Payment Card Fraud Rates in the United States Relative to Other Countries after Migrating to Chip Cards

By Fumiko Hayashi

Although the payment industry around the world has taken major steps to mitigate payment card fraud, the United States has lagged somewhat behind. In the 2000s, many countries adopted or began migrating to a chip card technology called "Europay, Mastercard, and Visa" (EMV) to mitigate fraud from counterfeit cards used for in-person and ATM (or "card-present") transactions. However, the U.S. payment industry did not begin migrating to EMV technology until 2015. In addition, while other countries require chip card users to input personal identification numbers (PINs) to prevent fraud from lost or stolen cards, the United States has yet to adopt this additional safeguard as standard practice, especially for credit card transactions.

These different fraud mitigation strategies may translate to differences in payment card fraud rates. However, comparing fraud rates across countries is challenging for a few reasons. First, fraud rates after U.S. EMV migration were not available until recently. Second, while some countries report fraud *values*, they do not report fraud *rates*; constructing the latter would require detailed transaction data. Third, the level of detail of available fraud rates varies across countries, making it difficult to identify where and why differences in fraud rates occur.

In this article, I compare U.S. payment card fraud rates to fraud rates in three countries with the best available data—Australia, France,

---

Fumiko Hayashi is a research and policy advisor at the Federal Reserve Bank of Kansas City. This article is on the bank's website at ***www.KansasCityFed.org***

and the United Kingdom—and assess what might explain the differences. I find that even after EMV migration, the United States has a significantly higher in-person fraud rate than all three countries but a lower fraud rate for phone, mail, and internet transactions (remote) than Australia and France. Factors explaining the higher in-person fraud rate include U.S. cardholders' greater tendency to use credit cards compared with cardholders in other countries, the U.S. payment industry's late migration to EMV, and EMV implementation without a strong card verification method, such as PINs. The United States' lower remote fraud rate may be partly explained by a smaller fraction of remote payments made at foreign merchants relative to domestic merchants.

Section I discusses challenges to mitigating fraud in the United States. Section II describes what fraud data are collected in the United States and other countries. Section III shows differences in in-person, remote, and overall fraud rates between the United States and other countries and provides potential factors explaining those differences.

I. Challenges to Mitigating Fraud in the United States

Relative to other developed countries, the United States has historically been slow to implement fraud mitigation measures for both in-person and remote transactions. For example, the United States was one of the last developed countries to migrate to EMV chip technology to mitigate counterfeit fraud in the card-present environment. The United States has fallen behind other countries in adopting stronger authentication technologies to mitigate remote fraud as well. France and the United Kingdom, for example, have progressively adopted authentication technologies, such as 3-D Secure (3DS), since the late 2000s. In the United States, however, card issuers are not expected to start supporting a new version of 3DS called EMV-3D Secure until late 2019.[1] This delay in particular may have implications for the overall fraud rate: in general, the remote fraud rate is significantly higher than the in-person fraud rate, and the share of remote payments has been increasing.

Although all countries need to overcome coordination problems in implementing large-scale fraud mitigation measures, such as EMV chip technology and 3DS, the United States may face greater challenges than other countries. First, the U.S. payment industry is highly complex. More than 10,000 financial institutions issue debit cards, many of which

issue credit cards as well. Millions of merchants, billers, and other businesses accept payment cards. Moreover, many card networks and payment service providers process transactions and offer services to mitigate card fraud. Compared with the United States, other countries have fewer card issuers, merchants, card networks, and service providers.

Second, U.S. public agencies, including the Federal Reserve, lack explicit power to regulate payment systems. Although the Federal Reserve plays an active role in improving security in check, automated clearinghouse, and wire systems, it has little involvement in the payment card system. With debit cards, the Board of Governors of the Federal Reserve System regulates only debit card routing and interchange fees received by large debit card issuers. In contrast, governments or central banks in other countries have regulatory power and thus require or pressure private-sector participants to implement fraud mitigation measures. For example, the Banque de France, whose mandate includes security measures for payment cards, led the nationwide adoption of EMV chip technology and 3DS (Stervinou 2015). The Reserve Bank of Australia (RBA), which has explicit payment regulation power, recently encouraged industry participants to implement a coordinated strategy to mitigate remote fraud (Reserve Bank of Australia 2018). And in the European Union, the revised Payment Services Directive required strong customer authentication for electronic payments starting September 14, 2019.[2]

