No. 22-0024

IN THE SUPREME COURT OF TEXAS

SALLY BEAUTY HOLDINGS, INC.,

Petitioner,

v.

VISA INC.,

Respondent.

On Appeal from the Second Court of Appeals
Fort Worth, Texas; No. 02-20-00339

BRIEF OF AMICUS CURIAE THE RETAIL LITIGATION CENTER, INC. IN SUPPORT OF SALLY BEAUTY HOLDINGS, INC.'S PETITION FOR REVIEW

Patrice Pujol
Texas State Bar No. 00794488
FORMAN WATKINS & KRUTZ, LLP
4900 Woodway Drive, Suite 940
Houston, Texas 77057
Telephone: 713-402-1717
Facsimile: 713-621-6746
Patrice.Pujol@formanwatkins.com

Spencer M. Ritchie
Admitted Pro Hac
FORMAN WATKINS & KRUTZ, LLP
210 East Capitol Street, Suite 2200
Jackson, Mississippi 39201
Telephone: 601-960-3172
Facsimile: 601-960-8613
Spencer.Ritchie@formanwatkins.com

Counsel for Amicus Curiae
The Retail Litigation Center, Inc.

IDENTITY OF PARTIES AND COUNSEL

Counsel for the Retail Litigation Center, Inc. identify *amicus curiae* and its counsel as follows:

The Amicus Curiae Submitting this Brief is:

Retail Litigation Center, Inc.

Rule 11(c) Statement:

No person or entity other than *amicus curiae* and its members contributed money to fund this brief's preparation and submission.

Amicus Curiae Submitting this Brief is Represented by:

Patrice Pujol
Texas State Bar No. 00794488
FORMAN WATKINS & KRUTZ, LLP
4900 Woodway Drive, Suite 940
Houston, Texas 77057
Telephone: 713-402-1717
Facsimile: 713-621-6746
Patrice.Pujol@formanwatkins.com

Spencer M. Ritchie
Admitted Pro Hac
FORMAN WATKINS & KRUTZ, LLP
210 East Capitol Street, Suite 2200
Jackson, Mississippi 39201
Telephone: 601-960-3172
Facsimile: 601-960-8613
Spencer.Ritchie@formanwatkins.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Regulations

Other Authorities

STATEMENT OF INTEREST

The Retail Litigation Center, Inc. ("RLC") is a public policy organization representing national and regional retailers in the United States. Its members include many of the country's largest retailers—including prominent Texas-based companies such as 7-Eleven and Michaels—employing millions of people throughout the United States and accounting for hundreds of billions of dollars in annual sales. The RLC identifies and engages in legal proceedings that have a national impact on the retail industry. It seeks to provide courts with retail-industry perspectives on important legal issues. This is such a case.

Retail is the nation's largest private sector employer driving the economy and supporting 52 million jobs in communities across the country. In Texas alone, retail employs more than 2.8 million people and supports 30 percent of jobs in the state. Texas is home to nearly 400,000 retail establishments that provide an annual direct impact on the state's GDP of more than $140 billion.

Many are surprised to learn that credit card fees represent an extraordinary cost to retailers. Often exceeded only by the cost of labor and sometimes real estate, credit card interchange fees can be a retailer's second or third highest operating expense. Every retailer that accepts credit cards for the convenience of their customers incurs enormous interchange fees, including every retailer in Texas. On

top of these already outsized fees, credit cards seek to impose even more fines and penalties whenever a retailer is the victim of a criminal computer network intrusion.

In this regard, Respondent Visa, through its unlawful Global Compromised Account Recovery ("GCAR") penalty program, has facilitated a windfall of fees and arbitrary payments that are ultimately extracted from retailers suffering data breaches by exploiting the insecure "magnetic stripe" payment card environment that Visa itself fostered. The district court's holding that the GCAR program is an unenforceable penalty—rather than a permissible liquidated damages provision—was correct as a matter of law and public policy. Accordingly, the RLC respectfully urges this Court to grant Sally Beauty Holdings, Inc.'s ("Sally Beauty") Petition for Review of the court of appeals' incorrect reversal of the district court.

I. SUMMARY OF ARGUMENT

Visa's use of the GCAR program and its arbitrary approach to imposing penalties in the aftermath of a data breach is an abusive practice reeking of bad faith given Visa's role in creating the environment in which breaches, such as those suffered by Sally Beauty, occurred. Indeed, if Visa had chosen to introduce chip-and-PIN technology into the United States—as it had in nearly every other part of the world—retailers and consumers would not have been as vulnerable. The sole reason for Visa's delay was that it profited more from the continued use of the old, insecure magnetic-stripe card in the United States.

