Payments System Research Briefing

Remote Card Payment Fraud: Trends and Measures Taken in Australia, France, and the United Kingdom

by: Fumiko Hayashi

November 25, 2020

Australia, France, and the United Kingdom have successfully reduced remote card payment fraud rates in recent years. In each of these countries, a self-regulated body, central bank, or trade association has led coordinated efforts to mitigate remote fraud.

Consumers have been shifting from in-person (card-present) payments to remote (card-not-present) payments for the last several years. This trend has reportedly accelerated during the COVID-19 pandemic, with implications for fraud, as remote payments are more prone to fraud than in-person payments. In this briefing, I examine remote fraud rates in Australia, France, and the United Kingdom—three countries that report data on payment fraud at least once a year. All three countries saw fraud increase with remote payment card use. However, all three also took measures to mitigate remote fraud and have successfully reduced their remote fraud rates in recent years. The experiences of these three countries may contain lessons for the United States, which has been slower to implement fraud mitigation measures.

Trending Up: The Share of Remote Card Payments

Over the last several years, the share of remote payments among all card payments has been trending up in Australia, France, and the United Kingdom. From 2015 to 2019, the share of remote card payments in terms of transaction value increased by 12 percentage points in Australia (from 18 percent to 30 percent), 6 percentage points in France (from 13 percent to 19 percent), and 6 percentage points in the United Kingdom (from 31 percent to 37 percent).[1]

Although it is not yet clear how much the share of remote card payments has increased during the COVID-19 pandemic, the accelerating shift to e-commerce has been widely reported. The Australian Payments Network (AusPayNet) reports that the industry "remains vigilant as e-commerce volumes increase during the COVID-19 pandemic" (AusPayNet 2020, p. 4). The Banque de France (2020) reports that while the number of in-person card payments fell significantly during the quarantine period (March–May 2020) relative to the same period in 2019, the number of e-commerce card payments remained close to its 2019 number. And the British Retail Consortium (2020) describes the pandemic as "accelerating a digital shift in 2020 with

record numbers of people now shopping online."