Third, participants in the U.S. payment card industry may not have strong incentives to mitigate fraud. U.S. card issuers receive significantly higher revenues from interchange fees charged to merchants relative to fraud losses than other countries, which may make them less sensitive to fraud. One reason for the higher interchange fees in the United States is that the United States regulates interchange fees only for large debit card issuers, while the European Union and Australia regulate interchange fees for all debit and credit card issuers (Hayashi and Maniff 2019). In the United States, the average interchange fee for a credit card transaction is about 2 percent of the transaction value, while the average interchange fee for a debit card transaction is about 0.6 percent of the transaction value for regulated card issuers and 1.15 percent of the transaction value for exempt issuers.[3] In contrast, in the European Union, interchange fees are capped at 0.3 percent of the transaction

value for credit cards and 0.2 percent for debit cards. In Australia, interchange fees are capped at 0.8 percent of the transaction value for credit cards and 0.2 percent for debit cards, though card networks also face additional caps.[4] As a result, even a small fraud rate difference affects card issuers' bottom line in the European Union and Australia, giving issuers a strong incentive to mitigate fraud.

Fourth, even strong incentives—for example, shifting the financial liability for payment fraud from card issuers to merchants—may not be sufficient to overcome some coordination challenges. Although card networks have been using liability shifts to incentivize parties to adopt fraud mitigation tools, such as EMV chip technology and EMV-3D Secure, the liability shift alone may not provide sufficient incentives. For instance, in the United States, liability for fraudulent transactions at fuel pumps not equipped to handle EMV chip cards was supposed to shift from card issuers to convenience stores in October 2017. However, the shift was postponed to October 2020 due to the significant cost of upgrading fuel pumps to support EMV transactions relative to the expected fraud losses convenience stores would avoid by upgrading. It is unclear whether convenience stores, especially smaller ones, will be ready even by the postponed date.[5]

Fifth, card networks themselves may have conflicting interests when it comes to adopting some fraud mitigation tools, such as PINs, in the United States. Although global card networks have mandated PINs for chip card transactions in many other countries, they have not adopted "chip and PIN" as a standard practice in the United States. These networks may want to promote more effective tools than PINs to mitigate fraud in the United States, such as fingerprint or facial recognition on mobile phones. However, global card networks may also want to avoid competing for merchants with domestic debit card networks that require PINs. When cardholders do not use PINs, merchants typically have no choice but to route transactions to global networks; in contrast, when cardholders use PINs, merchants can choose from at least two networks based on the fee charged to merchants. Credit card issuers may also hope to retain or expand their customer base by not adopting PINs; if U.S. consumers consider remembering multiple PINs burdensome, they may limit the number of credit cards they use.

Sixth, consumers in the United States may receive less information about how to mitigate fraud than consumers in other countries. For example, the United Kingdom's banking and retail industries sponsored a chip-and-PIN advertising campaign that informed consumers about the greater efficacy of PINs in mitigating card-present fraud relative to signatures. In France, the Banque de France has repeatedly communicated with cardholders about their obligations, including keeping PINs safe, protecting card data, and promptly reporting to card issuers any unauthorized transactions or lost or stolen cards. In contrast, U.S. consumers receive little or no information on the efficacy of PINs in mitigating fraud. In fact, U.S. consumers may receive information that *encourages* them to use more fraud-prone payment methods. For example, some debit card issuers have discouraged their cardholders from using PINs by offering rewards for transactions that use signatures, which carry higher interchange fees.

II. Collecting Data on Fraud Rates

Comparing payment card fraud rates in the United States to those in other countries requires consistent data. However, many countries define fraud in different ways, making direct comparisons of fraud rates challenging. Moreover, some countries do not provide detailed breakdowns of fraud rates by transaction type (for example, in-person versus remote). To account for some of these difficulties, I restrict my comparison to Australia, France, and the United Kingdom. In all three countries, the central bank or a well-established payment organization defines payment fraud and collects detailed fraud statistics.[6]