Adding insult to injury is the double-dipping that the GCAR program represents. Retailers already pay substantial "interchange fees" every time a customer swipes a payment (credit or debit) card. These interchange fees compensate banks that issue Visa cards—in advance—for costs like security expenses and fraud losses. Thus, there are strong legal and public policy reasons for applying California law to strike down the GCAR program as unlawful and prevent continuing harm to retailers across the country and in Texas.

Respectfully, this Court should grant the Petition for Review filed by Sally Beauty to reverse the decision of the court of appeals and reinstate the district court's holding that the Visa GCAR program is an unenforceable penalty under California law.

II. STATEMENT OF FACTS

RLC incorporates by reference the Statement of Facts set forth in Sally Beauty's Petition for Review.

III. ARGUMENT

A. Visa levies assessments under GCAR in bad faith.

The payment card device used by consumers has undergone multiple incarnations, but the technology at issue in the instant case is the magnetic-stripe ("magstripe") card. The magstripe payment card is an old technology, conceived by

IBM and adopted as a U.S. standard in 1969.[1] By the 1990's, this ubiquitous piece of plastic was notoriously insecure and fraud prone, as its encoded information could be easily copied.

The inherent insecurity of the magstripe led to larger and larger data breaches as criminals targeted payment processors, banks, and merchants to harvest payment card account numbers that could be readily monetized through easy-to-make counterfeit cards. Faced with rising fraud and emerging digital technologies to combat it, the payment networks Europay, Mastercard, and Visa collaborated (through their joint venture EMVCo) to implement standards using integrated-circuit-based chip cards that used cryptography to produce a secure form of authentication that could not be copied by fraudsters and would offer greater functionality than static magnetic stripes. As Mastercard's President of North America put it, whereas magstripe is like "8-track tape . . . [c]hip technology is really an iPod."[2]

Visa and Mastercard announced a (mostly) global migration to chip cards in 1999. EMV-chip cards and EMV-capable terminals were implemented around the world—except in the United States, even though the U.S. was the card networks'

[1] IBM, *Magnetic Stripe Technology*, https://www.ibm.com/ibm/history/ibm100/us/en/icons/magnetic/.

[2] S&P Capital IQ, McGraw Hill Financial, *Mastercard Incorporated Shareholder/Analyst Call* (Sept. 20, 2012) at 24.

largest market. In countries outside of the United States, Visa provided direct financial incentives for the conversion to chip through terminal subsidies or interchange incentive rates and configured the migration period to coincide with merchants' ordinary terminal replacement cycles—none of which Visa (or Mastercard) provided to U.S. merchants.[3] But why?

A key reason for this delayed rollout is that the operation of the magstripe data processing environment was (and is) highly profitable in the United States—both to Visa and Mastercard and to financial institutions issuing their cards—because they can charge higher network and interchange fees; in contrast, more secure chip-and-PIN transactions often came with lower network and interchange fees.[4] To wit, card

[3] Visa Management Committee, *Infrastructure Migration Strategy & Business Case* (Jan. 18-19, 1999) (recommending global transition to EMV with financial incentives and noting that "magnetic stripe technology is inadequate for combating skimmed counterfeit and that chip with a secure authentication method is the most viable solution"), https://www.justice.gov/sites/default/files/atr/legacy/2006/11/03/p-0543.pdf; Louise West, *Europe: Visa Speeds Up Move to Chip in Europe*, Credit Card Collections (May 25, 2001) (discussing Visa Europe's €168 million merchant incentive fund), http://www.creditcollectionsworld.com/news/052501_6.htm; Robert McKinley, *Smart Card Funding*, CardFlash (Nov. 27, 2001) ("Visa International Asia Pacific announced new policies and a US$25 million regional investment to accelerate the migration from today's magnetic stripe payment cards to EMV-standard smart cards. . . ."), https://cardflash.com/news/2001/11/smart-card-funding/; Adam J. Levitin, *Private Disordering: Payment Card Fraud Liability Rules*, Georgetown Business, Economics and Regulatory Law Research Paper No. 11-06 (2011) at 27 & n.122 ("Some card networks have also encouraged this shift by imposing an 'incentive interchange rate'—interchange penalties and rewards."), https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1612&context=facpub.

