No. 02-20-00339-CV

IN THE COURT OF APPEALS FOR THE SECOND DISTRICT OF TEXAS FORT WORTH, TEXAS

VISA INC.,

Appellant,

v.

SALLY BEAUTY HOLDINGS, INC.,

Appellee.

On Appeal from the 158th Judicial District Court, Denton County, Texas Cause No. 19-6924-158

BRIEF OF AMICUS CURIAE THE RETAIL LITIGATION CENTER, INC. IN SUPPORT OF SALLY BEAUTY HOLDINGS, INC.

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

W. Stephen Cannon
DC Bar No. 303727
Pro Hac Vice Application forthcoming
Richard O. Levine
DC Bar No. 203877
Pro Hac Vice Application forthcoming
CONSTANTINE CANNON LLP
1001 Pennsylvania Avenue NW
Suite 1300 North
Washington DC 20004
Telephone: 202-204-3500
Facsimile: 202-204-3501
scannon@constantinecannon.com

May 5, 2021

Deborah White
DC Bar No. 444974
Pro Hac Vice Application forthcoming
President
Retail Litigation Center
99 M Street SE
Suite 700
Washington, DC 20003
Telephone: 202-869-0088
deborah.white@rila.org

Owen Glist
NY Bar No. 4020186
MA Bar No. 651840
Pro Hac Vice Application forthcoming
CONSTANTINE CANNON LLP
335 Madison Avenue
New York, NY 10017
Telephone: 212-350-2700
Facsimile: 212-350-2701
oglist@constantinecannon.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

Owen Glist
NY Bar No. 4020186
MA Bar No. 651840
Pro Hac Vice Application forthcoming
CONSTANTINE CANNON LLP
335 Madison Avenue
New York, NY 10017
Telephone: 212-350-2700
Facsimile: 212-350-2701
oglist@constantinecannon.com

W. Stephen Cannon
DC Bar No. 303727
Pro Hac Vice Application forthcoming
Richard O. Levine
DC Bar No. 203877
Pro Hac Vice Application forthcoming
CONSTANTINE CANNON LLP
1001 Pennsylvania Avenue NW
Suite 1300 North
Washington DC 20004
Telephone: 202-204-3500
Facsimile: 202-204-3501
scannon@constantinecannon.com

Deborah White
DC Bar No. 444974
Pro Hac Vice Application forthcoming
President, Retail Litigation Center
99 M Street SE, Suite 700
Washington, DC 20003
Telephone: 202-869-0088
deborah.white@rila.org

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Regulatory Material

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 and most innovative 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, and to highlight the industry-wide consequences of significant pending cases.

This is such a case. Appellant Visa and amici American Bankers Association ("ABA") and the Credit Union National Association ("CUNA") have placed before this Court a fantasy world where financial institutions and the major card networks are benevolent protectors of the security of payment system data, and merchants large and small are to blame for the insecurity of that data. Thus, they proclaim, upholding the finding below that the Visa Global Compromised Account Recovery ("GCAR") program is an unlawful penalty program under California law would be both erroneous as a matter of law and contrary to public policy.

Nothing could be further from the truth, for it is Visa (along with Mastercard) and card-issuing banks that maintained an insecure payment environment in the United States based on obsolete magnetic-stripe card technology long after Visa and Mastercard migrated the rest of the world to more secure chip-based cards. In a payment-card environment uniquely susceptible to counterfeit fraud, Visa created the GCAR program to benefit its card-issuing member banks with financial assessments paid by merchants that are neither negotiated in advance to compensate for harm suffered by Visa nor assigned to merchants based on a causal link to a particular alleged breach—both prerequisites of a lawful liquidated damages provision.