Even this restricted sample poses some challenges. For example, the definition of payment fraud is consistent across only three of the four countries. The United States, Australia, and the United Kingdom define payment fraud as a transaction that a third party initiates without the authorization, agreement, or voluntary assistance of the lawful cardholder with the intent to deceive for personal gain. France, however, also includes first-party fraud in their definition. One example of first-party fraud is the authorized cardholder falsely claiming to be defrauded after performing a genuine transaction to purchase goods or services online. Nevertheless, fraud definitions in all four countries share one crucial feature: they do not include attempted fraud that was

prevented before the payment was settled. Thus, only payment fraud that resulted in financial loss, regardless of who incurred such loss, is included in these countries' fraud statistics.[7]

All four countries report the overall fraud rate in value—that is, the total value of all fraudulent transactions divided by the total value of all transactions, regardless of transaction channels, card types, and geographic areas. However, the availability of detailed fraud rates differs across countries. The United States and France report fraud rates broken down by transaction type, but Australia and the United Kingdom report only fraud *values* by transaction type. To calculate fraud rates by transaction type for Australia, I use detailed card transaction data from the RBA, coupled with detailed fraud values reported by the Australian Payments Network (AusPayNet). I cannot calculate detailed fraud rates for the United Kingdom, as detailed card transaction data are not readily available.

Table 1 shows the available fraud rates for different transaction types in all four countries. The availability of different rates varies significantly by country. For example, fraud rates for card-present transactions, which include both ATM and in-person purchase transactions, are available in the United States, Australia, and France, but not in the United Kingdom, which reports only the card-present fraud value. The United States and France divide the card-present fraud rate further into ATM and in-person fraud rates. And the United States subdivides the in-person fraud rate even further based on either authentication technology (chip or no chip) or card verification method (PIN or no PIN). Other countries do not subdivide in-person fraud rates in this way because in-person transactions in these countries typically use both chip and PIN. France and the United Kingdom, however, do report a contactless fraud rate. Card users make contactless transactions by waving or tapping their card at the card reader. Typically, these transactions are limited to small-value transactions and do not require a PIN.[8]

Although all four countries report remote fraud rates, only France and the United Kingdom report more detailed remote fraud rates. The United Kingdom reports an online fraud rate, and France reports both online and mail-or-telephone order fraud rates. In addition, France reports remote fraud rates for different merchant sectors.

Table 1
Data Availability for Fraud Rates in Value by Country

Country	United States	Australia	France	United Kingdom
Overall	x	x	x	x
Transaction types				
Card-present	x	x	x	
ATM	x		x	
In-person purchase	x		x	
Chip versus no chip	x			
PIN versus no PIN	x			
Contactless			x	x
Remote purchase	x	x	x	x
Online			x	x
Mail or telephone order			x	
By merchant sector			x	
Card types				
Credit versus debit	x			
Transaction or card origin				
Domestic versus foreign merchants		x	x	x
Domestic versus foreign cards		x	x	

Sources: Federal Reserve Board of Governors, AusPayNet, Banque de France, Financial Fraud Action UK, and UK Finance.

The United States distinguishes between debit and credit card fraud, while other countries do not break fraud statistics down by card type. Specifically, the United States reports separate fraud statistics for credit and debit cards and divides debit card fraud further into non-prepaid and prepaid card fraud.

Countries also provide different levels of detail on payment card fraud by card origin. Although all four countries report statistics on fraud conducted with cards issued domestically, Australia, France, and the United Kingdom break domestic card fraud down further based on whether the fraudulent transactions took place at domestic or foreign merchants.[9] In addition, Australia and France report statistics on fraud conducted with foreign-issued cards that are used at domestic merchants.

Finally, on top of the differences in fraud breakdowns shown in Table 1, the cross-country data differ in one other crucial aspect: frequency. The United Kingdom, France, and Australia have collected fraud data every year since 2001, 2002, and 2010, respectively, and all three countries

release the data with a modest delay. For example, 2018 data for all three countries became available within the first seven months of 2019. In contrast, the Federal Reserve System began collecting fraud statistics for the United States in 2012 and only recently released 2015 and 2016 fraud statistics in a report published by the Board of Governors.[10]