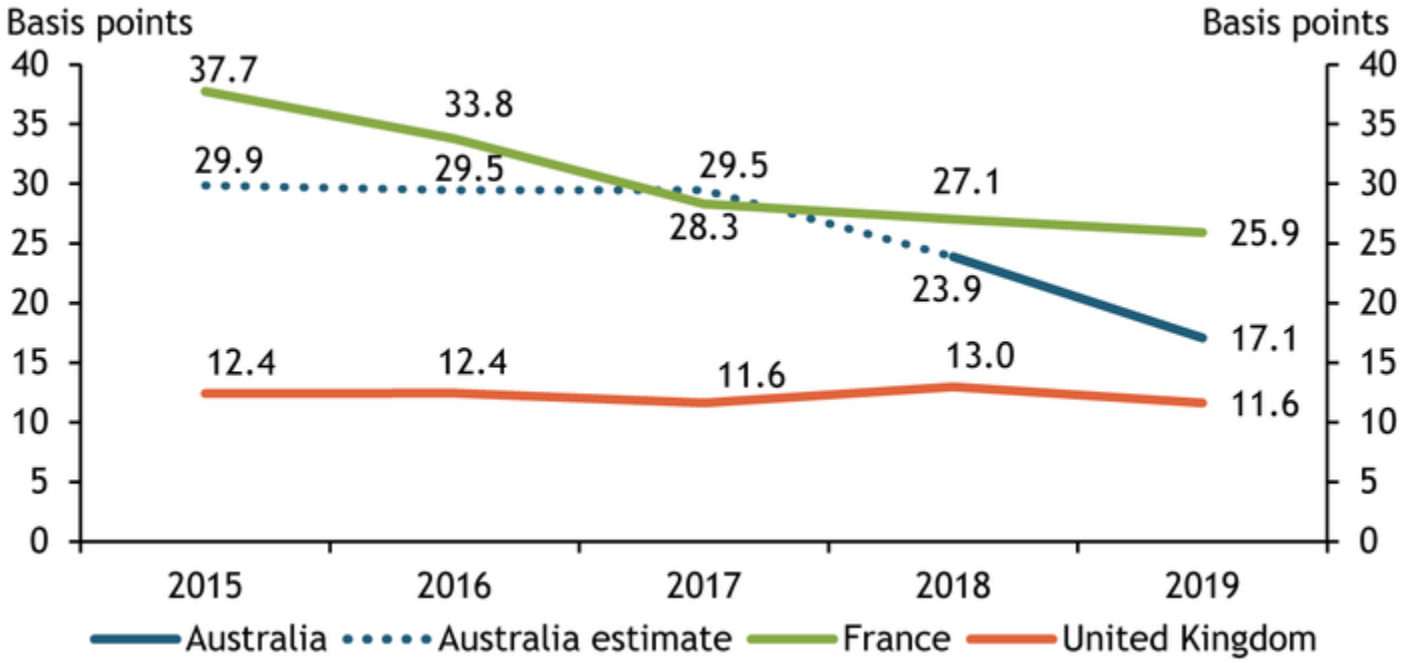
Trending Down: Remote Fraud Rates

Typically, remote fraud rates are much higher than in-person fraud rates. In 2019 in Australia, France, and the United Kingdom, the remote fraud rate was higher than the in-person fraud rate by at least 9 basis points. For transactions on domestically issued cards at both domestic and foreign merchants, the remote fraud rate was 16.1 basis points higher than the in-person fraud rate in Australia and 24.5 basis points higher in France (Banque de France 2020).[2] In the United Kingdom, the remote fraud rate on domestically issued cards was 11.6 basis points, while the in-person fraud rate on domestically issued contactless cards was 2.5 basis points (UK Finance 2020).

However, Australia, France, and the United Kingdom have successfully reduced or contained their remote fraud rates in the last several years. In each of these countries, the remote fraud rate has declined enough to reduce the country's overall payment card fraud rate even though the share of more fraud-prone remote card payments has increased.[3]

Remote fraud rates on domestically issued cards used at both domestic and foreign merchants have declined significantly in Australia and France, as shown in Chart 1. In Australia, the remote fraud rate declined by about 7 basis points in one year, from 23.9 basis points in 2018 to 17.1 basis points in 2019 (blue line).[4] In France, the decline in the remote fraud rate has been more gradual but persistent. The rate declined by about 4 basis points each year from 2015 to 2017 and by about 2 basis points each year from 2017 to 2019 (green line). In contrast, the remote fraud rate has hardly changed in the United Kingdom, which maintains the lowest rate among the three countries: the remote fraud rate has been steady around 12 basis points over the last five years (orange line).