Moreover, despite amici's claims, it is the major banks that issue the vast majority of payment cards that are the primary and significant financial beneficiaries of the GCAR program—not small credit unions. And it is retailers—along with consumers—that incur the consequences of this insecure system. Consumers face identity theft, temporary account cancellations and fraudulent credit card activity when their data are stolen. Merchants suffer financial and reputational loss when they are victims of a data breach, as well as regulatory penalties in some states. On top of those losses, merchants are also forced to bear the cost of the arbitrary assessments imposed by Visa's GCAR program.

The district court's holding that the GCAR program is an unenforceable penalty is correct as a matter of law and will not undermine the integrity of the payment system. But the harm to merchants from reversal of the decision—both from the imposition of unlawful penalties and from the prospect of continued Visa enforcement arrogance—will be real.

I. SUMMARY OF ARGUMENT

GCAR is an unlawful penalty program under California law. First, the GCAR program does not result from negotiations between merchants and Visa—for there is no contract between merchants and Visa. To the contrary, Visa avoids contractual privity with merchants, who therefore have no ability to challenge Visa fines and assessments directly. At the same time, the comprehensive system of rules that Visa promulgates to govern all parties in the system directs the banks that process merchants' card transactions (called "acquiring" banks) to enter into "merchant agreements" that bind merchants to follow Visa Rules and data security standards—rules and standards over which merchants have had no meaningful input. Thus, even though Visa technically imposes fines and assessments for alleged breaches of its Rules on acquiring banks—not merchants—everyone in the system knows that acquirers expect merchants to pay these amounts at the end of the day.

Even more significantly, the GCAR program is not intended to be a "reasonable endeavor" to provide an agreed-upon estimate of damages that are hard to calculate. Once cards are determined to be "at risk" in a "compromise event," assessments are made against merchants under GCAR without any showing that card data was in fact exported or that there is a causal link from a particular at-risk event to the actual use of card data by fraudsters. The ABA admits as much, but says that this is a feature, not a bug, of GCAR, because card data may be so thoroughly compromised from multiple breaches that tying a particular instance of fraud to a breach at a particular merchant is a fool's errand and not capable of proof. But this is just backward from the requirements of a valid liquidated damages provision. With GCAR, while fraud losses or incremental operating expenses incurred by an issuer may well be capable of calculation, a merchant's responsibility for them is committed to an undisclosed algorithm over which merchants have no say and which is not based on a causal link to purported damages stemming from a merchant's alleged data breach.

GCAR is also an unlawful penalty program because it facilitates double recovery of losses, an outcome prohibited by California liquidated damages law. The card networks have claimed that one purpose of the collective $100 billion in "interchange" fees that merchants pay to issuers annually every time a consumer swipes a credit card is to compensate issuers for costs like security expenses and

fraud losses. And at more than 2 percent of the value of every credit card transaction, these fees are more than enough to cover those expenses.

As an unlawful penalty, the GCAR program must be invalidated regardless of the practical consequences of doing so. But Visa and its amici vastly overstate those consequences. Unencumbered by the facts, the ABA and CUNA briefs seek to deflect attention from the impact to cardholders, including Texas cardholders, from Visa's maintenance of the outdated magnetic-stripe system, which uniquely exposed U.S. consumers to the increased cost and inconvenience of payment card fraud to the benefit of criminals throughout the world. In so doing, they proclaim that the GCAR fraud recovery process is crucial to the continued integrity of the Visa ecosystem.

But financial institution amici conveniently ignore the cherry on top: *Visa itself eliminated the fraud recovery component of GCAR in October 2017* as chip cards finally replaced magstripe-only cards in the United States. If GCAR was as instrumental to the payment card ecosystem as financial amici claim, surely Visa would not have voluntarily eliminated its centerpiece.

Indeed, because the GCAR Fraud Recovery element—the lion's share of the penalty imposed on Sally Beauty—was abolished as of October 14, 2017, the future effects of a court decision confirming that GCAR is an unenforceable penalty program are non-existent as to that piece. As for the remaining element

("Operating Expense Recovery"), GCAR's invalidation would leave untouched issuers' rights to assert claims directly against merchants when issuers suffer actual operational losses from data breaches for which merchants have legal liability—something issuers routinely do through class action litigation today. So for that piece as well, the invalidation of GCAR would not leave card issuers without a remedy where they deserve to have one following a data breach.