III. Comparing Fraud Rates across Countries

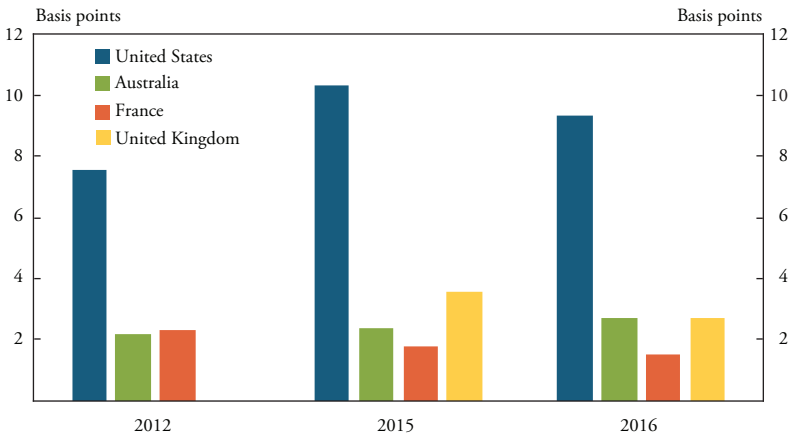
To facilitate direct comparisons across all four countries, I restrict my comparison years to 2012, 2015, and 2016—the three years for which detailed U.S. fraud statistics are available. In addition, I focus on fraud conducted with domestic cards, as the United States and the United Kingdom do not report statistics on fraud conducted with foreign cards at domestic merchants.[11] Finally, I focus on fraud rates in value for two reasons. First, detailed fraud rates measured by the number of transactions are unavailable in some countries; and second, the payment industry typically uses fraud rates in value as a benchmark, rather than fraud rates in number.

In-person fraud rates

In 2012, 2015, and 2016, the in-person fraud rate was more than three times higher in the United States than in any other country. Chart 1 compares in-person fraud rates in the United States, Australia, and France with the "contactless fraud rate" in the United Kingdom, the closest measure of in-person fraud available. Although Australia publishes a card-present fraud value, they do not break this value down into in-person and ATM fraud values. Thus, I calculate the highest possible in-person fraud rate for Australia by assuming a zero fraud rate for ATM transactions. Even though Australia's in-person fraud rates are overstated, the United States' in-person fraud rates (blue bars) were still higher than the in-person fraud rates in Australia (green bars) by 5 basis points in 2012, 8 basis points in 2015, and 7 basis points in 2016. In addition, the United States' in-person fraud rates were higher than those in France (orange bars) by 5 basis points in 2012 and by 8 basis points in 2015 and 2016. The United States' in-person fraud rate was also higher than the contactless fraud rate in the United Kingdom (yellow bars) by 7 basis points in 2016.[12]

Chart 1

In-Person Fraud Rates



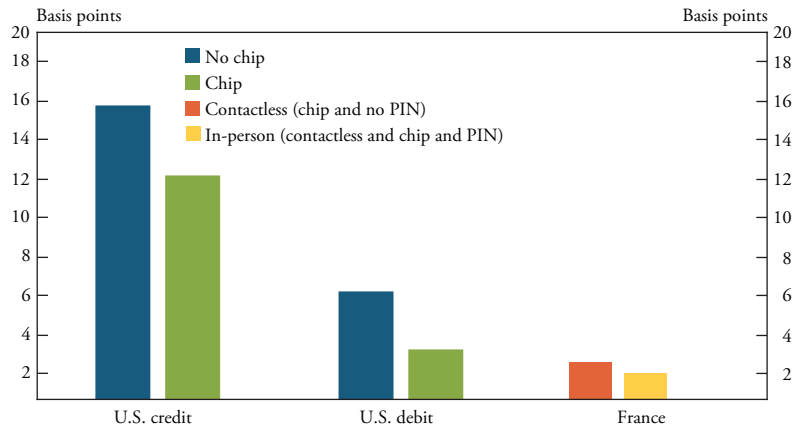
Notes: I calculate the in-person fraud rate in Australia by assuming the ATM fraud rate is zero. The rate shown for the United Kingdom is the contactless fraud rate.
Sources: Federal Reserve Board of Governors, AusPayNet, RBA, Banque de France, Financial Fraud Action UK, and author's calculations.