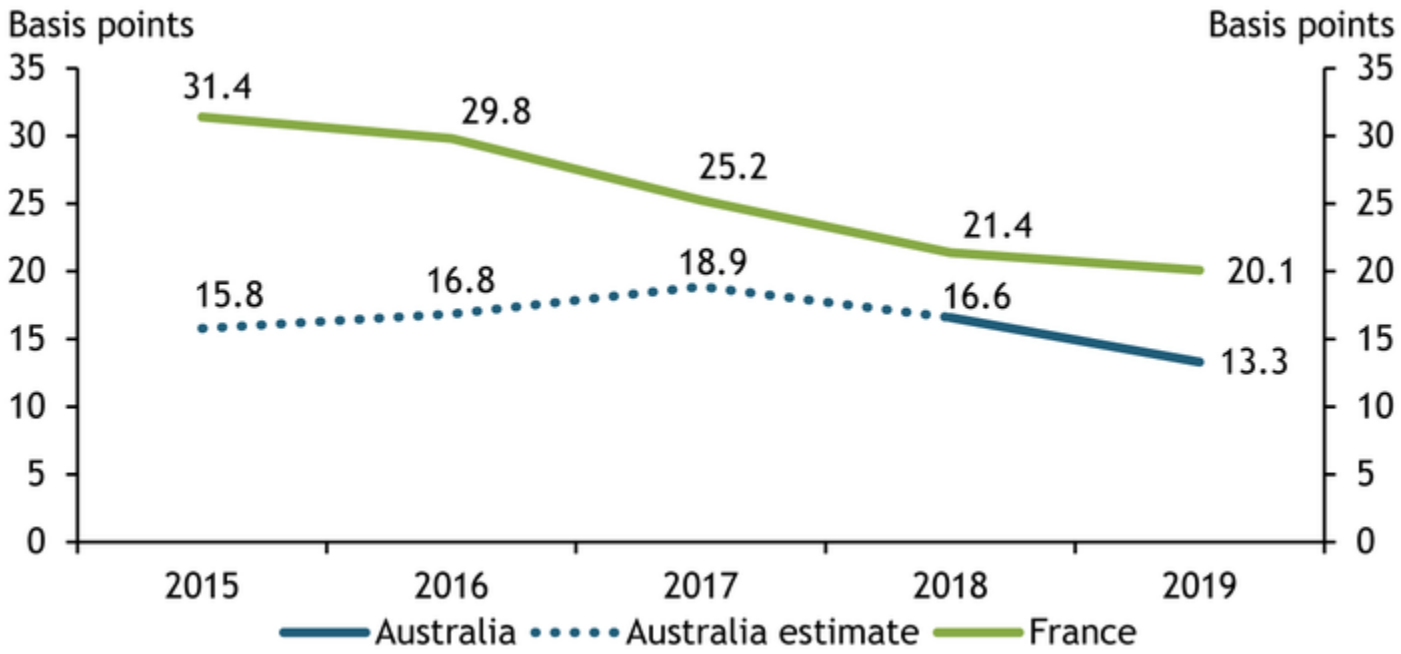
Chart 1: Trends in Remote Fraud Rates on Domestically Issued Cards



Note: Dotted blue line shows author's estimates due to a lack of detailed transaction data for Australia before 2018.Sources: AusPayNet, Reserve Bank of Australia, Banque de France, Financial Fraud Action UK, UK Finance, and author's calculations.

Remote fraud rates at domestic merchants on both domestic and foreign-issued cards has also declined. This rate is of special interest to merchants and their acquirers (entities that perform a variety of merchant-related functions in the payment card industry), because merchants can be financially liable for this type of fraud. While the remote fraud rate at domestic merchants is not available in the United Kingdom, Chart 2 shows that this rate has declined in both Australia and France.[5] In Australia, the rate peaked in 2017 at 18.9 basis points and has since declined to 13.3 basis points in 2019 (dotted and solid blue line). In France, the rate declined steadily every year, from 31.4 basis points in 2015 to 20.1 basis points in 2019 (green line).

Chart 2: Trends in Remote Fraud Rates at Domestic Merchants



Note: Dotted blue line shows author's estimates due to a lack of detailed transaction data for Australia before 2018.Sources: AusPayNet, Reserve Bank of Australia, Banque de France, and author's calculations.

Measures Taken to Reduce Remote Payment Card Fraud

In Australia, the significant drop in the remote fraud rate from 2018 to 2019 is likely due to increased awareness of fraud and the implementation of the Card-Not-Present (CNP) Fraud Mitigation Framework. In 2018, the Reserve Bank of Australia (RBA), which has explicit payment regulation power, encouraged industry participants to implement a coordinated strategy to mitigate CNP fraud. After consulting with various industry participants and RBA, AusPayNet, a self-regulated body in the payment industry, launched the Framework in July 2019. The Framework is a whole-of-industry approach to mitigating online CNP fraud by encouraging the adoption of secure technologies, including real-time monitoring, machine learning, tokenization, and strong customer authentication (SCA).[6] The Framework sets fraud thresholds for mandating SCA across online CNP transactions to those issuers and merchants who exceed the thresholds consistently.[7] AusPayNet monitors online CNP fraud through reporting by card issuers and merchant acquirers and ensures compliance with the Framework through its rules and codes. Among merchants who had exceeded the fraud threshold, two-thirds of them quickly reduced their fraud below the threshold and the remaining third have been working closely with acquirers to reduce their fraud. AusPayNet expects the full benefit of the Framework to be realized in the coming years (AusPayNet 2020).