In short, this Court should uphold the district court's finding that the Visa GCAR program is an unenforceable penalty program, affirming the constraints placed on Visa by California law—Visa's choice-of-law jurisdiction. The circumstances that surround the GCAR program explained below provide more context to support the lower court's decision, as well as more assurance that this Court can comfortably affirm without fear of amici's "Chicken Little" arguments. Indeed, the Court may do so if for no other reason than Visa itself eliminated a key element of GCAR in 2017 and the payment card network sky still has not fallen.

II. FACTUAL BACKGROUND: GCAR IS AN OUTGROWTH OF VISA'S INSECURE MAGNETIC-STRIPE STANDARD

When a consumer uses a payment card at a merchant checkout counter or website, a multi-step process takes place behind the scenes to debit the consumer's account and credit the merchant. The process involves three key parties: (1) the consumer's bank (known as a card "issuer" or "issuing bank"); (2) the merchant's bank (known as an "acquirer" or "acquiring bank" because they "acquire" the

transaction at the point-of-sale); and (3) the payment card network, such as Visa and Mastercard, that connects issuing and acquiring banks to authorize, clear, and settle the transaction between them. Visa considers both issuing banks and acquiring banks to be "members" of Visa's network.[1]

The payment card device employed by consumers to initiate a transaction 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.[2] By the 1990s it was well known that this ubiquitous piece of plastic was 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

[1] The majority of issuers and acquirers in this system are banks, so that term is used throughout this amicus brief, although credit unions also function as issuers or acquirers.

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

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."[3]

Visa and Mastercard announced a global migration to chip cards in 1999, and EMV-chip cards and EMV-capable terminals were implemented around the world—except in the United States, which was the card networks' largest market and therefore should have moved first, not last. In countries outside 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.[4] But why?

---

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

[4] 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

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 because they can charge higher network and interchange fees, whereas chip-and-PIN transactions in other countries often came with lower network and interchange fees.[5] In particular, Visa (and Mastercard) allows issuers to deduct interchange (or "swipe fees") from amounts due to merchants for both credit and debit card transactions. These fees reportedly amounted to $100 billion in 2020 and are in addition to the billions in finance charges and other fees these issuers charge to their cardholders (not to

---

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.

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

mention the additional fees with which merchants may get saddled under penalty programs such as GCAR).[6]

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 press release put it: "The United States of America is excluded from the figures as there are currently no EMV programmes deployed."[7]

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 "immigrant 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.[8] Implementation of EMV-chip technology worked when it

---

[6] 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.

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

[8] *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

finally arrived in the 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."[9]

As chip card adoption accelerated globally and the concurrent amount of counterfeit magstripe fraud increased in the United States, Visa did not choose to implement chip cards in the United States—which would have reduced fraud—but instead chose to establish GCAR's predecessor, the Account Data Compromise

---

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 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.").

[9] 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.

Recovery ("ADCR") program in the United States in 2006—a program designed to shift the cost burden for the fraud from issuers to merchants.

In 2012, Visa changed from the ADCR program to GCAR. At the times relevant to this case, the GCAR program had two components: (1) "Operational Expense Recovery," which provides issuers with per-card payments for cards notified to them as potentially compromised in a data breach, supposedly to cover the card issuing bank's expenses for potential card reissuance and enhanced fraud monitoring; and (2) "Fraud Recovery," purportedly to reimburse issuing banks for fraud claims allocated to a potential compromise by GCAR algorithms.

With ADCR and later GCAR, rather than address the problem at the source by introducing proven chip technology to the United States, Visa implemented mechanisms to simply shift the costs of the increased fraud burden to merchants. The GCAR system that existed at the time of this case remained in effect until October 2017. By this time, Visa had implemented different mechanisms to shift the cost of fraud to merchants and so rescinded the Fraud Recovery element of GCAR. Meanwhile, GCAR's Operational Expense Recovery element is still in place.

