kcFED Payments System Research Briefing

# Did Card-Present Fraud Rates Decline in the United States After the Migration to Chip Cards?

*By Fumiko Hayashi*

*The U.S. payments industry began migrating to EMV chip-card technology in the mid-2010s to mitigate card-present fraud, especially counterfeit fraud. However, for non-prepaid debit card transactions processed by dual-message networks, the counterfeit fraud rate has not declined, and the lost-or-stolen fraud rate and overall card-present fraud rate have increased. For these transactions, card-present fraud loss rates have declined for issuers but increased for merchants and cardholders.*

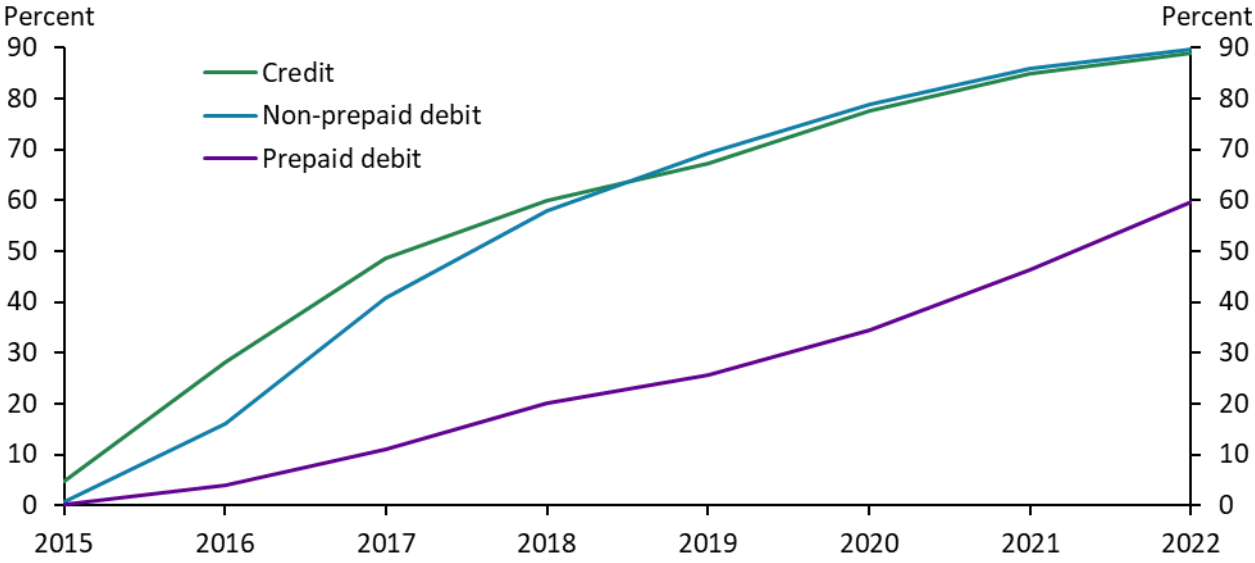
Since the migration to chip-card or "Europay, Mastercard, and Visa" (EMV) technology began, both counterfeit and lost-or-stolen fraud rates for card-present transactions have declined in many countries and jurisdictions. Has card-present fraud in the United States, a comparatively late adopter of EMV technology, followed the same trend? In this *Payments System Research Briefing*, I examine how counterfeit and lost-or-stolen fraud rates as well as the overall card-present fraud rate have changed in the United States for non-prepaid debit card transactions since EMV migration. I also discuss how fraud losses have been reallocated across issuers, merchants, and cardholders.