[4] *See* Fumiko Hayashi and Jesse Leigh Maniff, *Public Authority Involvement in Payment Card Markets: Various Countries (August 2020 Update)*, Federal Reserve Bank of Kansas

issuers (like banks) are allowed by Visa (and MasterCard) to siphon off and keep significant interchange (or "swipe fees") from amounts consumers pay to merchants for both credit and debit card transactions. These fees reportedly amounted to over $110 billion nationally in 2020 and are in addition to the billions in finance charges and other fees these issuers charge to their cardholders (not to mention the additional fees with which merchants may get saddled under penalty programs such as GCAR).[5]

EMVCo's statistics tell the tale. As of September 1, 2010, nearly 85 percent of merchant terminals and 65 percent of cards issued in Western Europe had been converted to chip technology, along with 55 percent of terminals and 26 percent of cards in the Western Hemisphere, *but 0.0 percent in the United States*. As EMVCo's

City, at 2-13 (outlining regulated interchange rates in markets all over the world), 15 (listing "Zero interchange fee" debit markets in Asia, Europe, and Canada), https://www.kansascityfed.org/documents/6660/PublicAuthorityInvolvementPaymentCardMarkets_VariousCountries_August2020Update.pdf; FINEXTRA, *Card firms trampling all over US interchange reforms* (Mar. 3, 2021) ("Credit card interchange . . . currently averages 2.25 percent with no cap, making up 80 percent of total U.S. card processing fees. . . . The U.S. rate is already the highest among countries covered by the report . . . . Most other nations have rates below 2 percent for credit and some charge no interchange for debit."), https://www.finextra.com/pressarticle/86435/card-firms-trampling-all-over-us-interchange-reforms.

[5] Nilson Report, Issue No. 1201 (July 2021); Jennifer Surane & David McLaughlin, *Visa's Incentives to Banks Examined by Justice Department*, Bloomberg Business (Apr. 8, 2021), https://www.bloomberg.com/news/articles/2021-04-08/visa-s-incentives-to-banks-examined-in-justice-department-probe.

press release put it: "The United States of America is excluded from the figures as there are currently no EMV programmes deployed."[6]

Predictably, as the adoption of chip cards elsewhere in the world drastically reduced counterfeit fraud, global criminal elements focused their attacks on the United States. Again, in the words of Mastercard's president, the United States attracted "fraud coming from other countries into the U.S. because we're the only island that has old magstripe technology," while the secure EMV-chip environment reduced incentives and opportunities for card data compromise elsewhere in the world.[7] Nonetheless, EMV-chip technology worked when it finally arrived in the

---

[6] EMVCO, *Increasing EMV Card and Terminal Deployments Confirm EMV as Global Payments Standard* (Oct. 6, 2010), https://www.emvco.com/media-centre/press-releases/.

[7] *See* S&P Capital IQ, *supra*, note 3; Patricia Moloney Figliola, Cong. Research Serv., R43925, *The EMV Chip Card Transition: Background, Status, and Issues for Congress* (May 17, 2016), at 9 (discussing the "phenomenon referred to as 'fraud migration,' with the fraud migrating primarily to the United States, the last major market to transition to chip cards."), https://fas.org/sgp/crs/misc/R43925.pdf; Richard J. Sullivan, *The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options*, Federal Reserve Bank of Kansas City, Economic Review 101, 115 (2d Qtr. 2010) ("In countries that adopt chip-and-PIN cards, experience shows that fraud will migrate to payment types with relatively weak security. . . . Much of this growth has been on transactions in the United States, where magnetic stripes are still used on payment cards."), https://www.kansascityfed.org/documents/1388/The_Changing_Nature_of_U.S._Card_Payment_Fraud_Industry_and_Public_Policy_Options_3EBF.pdf. *See also* Jesse D. Gossett, *Target, Negligence, Chips, and Chickens*, 49 U.S.F.L. REV. F. 1 (Sept. 26, 2014), at 2-3 ("What all of these frauds have in common is they take advantage of a serious flaw in the credit card payment processing system in the United States. Namely, our credit card system relies on forty-year-old magstripe technology. . . . However, an alternative to magstripes called EMV chip-and-PIN has existed for well over a decade. . . This technology is also widely used in Europe, Canada, and Australia, and has dramatically reduced domestic FTF [face-to-face] fraud by significant percentages in these regions as well. In fact, the United States is the only developed country that has not embraced this

United States. In May 2019, Visa reported that, "For merchants who have completed the chip upgrade, counterfeit fraud dollars dropped by 76 percent in December 2018 compared to September 2015."[8]

Against this backdrop of chip card adoption outside of the U.S. in the first decade of the century, the concurrent amount of counterfeit magstripe fraud increased in the United States. In response, Visa chose not to implement chip cards in the United States—which indisputably would have reduced fraud—but instead chose to establish GCAR's predecessor, the Account Data Compromise Recovery ("ADCR") program in the United States in 2006—a program purportedly designed to shift the cost burden for fraud and data breaches from issuers to merchants. In 2012, Visa consolidated the ADCR program into GCAR, which changed the name, but continued to place the economic burden on retailers for the fraud that was occurring with the insecure magstripe payment cards that Visa and MasterCard refused to replace.