III. ARGUMENT

Regardless of which elements of GCAR exist today, GCAR was and remains an unlawful penalty program because: (1) GCAR is not an agreement between Visa and merchants, who are the intended payers of GCAR assessments; and (2) GCAR does not represent a reasonable endeavor to estimate actual damages. Critically, upholding the decision below will not undermine the payment network and, even without GCAR, issuers may continue to avail themselves of the same lawful means of redress that the rest of the economic actors in America enjoy.

A. The GCAR Program Is an Unlawful Penalty Because It Is Not an Agreement Between Visa and Merchants, the Intended Payers of GCAR Assessments.

GCAR assessments are not the result of an agreement between Visa and merchants, who are the expected and thus the intended payers of GCAR assessments. *Cf. Mo-Vac Serv. Co. v. Escobedo,* 603 S.W.3d 119, 128-29 (Tex. 2020) (a person intends a consequence to an individual that the person knows is substantially certain to occur). Here, Visa has built a system based on a series of fictions in which merchants are treated as mere bystanders to a mechanism that nonetheless imposes liability on them. Visa avoids contractual privity with merchants—dealing instead with merchant acquiring banks—but does so with full

knowledge that acquirers hold merchants liable for the penalties and assessments that Visa imposes on them.

Visa makes clear that it established the GCAR program to balance the aggregate interests of the *financial institutions* that issue cards to consumers and the acquiring *financial institutions* that process transactions on behalf of merchants in order to deal with the large volume of potentially compromised cards and transactions circulating through the Visa system. Indeed, amici confirm that GCAR is not intended to compensate Visa (the only party to the contract with the acquirer that is subject to the GCAR assessment). *See* CUNA Br. at 5 (GCAR "is a loss allocation program for data breaches."). Nothing in the GCAR program is intended to address any harm to Visa itself from a data breach, even though Visa designs and sets the technology specifications for payment cards. Moreover, the needs or procedural rights of merchants are not part of Visa's concerns: "Global Compromised Account Recovery (GCAR) is . . . designed to balance the *needs of Visa clients*," i.e., issuing banks and acquiring banks. *Visa Global Compromised Account Recovery (GCAR) User Guide*, January 2015, Public ("2015 GCAR User Guide") at 1 (emphasis added).[10]

[10] Visa's website no longer provides access to its 2015 GCAR User Guide. For ease of reference, a true and correct copy of the document has been placed at the following link: https://constantinecannon.box.com/s/5szh80lyx2hwbacgsaf07a8zeuloqkxt

Next, Visa's Rules mandate that each acquirer have an agreement with each merchant. These "merchant agreements" must require merchant compliance with Visa's Rules as applicable to merchants, including its risk and security programs.[11] In particular, Visa requires that U.S. merchant agreements contain, "A requirement that the Merchant and its Agents comply with the provisions of the Account Information Security Program," which includes adherence to data security standard requirements.[12]

Next, acquirers insert in their merchant agreements non-negotiable provisions requiring merchants to indemnify them for all fines and assessments imposed on them as an acquirer under GCAR and the equivalent programs of other networks. Indeed, many such agreements permit acquirers to establish "reserve accounts" in anticipation of *potential* GCAR assessments once the networks open a data breach investigation. Acquirers fund these "reserve accounts" by seizing amounts due to merchants from their payment card transactions with customers.

Finally, even though Visa mandates that an acquirer must ensure that its merchants agree to comply with all Visa data security rules, and even though all industry participants know fines and assessments are *always* passed on to

---

[11] Visa Rule 1.5.2, *Visa Core Rules and Visa Product and Services Rules* (Oct. 17, 2020) ("Visa Rules"), https://usa.visa.com/dam/VCOM/download/about-visa/visa-rules-public.pdf.