**EMV migration in the United States**

The United States migrated to EMV chip-card technology relatively late compared with many other countries. In some countries, EMV migration began during the 2000s and was often driven by government initiatives or mandates. In the United States, however, EMV migration was led by the payments industry, partly via changes to card networks' rules. In 2011 and 2012, U.S. card networks announced that effective October 1, 2015, fraud liability for card-present transactions would shift from issuers to merchants if the merchant had not installed a point-of-sale terminal to accept an issuer's chip card.[1] The card issuer would remain liable for card-present fraud if neither or both issuer and merchant had adopted chip technology.[2]

Since the fraud liability shift took effect in 2015, EMV adoption has increased significantly in the United States, and the share of chip-to-chip transactions (in which the chip embedded in a card sends information to a chip-enabled point-of-sale terminal) has risen steadily. Chart 1 shows that the share of chip-to-chip transactions in card-present transactions increased from less than 5 percent in 2015 to nearly 90 percent in 2022 for credit cards (green line) and non-prepaid debit cards (blue line), and from almost zero in 2015 to 60 percent in 2022 for prepaid debit cards (purple line). Nevertheless, the United States still lags other parts of the world except the Asia-Pacific region in EMV adoption. In 2022, chip-to-chip transactions accounted for almost all card-present transactions in western Europe, Africa, the Middle East, Canada, Latin America, and the Caribbean, and for more than 95 percent of card-present transactions in eastern Europe (EMVCo 2024).

**Chart 1: Share of chip-to-chip transactions in card-present transactions in the United States**




Source: Board of Governors of the Federal Reserve System.

**Counterfeit, lost-or-stolen, and card-present fraud rates in the United States**

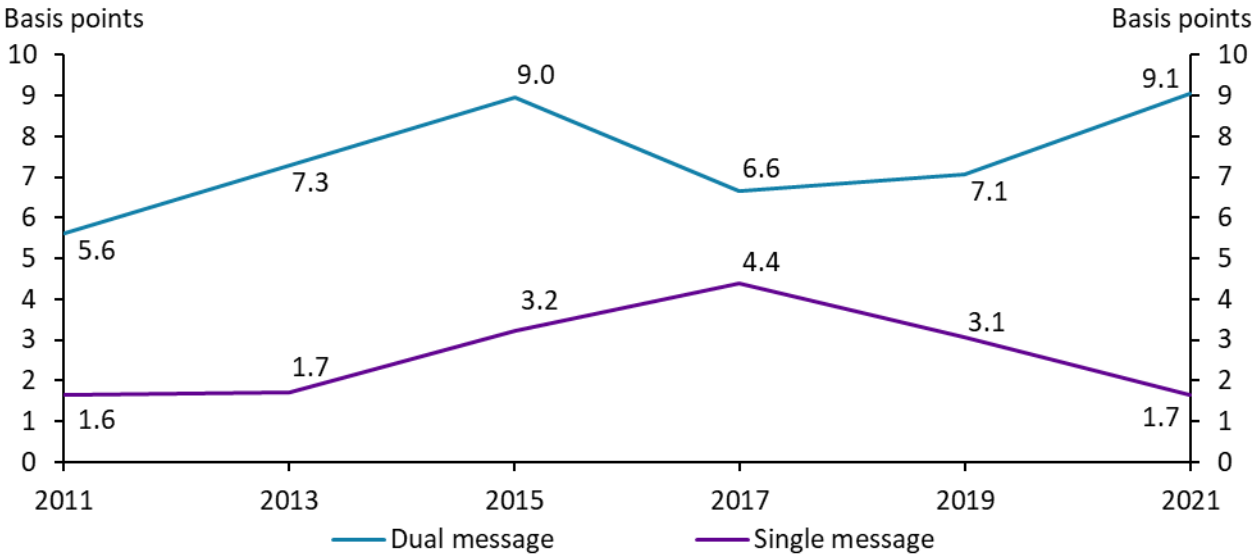
EMV chip-card technology was intended to mitigate card-present fraud from counterfeit cards. The chip embedded in a card generates a unique code for each transaction, making replication or reuse of the information virtually impossible. In many countries, chip cards are used with a PIN to mitigate fraud due to lost or stolen cards, because in theory, only cardholders know their PINs. However, in the United States, credit cards with chips require either a signature or no authentication, while debit cards with chips use a PIN only if required by the network on which the transaction is processed. Dual-message networks (such as Visa, Mastercard, and Discover), which send separate messages for transaction authorization and payment clearing, use the same infrastructure as credit card networks, and thus cardholders are traditionally authenticated with a signature.[3] Single-message networks (such as STAR, NYCE, Pulse, and others), which send a single message for both transaction authorization and payment clearing, originated from ATM networks, so cardholder authentication is traditionally done with a PIN (Hayashi, Sullivan, and Weiner 2003). Because counterfeit and lost-or-stolen fraud account for more than 80 percent of card-present fraud for U.S. debit cards, EMV chip-card technology could also mitigate overall card-present fraud.