---

technology. This makes the United States the last great target for international fraudsters, which is why this is increasingly becoming a unique problem for U.S. citizens.), at 6 ("The credit card industry has had knowledge of the superiority of chip-and-PIN technology over magstripes for several years but has chosen not to implement it. The industry made a calculated decision to prefer their profits to the risk of subjecting their customers to credit card fraud and identity theft.").

[8] Visa Blog, *Chip technology helps reduce counterfeit fraud by 76 percent* (May 28, 2019), https://usa.visa.com/visa-everywhere/blog/bdp/2019/05/28/chip-technology-helps-1559068467332.html.

Thus, rather than address the problem at its source by introducing proven chip technology to the United States, as it had everywhere else, Visa chose to exploit the insecure card payment environment that Visa itself had fostered and shift the costs of the increased fraud burden to merchants.

B. Visa uses GCAR to facilitate an unlawful windfall for fraud losses on the backs of merchants and does so in an arbitrary manner.

Visa allows the intermediary banks and other entities that issue credit cards to deduct interchange fees (sometimes referred to as "swipe fees") from the amounts consumers send to merchants to pay for the purchases that consumers make with both credit and debit cards. These exorbitant fees are justified as necessary in order to compensate card issuers for operating their payment card programs, including their security expenses and potential fraud losses.[9]

Interchange fees that are extracted from the money owed to merchants are extraordinarily high. In 2020 alone, these fees amounted to just over $110 billion.[10]

---

[9] *See, e.g.*, Gov't Accountability Off., *Credit Cards: Rising Interchange Fees Have Increased Costs for Merchants, but Options for Reducing Fees Pose Challenges*, at 21 (2009) (interchange fees used to cover issuer costs, including fraud losses), https://www.gao.gov/products/gao-10-45. For debit cards, a portion of the interchange fees merchants pay to issuing banks is expressly designed to cover issuer fraud losses. Following the passage of the 2010 Dodd-Frank Act, the Federal Reserve allowed larger debit card issuers, including large credit unions, to receive 5 basis points as a fraud recovery surcharge plus a 1-cent fraud prevention fee on every debit card transaction, including the cost of measures taken in response to networks' notification of card compromises. *See* 76 Fed. Reg. 43,394, 43,422 (July 20, 2011); 77 Fed. Reg. 46,258, 42,263 (Aug. 3, 2012).

[10] Nilson Report, Issue No. 1201 (July 2021).

To take one example, Bank of America received $4 billion in ***net*** income just from interchange fees paid by merchants in 2020.[11] At more than 2 percent of the value of *every* credit card transaction, these fees are more than enough to cover security expenses and fraud losses incurred by card issuers. Visa's use of GCAR to assess fines *on top* of the substantial interchange fees paid by merchants represents an appalling double penalty on merchants victimized by data breaches.

Interchange fees are a substantial burden borne by all merchants that accept credit and debit cards for the convenience of their consumers, including thousands of Texas retailers. Interchange fees are particularly burdensome for small businesses, who often have narrow profit margins. And, as with other costs, these expenses are ultimately passed on to consumers in Texas and across the country. And yet, not only does Visa use GCAR to pay a windfall to issuing banks, Visa's GCAR program does so in an arbitrary manner unconnected to specific instances of consumer harm. In this way, GCAR cannot possibly meet the required legal standard of representing a reasonable endeavor to determine a damages' sum that bears a reasonable relationship to the range of actual damages that the parties could have anticipated would have flowed from the breach.

[11] Bank of America Annual Report 133 (2020), https://investor.bankofamerica.com/annual-reports-and-proxy-statements.