[12] Visa Rule 5.2.1.7

merchants by Visa-member acquirers, Visa's regulations mandate that in communicating to merchants, acquirers must never blame Visa at all for the assessments Visa imposes:

> A non-compliance assessment is imposed by Visa on a Member [i.e., financial institution]. A Member is responsible for paying all non-compliance assessments, regardless of whether it absorbs them, passes them on, or increases them in billing its customer (for example: Cardholder or Merchant). *A Member must not represent to its customer that Visa imposes any non-compliance assessment on its customer*.

Visa Rule 1.12.2.5 (emphasis added).

One direct effect of this no-relationship fiction is that *only* the acquirer can appeal a Visa fine or assessment—the affected merchant cannot do so. And even if the acquirer does submit an appeal, whether to grant such an appeal is fully within Visa's discretion, with no further appeal rights. 2015 GCAR User Guide at 31.

In sum, because the GCAR program was unilaterally adopted by Visa and does not result from negotiation between Visa and merchants, the GCAR mechanism fails the first element of a lawful liquidated damages clause: the existence of an agreement between the parties. *Ridgely v. Topa Thrift & Loan Ass'n*, 953 P.2d 484, 488 (Cal. 1998).

B. GCAR Is an Unlawful Penalty Because It Does Not Represent a "Reasonable Endeavor" to Estimate the Range of Actual Damages Resulting from a Breach and Permits Double-Recovery.

As the California Supreme Court has ruled, a liquidated damages provision may be upheld only if it constitutes a "reasonable endeavor" among the parties to

determine a damages sum that bears "a reasonable relationship to the range of actual damages that the parties could have anticipated would flow from the breach." *Ridgely*, 953 P.2d at 488.

Visa's Rules and the briefs submitted by the ABA and CUNA make no pretense of meeting these prerequisites of a causal link between a *predetermined* liability amount and an actual contractual breach. As Visa describes it:

> [GCAR] is a *loss-allocation* program designed to balance the needs of Visa clients in the event of a large scale Account Data Compromise Event. It provides a fair, efficient, and streamlined process to *enable issuers to recover a portion* of their estimated Incremental Counterfeit Fraud losses and operating expenses in *exchange for establishing limits on potential acquirer liability*.

2015 GCAR User Guide at 1 (emphasis added).

Arbitrariness and uncertainty occur at every step of the way in Visa's GCAR program. Under the GCAR Fraud Recovery program, 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 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.

As for GCAR Operating Expense Recovery, 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 multiplying the number of the issuer's "at risk" accounts by a fixed per card amount. 2015 GCAR User Guide 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.

The ABA argues that the fact that GCAR's allocation methodology makes no attempt to causally link (rather than to algorithmically assign) losses by financial institutions is a virtue, not a vice, of GCAR. Most revealing, the ABA argues that the circulation of compromised card data on global criminal web sites is so pervasive that attempts to link a potential compromise at a merchant location with any particular losses by a financial institution would be difficult: "One of the greatest uncertainties in data-breach litigation can be establishing the requisite

connection between a card-holder's fraud-related losses and a merchant's data breach. . . . The task is only getting harder as data breaches become more common, making it 'increasingly likely that someone will have their' data 'compromised by multiple data breaches.'" ABA Br. at 12, 13-14 (citations omitted).

But an algorithm that assigns the fraud claims entered into Visa systems with cards that have merely been potentially compromised by a breach at a specific merchant is the opposite of a lawful liquidated damages calculation. Rather than estimate damages for breach of a contract where a causal link between the breaching party and the injury is clear, here the "endeavor" by Visa is to allocate liability for alleged damages to a particular merchant regardless of whether a causal link to the merchant exists at all. Such a mechanism is not countenanced under California law.