In France, the adoption of 3D Secure contributed to the decline in remote fraud rates in recent years. 3D Secure is a messaging protocol that strengthens the authorization of online transactions using digital certificates and passwords to authenticate both customer and payment method credentials. After migrating to EMV chip card technology in the early to mid-2000s, France

experienced an initial increase in remote card payment fraud. Consequently, the Banque de France led a nationwide adoption of 3D Secure (Stervinou 2015). The Observatory for the Security of Payments—chaired by the Governor of the Banque de France—revealed the growing problem of online payment fraud, educated industry participants about the value of 3D Secure for enhancing authentication, and engaged issuers and merchants in a working group to find ways to reduce cart abandonment among consumers.[8] Adoption of 3D Secure has grown since the late 2000s; by 2019, 98 percent of cardholders and 75 percent of e-merchants were enrolled in the 3D Secure system (Banque de France 2019). France is currently migrating to SCA under the European Union's Revised Payment Services Directive (PSD2) for e-commerce card payments, and the Observatory has been coordinating migration plans. Their migration plans were slightly delayed by the COVID-19 crisis, and high-level compliance is now expected in the first quarter of 2021.

Similar to France, adoption of 3D Secure in the United Kingdom started in the late 2000s, and by 2013, nearly 70 percent of e-merchants were using 3D Secure to combat online payment fraud (British Retail Consortium 2014). As in France, online payment fraud grew in the United Kingdom after EMV chip card migration had been completed around the mid-2000s. However, in the United Kingdom, the concerted efforts of issuers, networks, merchants, and their acquirers drove the adoption of 3D Secure instead of a central bank. Merchant acquirers provided merchants incentives to adopt 3D Secure and promote cardholder enrollment. Issuers and networks enabled merchants to choose authentication methods based on fraud risks and simplified the transaction process to reduce cart abandonment (Hayashi, Moore, and Sullivan 2015). Like France, the United Kingdom is currently migrating to SCA, and UK Finance, a trade association for the UK banking and financial service sector, has been coordinating migration plans with its members and the British Retail Consortium, a trade association for merchants. Enforcement actions will be taken by the Financial Conduct Authority for any firms that fail to comply with SCA requirements after September 14, 2021. Another noteworthy anti-fraud measure taken in the United Kingdom is the financial industry's sponsorship of a special police unit, the Dedicated Card and Payment Crime Unit (DCPCU), which targets organized criminal groups responsible for card fraud. The DCPCU has taken down 1,600 social media accounts linked to fraudulent activities such as trading stolen card details online and recruiting people as money mules (UK Finance 2020).

Potential Lessons for the United States

While comparable data on payment card fraud are not yet available for the United States, remote card payments are also trending up, increasing concerns about payment card fraud. The share of remote card payments among all card payments was higher in the United States than in Australia, France, and the United Kingdom from 2015 to 2018.[9] In 2016, the year with the most recent comprehensive fraud data available in the United States, the remote fraud rate was 9 basis points higher than the in-person fraud rate (18.7 basis points versus 9.3 basis points) (Board of Governors of the Federal Reserve System 2018). As in other countries, the onset of the pandemic boosted remote payments. In May, PAYMENTS.com reported, "In just eight short weeks, we have observed six times more consumers working from home, four times more consumers buying groceries online instead of going into the grocery store, four times more consumers ordering takeout from aggregators or their favorite restaurants, and three times more consumers shopping online for things other than groceries" (Webster 2020).

Experiences in Australia, France, and the United Kingdom suggest that the strong leadership roles taken by AusPayNet, Banque de France, and UK Finance were key to successfully reducing remote card payment fraud rates. These institutions advanced industry-wide initiatives by coordinating among various stakeholders, including banks, card networks, other payment service providers, merchants, and consumers. In addition, these institutions either enforced, or worked closely with supervisory entities that enforced, security measures such as SCA. Furthermore, these institutions are armed with timely fraud statistics and other data to assess the progress of their efforts and find effective ways to mitigate payment fraud.