Specifically, under the Fraud Recovery portion of the GCAR program[12], issuing banks report instances of fraud on their cardholders' accounts to Visa, resulting in a stream of reported fraud losses involving both credit and debit cards. 2015 GCAR User Guide at 16-17. Then, when a data breach is determined to have occurred at a merchant or other downstream entity, Visa establishes a temporal "fraud window" in the ongoing stream of fraud losses. *Id.* at 9. GCAR algorithms then associate fraud that is reported within the window with cards that have been reported as having been at risk in the data breach. *Id.* at 20-27. Under this process, there is no pretense that the fraud was caused by the breach; only that a fraud event occurred on an at-risk card during the Visa-calculated fraud window. If there are multiple breaches that have exposed a card, the loss is assigned only to the first breach, even if the actual fraud was caused by criminals stealing card information from a subsequent breach. It may even be the case that card data that was "at risk" from an unreported breach or that card data that was at risk was never actually used by the criminals at all.

Moreover, as for the Operating Expense portion of the GCAR program, Visa does not rely on any reporting or information from issuers about their actual expenses at all. Instead, Visa calculates operating expense recovery for an issuer by

[12] At the times relevant to this case, GCAR had two component programs: (1) the Fraud Recovery program; and (2) the Operating Expense Recovery program.

multiplying the number of the issuer's "at risk" accounts by a fixed per card amount. *Id.* at 27. An issuer thus receives an amount from Visa under GCAR without having to provide evidence of losses. The issuer receives this fixed amount even if its actual costs are much lower or even if the issuer did not actually incur any costs in response to a particular data breach.

Because GCAR enables a double recovery from merchants for fraud losses that is accomplished in a highly arbitrary manner, it cannot represent a "reasonable endeavor" by Visa to determine a damages' sum bearing "a reasonable relationship to the range of actual damages that the parties could have anticipated would have flowed from the breach." *Ridgely v. Topa Thrift & Loan Ass'n*, 953 P.2d 484, 488 (Cal. 1998). Visa's use of GCAR, therefore, is unlawful. *Id.*

IV. CONCLUSION

As discussed above, this case has significant ramifications for retailers large and small in Texas and all fifty states. Visa's egregious GCAR program impacts Texas businesses, their employees, and their customers. For this reason and those set forth above, RLC respectfully urges the Court to grant Sally Beauty's Petition for Review.

Respectfully submitted this 18th day of March, 2022.

/s/ *Patrice Pujol*

Patrice Pujol
Texas State Bar No. 00794488
FORMAN WATKINS & KRUTZ, LLP
4900 Woodway Drive, Suite 940
Houston, Texas 77057
Telephone: 713-402-1717
Facsimile: 713-621-6746
Patrice.Pujol@formanwatkins.com

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Tex. R. App. P. 9.4(i)(2)(B) because it contains 3,864 words, excluding the parts of the brief exempted by Tex. R. App. P. 9.4(i)(1).

2. This brief complies with the typeface requirements of Tex. R. App. P. 9.4(e) because it has been prepared in a proportionally spaced typeface using Microsoft Word for Microsoft 365 MSO in 14-point Times New Roman font (and 13 point for footnotes).

/s/ *Patrice Pujol*
Patrice Pujol

CERTIFICATE OF SERVICE

I hereby certify that, on March 18, 2022, a true and correct copy of the foregoing Brief of Amicus Curiae was served via email on all counsel of record in this case.

John H. Cayce
Kelly Hart & Hallman LLP
201 Main Street, Suite 2500
Fort Worth, Texas 76102
John.cayce@kellyhart.com

Claudia Wilson Frost
Orrick, Herrington & Sutcliffe LLP
609 Main Street, 40th Floor
Houston, Texas 77002
cfrost@orrick.com

Seth Harrington
Orrick Herrington & Sutcliffe LLP
222 Berkeley Street, Suite 2000
Boston, Massachusetts 02116
sharrington@orrick.com

Douglas H. Meal
Orrick, Herrington & Sutcliffe LLP
222 Berkeley Street, Suite 2000
Boston, Massachusetts 02116
dmeal@orrick.com

Allyson N. Ho
Andrew P. LeGrand
Elizabeth A. Kiernan
Joseph E. Barakat
Emily A. Jorgens
Gibson, Dunn & Crutcher, LLP
2001 Ross Avenue, Suite 2100
Dallas, Texas 75201
aho@gibsondunn.com

Christopher M. Jordan
TX State Bar No. 4087817
Munsch Hardt Kopf & Harr, P.C.
700 Milam Street, Suite 2700
Houston, Texas 77002
cjordan@munsch.com

J. Carl Cecere
Texas State Bar No. 24050397
Cecere PC
6035 McCommas Blvd.
Dallas, TX 75206
(469) 600-9455
ccecere@cecerepc.com

/s/ *Patrice Pujol*
Patrice Pujol