Three factors may explain why the in-person fraud rate has been significantly higher in the United States than in other countries. First, the United States has a smaller share of chip transactions in total in-person transactions. EMV migration did not occur in the United States until 2015. In 2016, the first full year after the migration, chip transactions accounted for 23 percent of the value of all in-person transactions. In the western European countries, which include France and the United Kingdom, chip transactions already accounted for 97 percent of the value of all in-person transactions in 2015 (EMVCo 2016).[13] These differences likely contributed to differences in fraud rates, as chip transactions are less likely to be fraudulent overall. The left side of Chart 2 shows that in 2016, the U.S. no-chip fraud rate (blue bar) was 4 basis points higher than the chip fraud rate (green bar) for credit card transactions and 3 basis points higher for debit card transactions.

The second factor that may contribute to the United States' higher in-person fraud rate is that the United States uses weaker card verification methods with its chip transactions than other countries. In Australia, France, and the United Kingdom, card users provide PINs when making a chip transaction, unless that transaction is contactless.[14] Because only cardholders should know their PINs, these transactions

Chart 2

Fraud Rates by Card Type and Authentication Method in 2016



Sources: Federal Reserve Board of Governors and Banque de France.

are less likely to be fraudulent. Indeed, the right side of Chart 2 shows that in 2016, the French fraud rate for contactless transactions (orange bar) was 0.7 basis points higher than for in-person transactions, which include both contactless and chip-and-PIN transactions. Although data on chip-and-PIN transactions alone are not available, the comparison makes clear that contactless transactions are more susceptible to fraud. In contrast, in the United States, the vast majority of credit card chip transactions and some debit card chip transactions are made with no card verification or a weak card verification method, such as a signature. Although some in-person transactions are made with a strong non-PIN card verification method, such as fingerprint verification or facial recognition, those transactions account for a very small proportion of chip transactions. A weak or absent card verification method may partly explain the higher chip fraud rate for U.S. credit cards (the first green bar in Chart 2) than debit cards (the second green bar).

The third factor that may contribute to the United States' higher in-person fraud rate is that U.S. cardholders are more likely to use credit cards than cardholders in some other countries. Credit card transactions accounted for 44 percent of the value of U.S. in-person transactions in 2016. Although the share was similar in Australia, the share in the United Kingdom was only 28 percent. The equivalent statistic is not available in France, but credit card transactions accounted for only

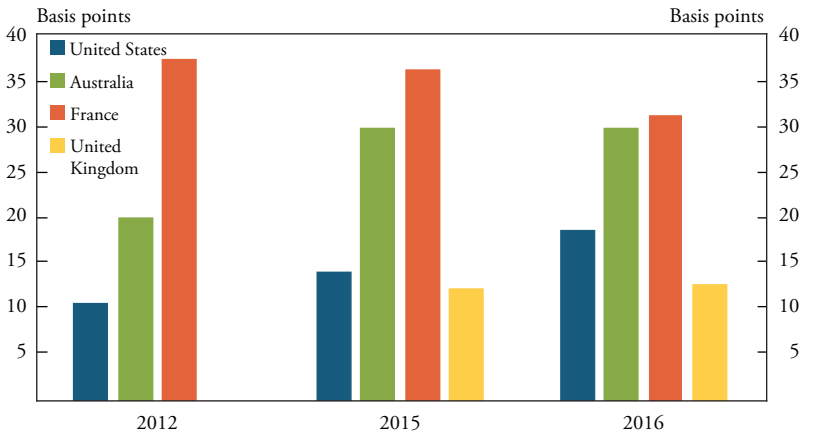
31 percent of the value of *all* purchase transactions in 2016. The higher share in the United States may partly explain the higher rate of in-person fraud. The first two sets of bars in Chart 2 show that credit cards carry higher fraud rates than debit cards regardless of whether they use chips. Why credit cards are more prone to fraud than debit cards requires further research; however, the two card types differ notably in both the distribution of transactions between business and consumer cardholders and their shares of card application fraud. In the United States, the share of business transactions was significantly higher in credit card transactions than in debit card transactions (31 versus 9 percent). The share of fraudulent application—perpetrators using stolen identities or false information to obtain a new card and make payments using that card—was also significantly higher for credit cards than debit cards (6.9 versus 0.1 percent).[15]

Remote fraud rates

Unlike in-person fraud rates, the remote fraud rate in the United States has been lower than in Australia and France but higher than in the United Kingdom. Chart 3 shows the remote fraud rates for the United States, Australia, and France in 2012, 2015, and 2016 as well as the e-commerce fraud rate for the United Kingdom in 2015 and 2016.[16] In 2012, the U.S. remote fraud rate (blue bars) was 27 basis points lower than that of France (orange bars). This gap narrowed to 22 basis points in 2015 and again to 13 basis points in 2016. The U.S. remote fraud rate was also 11 basis points lower than that of Australia (green bars) in 2016. However, the United States has had a higher rate of remote fraud relative to the rate of e-commerce fraud in the United Kingdom (yellow bars). Specifically, the U.S. remote fraud rate was 2 basis points higher in 2015 and 6 basis points higher in 2016.