To assess the effect of EMV adoption on fraud in the United States, I calculate counterfeit, lost-or-stolen, and card-present fraud rates using data from the Board of Governors of the Federal Reserve System. The Federal Reserve Board (2018) provides estimates of U.S. card-present (or in-person) and card-not-present (or remote) fraud rates for credit, non-prepaid debit, and prepaid debit card transactions in 2012, 2015, and 2016. Since then, these specific fraud rates have not been estimated in the United States. However, the Federal Reserve Board's biennial reports on debit cards include fraud data from 2011 to 2021.[4] I use these data to calculate fraud rates for non-prepaid debit card transactions processed by dual-message networks and single-message networks separately.[5] I define the counterfeit, lost-or-stolen, or card-present fraud rate as the value of counterfeit, lost-or-stolen, or card-

present fraud divided by the value of card-present transactions (including both fraudulent and non-fraudulent transactions).[6]

Since EMV migration, the counterfeit fraud rate of non-prepaid debit cards has declined for single-message networks but not for dual-message networks. Chart 2 shows that for single-message networks (purple line), the counterfeit fraud rate increased from 3.2 basis points in 2015 (when EMV fraud liability shifted) to 4.4 basis points in 2017 but then declined to 1.7 basis points in 2021. For dual-message networks (blue line), the counterfeit fraud rate declined from 9.0 basis points in 2015 to 6.6 basis points in 2017, then increased to 9.1 basis points in 2021. While the counterfeit fraud rate for single-message networks has been trending down recently, the rate is still high relative to countries such as Australia and France, where the counterfeit fraud rate of both credit and debit cards was around 0.1 basis points in 2021.[7]

**Chart 2: Counterfeit fraud rates of non-prepaid debit cards**



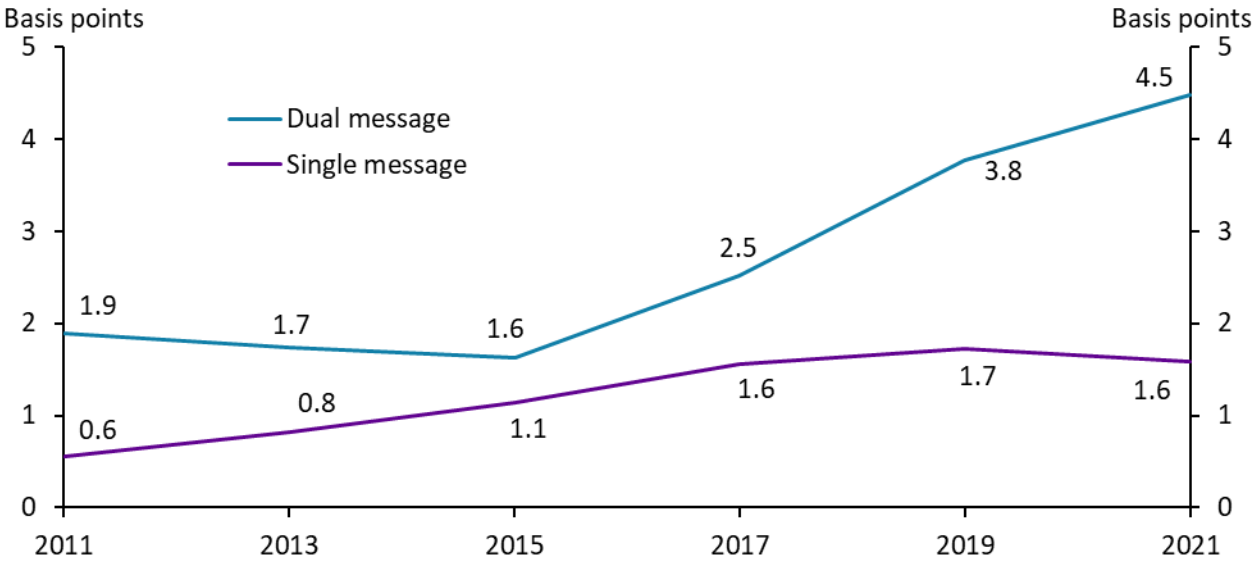

Sources: Board of Governors of the Federal Reserve System and author's calculations.

