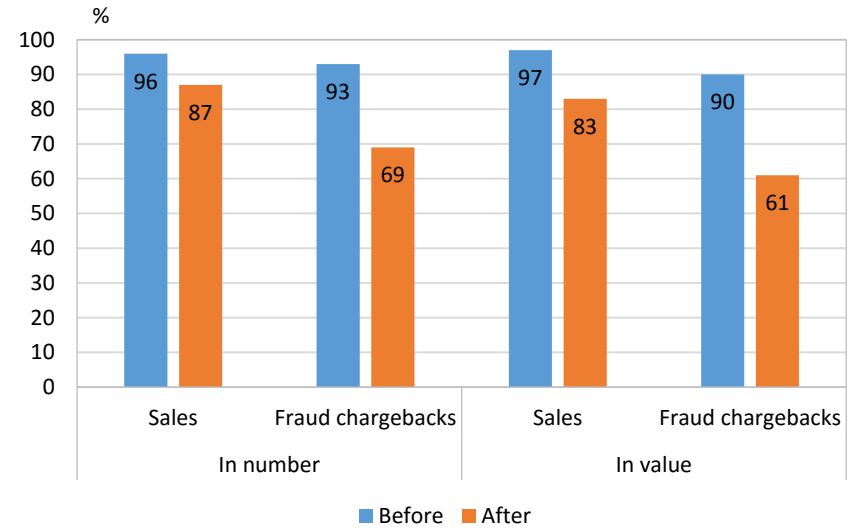
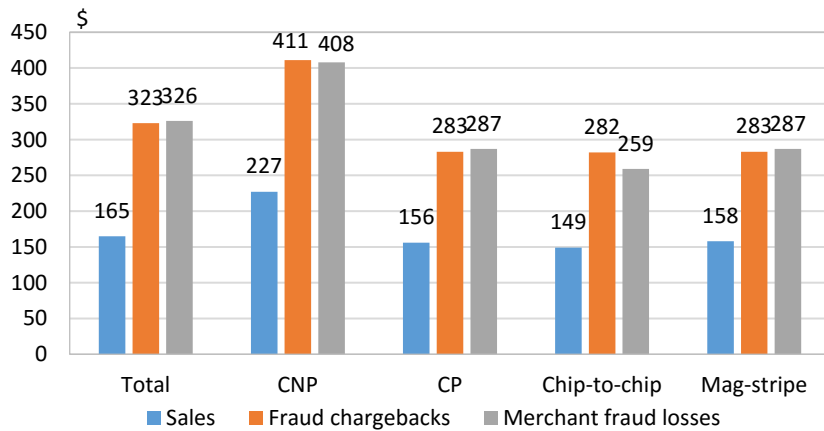


Chart D20: Average value per transaction for signature-based transactions



All merchants

Chart D21: Fraud chargeback and merchant loss rates, CNP channel

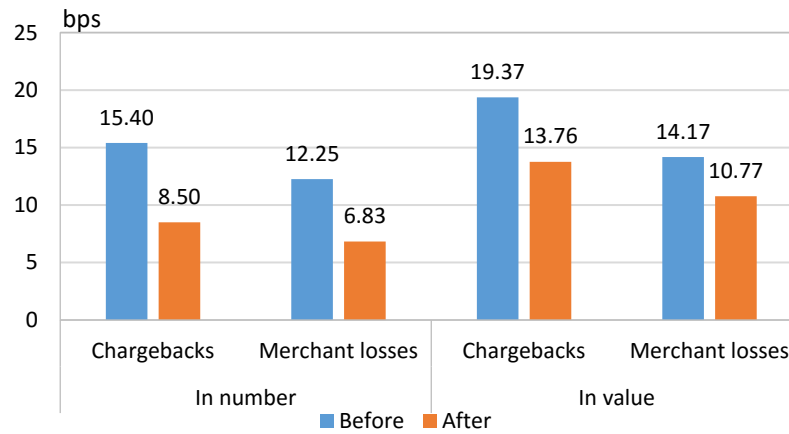


Chart D22: Average value per transaction for signature-based transactions