Two factors may at least partly explain the lower remote fraud rate in the United States relative to Australia and France. First, the vast majority of remote transactions on U.S.-issued cards are made at domestic merchants rather than at foreign merchants. Even if I assume that all U.S. transactions made at foreign merchants were remote transactions, transactions at foreign merchants accounted for less than 6 percent of the value of remote transactions in 2016. In contrast, remote transactions at foreign merchants accounted for 26 percent of the value of all

Chart 3
Remote Fraud Rates



Notes: I calculate the remote fraud rates in Australia by assuming that transactions at foreign merchants are distributed between in-person and remote transactions in the same way as transactions at domestic merchants. The rate shown for the United Kingdom is the e-commerce fraud rate.
Sources: Federal Reserve Board of Governors, AusPayNet, RBA, Banque de France, Financial Fraud Action UK, and author's calculations.

remote transactions on French-issued cards, more than 13 percent on UK-issued cards, and about 7 percent on Australian-issued cards. These shares likely influence remote fraud rates: although equivalent data for the United States are not available, evidence from the other three countries suggests that remote fraud is significantly more prevalent at foreign merchants than domestic merchants. In 2018, for example, the Australian remote fraud rate was 151 basis points higher at foreign merchants than that at domestic merchants.[17]

Second, the composition of remote transactions by merchant sector in the United States may differ from other countries. If remote transactions in the United States are more concentrated in merchant sectors with less fraud, such as utilities, the remote fraud rate might be lower than in countries whose remote transactions are more concentrated in higher fraud sectors, such as travel and transportation or online gaming. Although data on merchant composition is not available in the United States, remote fraud varies significantly by merchant sector in France (Banque de France 2019). In addition, Hayashi, Markiewicz,

and Minhas (2018) show that fraud chargeback rates for card-not-present transactions vary significantly by merchant sector in the United States. This rate may be a good proxy for remote fraud rates given that merchants are generally liable for remote fraud. Furthermore, about 20 percent of remote payments in the United States in 2015 were recurring, installment, or other non-purchase payments. These payments may have lower fraud rates than ad hoc purchase transactions because recurring and installment payments require prior contracts between consumers and merchants, such as billers and installment loan providers. These merchants thus know more details about their customers, making them more likely to detect fraudulent transactions.

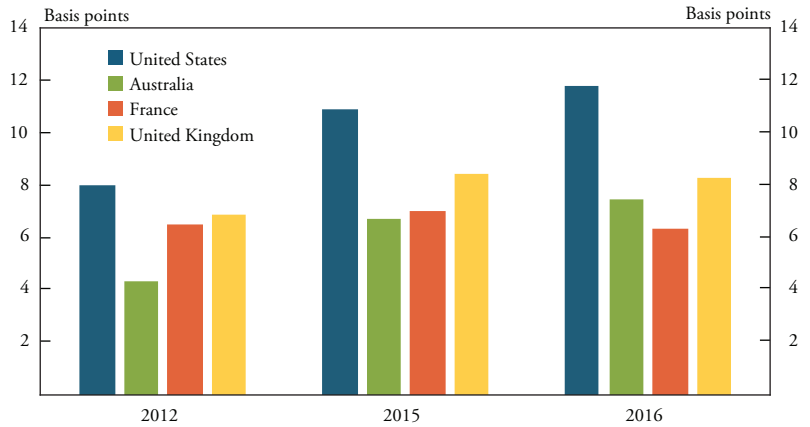
Overall fraud rates

The overall fraud rate, which is the weighted average of in-person, remote, and ATM fraud rates, has been the highest in the United States. Chart 4 shows that the United States had the highest overall fraud rate of all four countries in 2012, 2015, and 2016. The United States' 11.8 basis points fraud rate in 2016 may in fact be understated: because the U.S. ATM fraud rate is not available for 2016, I assume the ATM fraud rate was zero when constructing the overall fraud rate for that year. Even under this assumption, the gap between the United States and the other three countries appears to have widened over time. For example, the U.S. fraud rate (blue bars) was higher than the rate in the United Kingdom (yellow bars) by 1.1 basis points in 2012, 2.5 basis points in 2015 and at least 3.5 basis points in 2016.