Card skimming may partially explain the recent increase in the counterfeit fraud rate for dual-message networks. Card skimming occurs when criminals illegally install devices on ATMs, point-of-sale terminals, or fuel pumps' card readers to capture card data and record cardholders' PINs. Criminals use the data to create counterfeit cards with an intentionally damaged chip, then make unauthorized purchases. These cards may be more likely to be used at non-chip terminals, but even when they are presented at chip terminals, transactions may occur as fallback transactions, which read information on the magnetic stripe instead of the chip (U.S. Payment Forum 2016; Visa 2016).[8] FICO data show a significant increase in compromised cards resulting from card skimming in 2022 and 2023 (Cobb 2023, 2024). However, card skimming may have increased earlier than 2022 and contributed to the increase in the counterfeit fraud rate for dual-message networks from 2017 to 2021.

The lost-or-stolen fraud rate of non-prepaid debit cards has increased for both types of networks since EMV migration. Chart 3 shows that for dual-message networks (blue line), the rate has almost tripled

from 1.6 basis points in 2015 to 4.5 basis points in 2021. For single-message networks (purple line), the rate increased slightly from 1.1 basis points in 2015 to 1.6 basis points in 2017 but has been flat since. Although the lost-or-stolen fraud rate is lower for single-message networks than for dual-message networks, it is still higher than in countries such as Australia and France, where the lost-or-stolen fraud rate of both credit and debit cards was less than 1 basis point in 2021.[9]

**Chart 3: Lost-or-stolen fraud rates of non-prepaid debit cards**

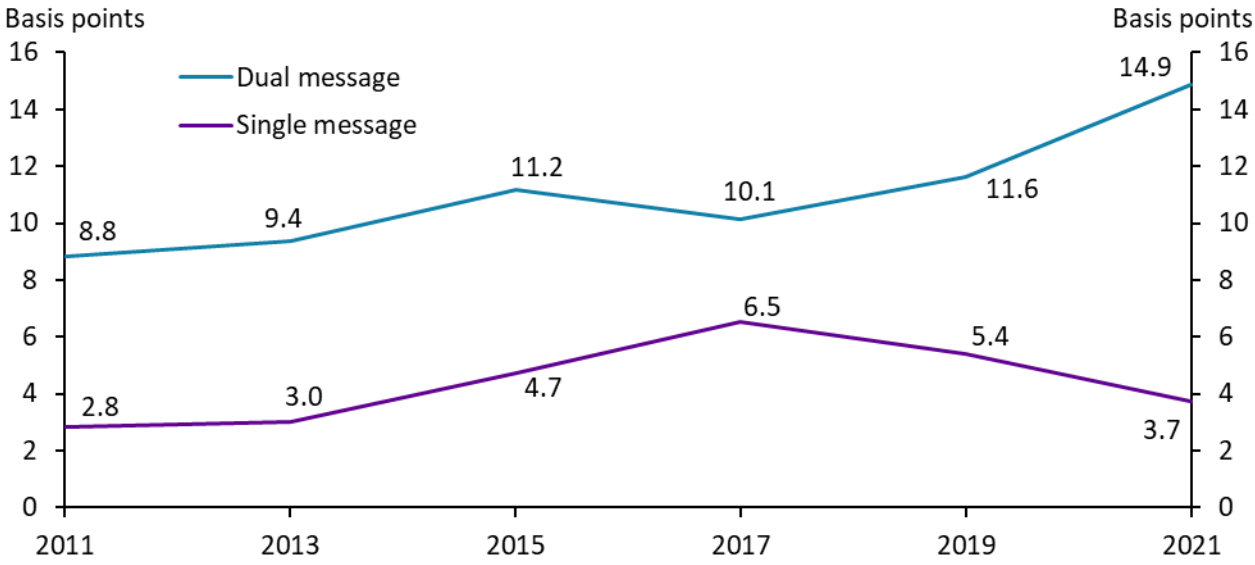



Sources: Board of Governors of the Federal Reserve System and author's calculations.