Relative to other countries, the United States has been slow to implement fraud mitigation measures.[10] The United States does not have government regulation or industry self-regulation requiring SCA. Instead, industry efforts to promote fraud mitigation measures and best practices are currently underway. For example, the U.S. Payments Forum, a cross-industry body focused on addressing issues that require broad cooperation and coordination across many constituents in the payments industry, is promoting best practices for mitigating remote card payment fraud. Card networks are also promoting 3D Secure Version 2 by shifting the liability of remote card fraud from merchants to issuers. Whether these efforts can lead to mass adoption of fraud mitigation measures and reduce remote fraud rates remains to be seen.

The COVID-19 pandemic has generated new challenges to mitigating fraud. Many merchants who had not previously used remote channels such as online and mobile applications now use those channels to interact with their customers and take payments. Merchants who are new to remote channels may be vulnerable to fraud and data breaches until they learn and adopt best practices for mitigating those risks. In addition, some consumers who were not frequent users of remote channels before the pandemic may also be vulnerable to fraud or scams.

Payment fraud might have increased since the pandemic not just because payments have shifted to remote channels but also because fraudsters may have exploited these new vulnerabilities. Having timely fraud statistics allows institutions to identify

such vulnerabilities quickly. Coordinated efforts such as those led by institutions in Australia, France, and the United Kingdom may be more effective than solely depending on individual acquirers or issuers to educate merchants or consumers.

Endnotes

[1] These calculations are based on data from the Reserve Bank of Australia, Banque de France (2020), and UK Finance (2020). Card payments include cash withdrawals at ATMs.

[2] The fraud rates in Australia are the author's calculations based on data from AusPayNet (2020) and the Reserve Bank of Australia.

[3] From 2015 to 2019, the overall fraud rate for transactions with domestically issued cards declined from 6.7 basis points to 5.7 basis points in Australia, from 7.4 basis points to 6.4 basis points in France, and from 8.4 basis points to 7.5 basis points in the United Kingdom (AusPayNet 2020; Banque de France 2020; UK Finance 2020).

[4] I assume that the distribution of in-person and remote transactions on domestically issued cards is the same as at domestic and foreign merchants.

[5] In Australia and France, remote fraud rates for domestic payments and two types of cross-border payments have declined recently. Domestic payments are those made with domestically issued cards at domestic merchants. The two types of cross-border payments are those made with domestically issued cards at foreign merchants and those made with foreign-issued cards at domestic merchants. Cross-border CNP payments are significantly more fraud-prone than domestic CNP payments.

[6] Cross-border online CNP payments are out of the Framework's scope. SCA requires at least two of the following three elements: something the customer knows (such as a password), something the customer possesses (such as a smartphone), and something inherent to the customer (such as a fingerprint).

[7] The thresholds are currently set at a fraud rate of 15 basis points for issuers and 20 basis points with a fraud value of $50,000 per quarter for merchants.

[8] Cart abandonment occurs when online shoppers add products to their virtual shopping cart or start the checkout process, but leave the e-commerce sites before completing their purchases. Cart abandonment can be caused by authentication methods that make the checkout process longer or cumbersome.

[9] This calculation is based on data from the Board of Governors of the Federal Reserve System in 2019 and October 2020.

[10] Hayashi (2019) discusses several challenges to mitigating fraud in the United States.

Author

Fumiko Hayashi

Senior Policy Advisor

Fumiko Hayashi is a Senior Policy Advisor specializing in payments in the Economic Research Department at the Federal Reserve Bank of Kansas City. Since joining the Federal Reserve in 2001, Ms. Hayashi published studies on the ATM and debit card industry, regulatory developments around interchange fees and card network rules, consumer payment choice, various types of payment methods (including credit, debit, and prepaid cards, mobile and QR code-based payments, instant payments, and central bank digital currency), payment fraud and security, nonbanks and fintechs in the payment system. She is currently conducting research on undeserved consumers in payments, fraud and scams involving instant payments, role of intermediaries in the payment system modernization, among others.Prior to joining the Federal Reserve Bank of Kansas City, Ms. Hayashi conducted research examining consumer savings and long-tern care insurance, social security reform in Japan, and nursing home markets in the United States. She holds a B.A. and a M.A. in economics from Hitotsubashi University, and a Ph.D. in economics from the University of Minnesota.