Two main factors may explain the United States' highest overall fraud rate. First, as discussed previously, the United States has a significantly higher in-person fraud rate than other countries, contributing to its higher overall fraud rate. Second, the United States has a greater share of remote transactions in total card transactions, also likely contributing to its higher overall fraud rate. Although the remote fraud rate is lower in the United States than that in Australia or France, remote transactions are still more prone to fraud than in-person and ATM transactions. Thus, a country with a larger share of remote transactions is more likely to have a higher overall fraud rate.

Chart 4

Overall Fraud Rate



Note: The U.S. overall fraud rate in 2016 is calculated assuming a zero fraud rate for ATM transactions.
Sources: Federal Reserve Board of Governors, AusPayNet, RBA, Banque de France, Financial Fraud Action UK, and author's calculations.

Conclusion

The United States was one of the last developed countries to migrate to EMV chip technology to mitigate counterfeit card fraud. The United States continues to lag behind some European countries in adopting other fraud-mitigation initiatives, such as chip-and-PIN or 3DS authentication. However, comparing payment card fraud across countries can be challenging: available data vary by country and statistics on U.S. payment card fraud after the EMV migration became available only recently.

I compare in-person, remote, and overall fraud rates in the United States to those in Australia, France, and the United Kingdom, and examine factors explaining the differences. I find that the United States has a significantly higher in-person fraud rate than Australia, France, and the United Kingdom but a lower remote fraud rate than Australia and France. In addition, I find that the United States has the highest overall fraud rate, which is the weighted average of ATM, in-person, and remote fraud rates. A weaker authentication technology (no chip) and a weaker or absent card verification used for many of the in-person transactions—as well as a greater share of credit card transactions for in-person transactions—may explain the United States' higher in-person

fraud rate. A smaller proportion of remote transactions made at foreign merchants may explain the United States' lower remote fraud rate. And both the higher in-person fraud rate and greater share of remote transactions in card transactions may explain the United States' higher overall fraud rate.

Although the overall fraud rate reveals the prevalence of fraud, it may not be a good measure of the effectiveness of fraud mitigation. Fraud rates vary significantly by transaction type, and the composition of transactions across these types varies across countries and may shift from year to year within a country. Detailed fraud rates would help better assess the effectiveness of fraud mitigation. The United States has collected more detailed fraud statistics than some other countries, but it does not break down fraud rates by card verification methods, foreign versus domestic merchants, and business versus consumer card users. Collecting and publicizing these breakdowns may help the U.S. payment industry more effectively monitor and mitigate fraud.

Endnotes

[1]3DS is a messaging protocol that strengthens the authorization of online or e-commerce transactions using digital certificates and passwords to authenticate both customer and payment method credentials. The three domains consist of the merchant/acquirer, the issuer, and the payment system. EMV-3D Secure is a new protocol with improved features such as seamless authentication steps, mobile capabilities, and more transaction data. Visa postponed the U.S. activation date for EMV-3D Secure to August 2020, while Mastercard aims to activate the standard in December 2019.

[2]Strong customer authentication requires at least two of the following three elements: something the customer knows (such as a password), something the customer has (such as a mobile phone), and something inherent to the customer (such as a fingerprint). Although the effective date of the strong customer authentication requirement was September 14, 2019, the Financial Conduct Authority agreed not to take enforcement action against firms in areas covered by the migration plan until 18 months after the effective date.

[3]The interchange fee received by large debit card issuers, defined as issuers with assets of $10 billion or more, is capped at 21 cents per transaction plus 0.05 percent of the transaction value.

[4]In addition to the 0.8 percent cap, each credit card network must set interchange fees so that the total value of interchange fees payable on credit card transactions in a year do not exceed 0.5 percent of their total value. An interchange fee for a debit card transaction must not exceed 0.2 percent of the transaction value when the interchange fee is assessed as a percentage of the transaction value and must not exceed 15 cents when the interchange fee is a fixed amount per transaction.