The higher lost-or-stolen fraud rates in the United States relative to other countries may be explained by the authentication methods used with chip cards. While many other countries adopted chip-and-PIN authentication for both credit and debit cards, dual-message networks (as well as credit card networks) in the United States adopted chip-and-signature authentication at the start of EMV migration and then dropped the signature requirement in 2018. Although single-message networks still use PINs, some networks have started allowing card-present transactions to be "PIN-less" if the amount transacted is below a certain threshold.

Similarly to the counterfeit fraud rate, the overall card-present fraud rate has declined for single-message networks but increased for dual-message networks since EMV migration began. Card-present fraud includes not only counterfeit and lost-or-stolen fraud, but also other types, such as fraud due to identity theft or synthetic identity and payment orders modified by fraudsters.[10] Chart 4 shows that the card-present fraud rate for dual-message networks has increased from 10.1 basis points in 2017 to 14.9 basis points in 2021 due to increases in both counterfeit and lost-or-stolen fraud rates (as shown in Charts 2 and 3). In contrast, the card-present fraud rate for single-message networks has gradually declined from 6.5 basis points in 2017 to 3.7 basis points in 2021, thanks mainly to the decline in the counterfeit fraud rate (shown in Chart 2). Card-present fraud rates of both credit and debit cards in other countries are substantially lower, from slightly above 1 basis point in France in 2021, to less than 1 basis point in Australia in 2021 and the European Economic Area in 2022 and 2023.[11]

**Chart 4: Card-present fraud rates of non-prepaid debit cards**




Sources: Board of Governors of the Federal Reserve System and author's calculations.

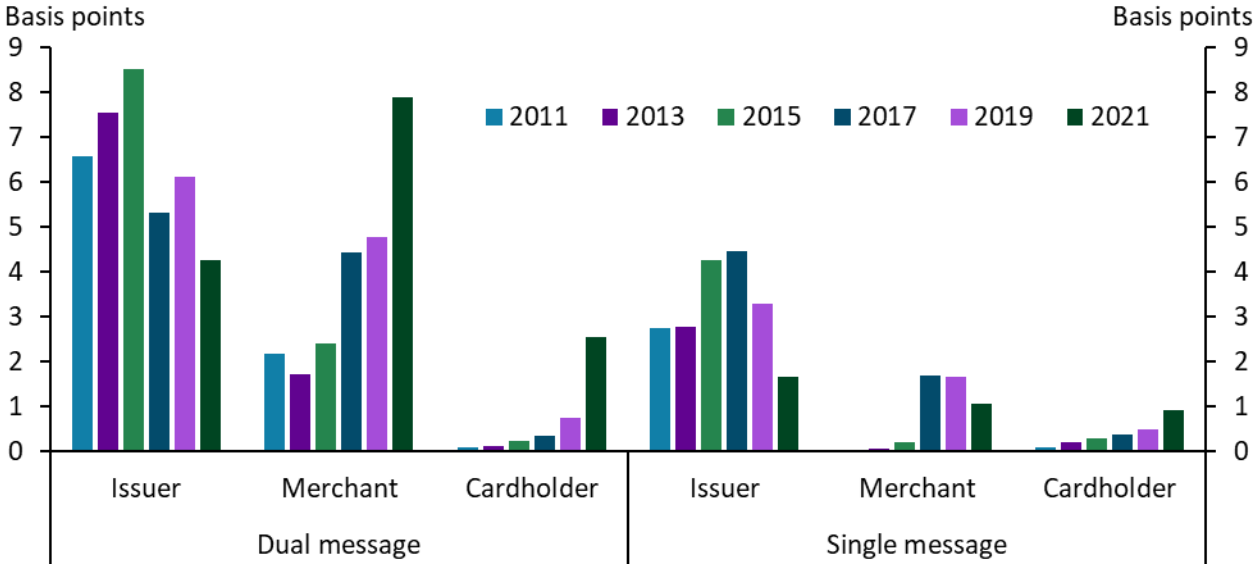
**Card-present fraud loss allocation across issuers, merchants, and cardholders**