[5]The upgrading cost is estimated to be $100,000 to $250,000 per store.

[6]The European Central Bank has reported card fraud statistics in the Single European Payments Area (SEPA) (European Central Bank 2018). I exclude the SEPA from the comparison so that I can separately examine France and the United Kingdom, two of the three countries that historically have the highest fraud rates in the SEPA.

[7]The United Kingdom reports attempted fraud separately.

[8]A supplemental regulation (2018/389) to the revised European Payments Directive limits the value of individual contactless transactions to €50. Cardholders can continue their contactless transactions without using a PIN until their cumulative value of contactless transactions since their last use of a PIN reaches €150 or until they make five consecutive contactless transactions.

[9]In France, foreign cards and foreign merchants are further divided into SEPA and non-SEPA cards or merchants.

[10]In addition, the Board has reported debit card fraud statistics biennially in its mandatory studies on debit card issuers whose interchange fees are regulated

under Regulation II (Debit Card Interchange Fees and Routing); the most recent study reports the 2017 statistics.

[11]Fraud statistics involved with foreign cards at domestic merchants have not been collected in the United States and the United Kingdom. However, for domestic merchants and their processors, understanding statistics of fraud involved with foreign cards is important because they could be financially liable for such fraud. In Australia and France, fraud rates of foreign cards are higher than those of domestic cards, especially for remote transactions.

[12]France reports both in-person and contactless fraud rates, and the latter has been 0.1 to 0.7 basis points higher than the former during the 2015–17 period.

[13]Although data on chip transactions are unavailable for Australia, the share is likely greater than in the United States because Australia began EMV migration several years earlier.

[14]In 2017, contactless payments accounted for 3 percent of the value of all in-person transactions in France and 13 percent in the United Kingdom.

[15]Fraudulent application is the fastest growing fraud type in the United States. This type of fraud may include synthetic identity fraud, in which perpetrators combine fictitious and real information to create new identities to defraud credit card issuers, other financial institutions, government agencies, or individuals. The Federal Reserve Banks (2019) discuss causes and contributing factors of synthetic identity fraud.

[16]Neither the remote fraud rate nor the e-commerce fraud rate is available for 2012 in the United Kingdom. I use the e-commerce fraud rate for 2015 and 2016 in the United Kingdom because the remote fraud rate is unavailable in those years. In 2018, the remote and e-commerce fraud rates were almost equivalent, suggesting the e-commerce rate may be a good proxy.

[17]In 2018, the remote fraud rates at domestic and foreign merchants were 14 basis points and 165 basis points in Australia, 17 basis points and 68 basis points in France, and 11 basis points and 25 basis points in the United Kingdom.

References

Banque de France. 2019. *Rapport Annuel de l'Observatoire de la Sécurité des Myens de Paiement 2018*. Paris: Banque de France.

EMVCo. 2016. "Number of EMV Chip Payment Cards in Global Circulation Increases to 4.8 Billion." June.

European Central Bank. 2018. *Fifth Report on Card Fraud, September 2018*. Frankfurt, European Central Bank.

Federal Reserve Banks. 2019. "Synthetic Identity Fraud in the U.S. Payment System: A Review of Causes and Contributing Factors." Federal Reserve Banks, *Payments Fraud Insights*, July.

Hayashi, Fumiko, and Jesse Leigh Maniff. 2019. "Public Authority Involvement in Payment Card Markets: Various Countries. August 2019 Update." Federal Reserve Bank of Kansas City, Payments System Research, August. Available at https://doi.org/10.18651/ICF/PublicAuthority

Hayashi, Fumiko, Zach Markiewicz, and Sabrina Minhas. 2018. "The Initial Effects of EMV Migration on Chargebacks in the United States." Federal Reserve Bank of Kansas City, Research Working Paper no. 18-10, December. Available at https://doi.org/10.18651/RWP2018-10

Reserve Bank of Australia. 2018. "Payments System Board Update: August 2018 Meeting." Press release, August.

Stervinou, Alexandre. 2015. "Monitoring Payment Fraud: A Key Piece to the Puzzle." Proceedings from the Federal Reserve Bank of Kansas City 2015 International Payments Conference, *The Puzzle of Payments Security: Fitting the Pieces Together to Protect the Retail Payments System*, Kansas City, MO, June 25–26.