Although the EMV liability shift implemented in 2015 changed issuers' and merchants' liability for fraud losses, it did not change cardholders' liability. Regulations and card networks' rules limit consumers' liability for unauthorized fraud as long as they follow proper procedures, such as reporting a lost or stolen card or reporting fraudulent activity on their cards promptly. However, because cardholders can be liable for fraud loss if they do not follow these procedures, I include cardholders along with issuers and merchants in my analysis of fraud loss allocation.

To examine how fraud losses have been reallocated since EMV migration, I calculate each party's fraud loss rates for non-prepaid debit card transactions for both single- and dual-message networks based on data reported in the Federal Reserve Board's biennial reports on debit cards. The sum of the three parties' fraud loss rates should be the same as (or very close to) the card-present fraud rates shown in Chart 4.

The left side of Chart 5 shows historical fraud loss rates from card-present fraud for each of the three parties for dual-message networks. Despite the increase in the card-present fraud rate for dual-message networks, the card-present fraud loss rate for issuers declined from 2015 to 2017 and again from 2019 to 2021 due to the EMV liability shift. The same fraud loss rate for merchants, on the other hand, increased significantly during both of those two periods; moreover, in 2021, merchants' fraud loss rate (7.9 basis points) exceeded issuers' (4.3 basis points). In contrast to fraud loss rates for issuers and merchants, the fraud loss rate for cardholders has been low, though it has increased gradually until 2019 and jumped up to 2.5 basis points in 2021.

**Chart 5: Card-present fraud loss rates of non-prepaid debit cards by party**




Sources: Board of Governors of the Federal Reserve System and author's calculations.

The right side of Chart 5 shows that card-present fraud loss rates for issuers on single-message networks began declining after 2017. Although merchants' fraud loss rate significantly increased immediately after the EMV liability shift in 2015, their fraud loss rate has declined since 2017 along with the card-present fraud rate. As a result, issuers continue to have a higher fraud loss rate than merchants. Cardholders have had the lowest fraud loss rate among the three parties, with a fraud loss rate lower than 1 basis point in 2021; however, their fraud loss rate has been trending up over the past decade.

The increases in cardholders' card-present fraud loss rates on both types of networks are somewhat surprising. No changes were made during the 2011–21 period in consumer protections against fraud losses through regulation or in networks' rules.[12] Potentially, gross negligence by cardholders (such as a delayed notification to their issuers about lost or stolen cards or unauthorized use) may have become more prevalent, or issuers may have tightened requirements for cardholders to receive the full reimbursement of their fraud losses. However, identifying the true causes of this increase in cardholder fraud loss rates requires further investigation.

**Conclusion**

The U.S. migration to EMV chip-card technology was intended to lower card-present fraud, especially counterfeit fraud. Although the card-present fraud rate of non-prepaid debit cards has been trending down for single-message networks since EMV migration, the rate has been trending up for dual-message networks in the United States. The counterfeit fraud rate has not declined for dual-message networks and the lost-or-stolen fraud rate has increased for both types of networks. After the EMV liability shift in 2015, card-present fraud loss rates for both issuers and merchants have declined for single-message networks. Although issuers' fraud loss rate has declined for dual-message networks, merchants' fraud loss rate has increased. And while cardholders' fraud loss rate has been the lowest among the three parties, the rate has been increasing for both types of networks. Understanding why cardholders' card-

present fraud loss rates have increased and why counterfeit, lost-or-stolen, and overall card-present fraud rates have not declined, especially for dual-message networks, will require detailed fraud data and further research.

## Endnotes

[1] For gas stations, the liability shift did not take effect until October 2020.
[2] The exact liability shift varies slightly by card network. See Hayashi, Markiewicz, and Minhas (2018) for more detail.
[3] Card networks dropped the signature requirement for credit and dual-message debit card transactions in April and October 2018.
[4] In these reports, fraud information was provided by debit card issuers subject to Regulation II's interchange fee cap (covered issuers), and more than two-thirds of non-prepaid debit card transactions in value have been made with the covered issuers' cards.
[5] These data show all fraud, card-not-present fraud, counterfeit fraud, and lost-or-stolen fraud separately. I assume all lost-or-stolen fraud occurred in the card-present environment, though some may have occurred in the card-not-present environment.
[6] In the Federal Reserve Board's biennial reports, data on how covered issuers' transactions in value are distributed between card-present and card-not-present transactions are not available. I assume that their distribution for a given type of networks is identical to the industry-wide distribution (including both non-prepaid and prepaid debit card transactions made with both covered and exempt issuers' cards) for that type of network, which is available in the reports.
[7] Author's calculations based on fraud data reported in AusPayNet (2022) and Banque de France (2022) and payment data reported by the Reserve Bank of Australia.
[8] Merchants are liable for counterfeit fraud occurring at non-chip terminals and issuers are generally liable for counterfeit fraud occurring during fallback transactions.
[9] Author's calculations based on fraud data reported in AusPayNet (2022) and Banque de France (2022) and on payment data reported by the Reserve Bank of Australia.
[10] Synthetic identity fraud is defined as a crime in which a perpetrator combines fictious and sometimes real information to create new identities to defraud financial institutions, government agencies, or individuals (Federal Reserve System 2019).
[11] Author's calculations based on fraud data reported in AusPayNet (2022), Banque de France (2022), and European Banking Authority and European Central Bank (2024), and on payment data reported by the Reserve Bank of Australia.
[12] Regulation E, which implements the Electronic Fund Transfer Act, limits a consumer's liability for unauthorized (electronic) transactions at $50 if the consumer notifies their financial institution within two business days of learning of the loss or theft of an access device, or $500 if the consumer fails to do so. A consumer must provide notice to the financial institution within 60 days of receiving a periodic statement on which an unauthorized transaction appears; if the consumer fails to do so, the consumer may have unlimited liability for any unauthorized transactions after that 60-day period.

## References

AusPayNet (Australian Payments Network). 2022. "Australian Payment Fraud 2022: January – December 2021 Data." August 22.
Banque de France. 2022. "Observatoire De La Sécurité Des Moyens De Paiement Rapport Annuel 2021." July 22.
Cobb, Debbie. 2024. "Debit Card Compromises Nearly Doubled in 2023 – FICO Data." FICO Blog, March 6.
———. 2023. "U.S. Card Skimming Grew Nearly 5x in 2022, New FICO Data Shows." FICO Blog, February 16.
EMVCo. 2024. "Worldwide EMV Deployment Statistics." Accessed on January 10, 2025.
European Banking Authority and European Central Bank. 2024. "2024 Report on Payment Fraud." August 1.

Federal Reserve Board (Board of Governors of the Federal Reserve System). 2024. "Networks, Processors, and Issuers Payments Survey (NPIPS) Detailed Data, 2015-2022." November 13.

———. 2023. "2021 Interchange Fee Revenue, Covered Issuer Costs, and Covered Issuer and Merchant Fraud Losses Related to Debit Card Transactions." October.

———. 2018. "Changes in U.S. Payments Fraud from 2012 to 2016: Evidence from the Federal Reserve Payments Study." October.

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

Hayashi, Fumiko. 2019. "Payment Card Fraud Rates in the United States Relative to Other Countries after Migrating to Chip Cards." Federal Reserve Bank of Kansas City, *Economic Review*, vol. 104, no. 4.

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.

Hayashi, Fumiko, Richard J. Sullivan, and Stuart E. Weiner. 2003. *A Guide to the ATM and Debit Card Industry*. Federal Reserve Bank of Kansas City.

U.S. Payment Forum. 2016. "EMV Implementation Guidance: Fallback Transactions." Version 2.0, December.

Visa. 2016. "Mitigating Fraud on Chip Fallback Transactions."

*Fumiko Hayashi is a vice president at the Federal Reserve Bank of Kansas City. The views expressed are those of the author and do not necessarily reflect the positions of the Federal Reserve Bank of Kansas City or the Federal Reserve System.*