Further, rather than being a predetermined amount, Visa Rule 10.10.1.1 provides that the amount of GCAR recoveries rests wholly within Visa's discretion: "Visa has the authority and discretion to determine Account Data Compromise Event qualification, Operating Expense Recovery amounts, Issuer eligibility, and Acquirer liability under the GCAR program . . . ." Indeed, in the case of a particularly large financial liability, a merchant may find itself at Visa's mercy. Visa may declare an event to be potentially "catastrophic" to a merchant after reviewing three years of its financials. If an event is deemed catastrophic by

Visa, "in its sole and absolute discretion, Visa reserves the right to implement an alternate process to the GCAR program." 2015 GCAR Users Guide at 36. These are hardly the indicia of a true, enforceable liquidated damages mechanism.

Finally, GCAR is an unlawful penalty because it facilitates double recovery of fraud losses. Merchants pay some $100 billion in swipe fees to issuing banks annually, fees designed to compensate issuers for operating their payment card programs, including security expenses and fraud losses, and provide issuers with billions in net profits.[13]

C. Visa's Own Changes to GCAR Underscore That Upholding the Decision Below Will Not Harm the Integrity of the Visa Payment System.

In their briefs, both CUNA and the ABA place the GCAR program at the heart of processes designed to ensure the integrity of the payment system. They claim that if the GCAR program were found to be an unlawful penalty, the public

---

[13] *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. To take one example, Bank of America received $4 billion in ***net*** income just from interchange fees paid by merchants in 2020. Bank of America Annual Report 133 (2020), https://investor.bankofamerica.com/annual-reports-and-proxy-statements. 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).

would be seriously harmed. *See, e.g.*, CUNA Brief at 8 ("Put simply, these loss allocation programs are essential to the safety and sound functioning of payment card networks."); ABA Br. at 17-18 ("[U]pholding the lower court's ruling invalidating the GCAR Assessment would present a serious, multifaceted threat to Visa's payment network."). But these claims are belied by the fact that Visa itself eliminated GCAR Fraud Recovery—the aspect of the penalty program that constitutes the bulk of the assessment levied in this case—over three years ago, and yet the payment system has not suffered.

Why did Visa eliminate the largest piece of a program that it and its amici now claim is essential? The short answer is that, as Visa finally brought chip technology to the United States to reduce fraud and found other ways to shift the cost burden from issuers to merchants, Fraud Recovery under GCAR was no longer needed to accomplish Visa's goal.

The longer answer requires some context (somewhat simplified here) to understand that GCAR Fraud Recovery was solely concerned with one, now-largely-obsolete form of fraud—counterfeit, the type of fraud committed by a fraudster in-person by swiping fake magstripe payment cards, and the type of fraud prevented by EMV chip cards. In the ordinary course, issuing banks, not merchants, were liable for fraud committed using counterfeit cards, and they accounted for this fraud as a cost of operating their card programs. Issuing banks,

not merchants, were held liable because, to a merchant, nothing was amiss—a customer swiped their payment card and the issuing bank electronically approved the transaction. If a cardholder later complained to their bank that they suspected fraud, and the transaction took place in person, the bank credited the cardholder and absorbed the loss. Against this backdrop where issuers were generally responsible for magstripe transactions that they authorized, GCAR Fraud Recovery was adopted as a mechanism to shift the costs of these fraudulent transactions from issuers to merchants.

In contrast, e-commerce or "card-not-present" transactions, were never subject to GCAR Fraud Recovery because merchants were held liable for any fraud that occurred in these transactions from the get-go. For these transactions, if a cardholder reported fraud, the transaction was immediately reversed or "charged back" to the e-commerce merchant—the issuing bank was not liable for any fraud loss, on the theory that it was the merchant taking the risk of accepting the transaction without the card or the cardholder "present." Because merchants, not issuing banks, paid for these fraud losses, they were not part of GCAR Fraud Recovery.

GCAR's usefulness began to wane as Visa announced the U.S. migration from magstripe to chip in the fall of 2011. That long-delayed transition was combined with the new rules from Visa that shifted all liability for counterfeit

magstripe fraud from issuing banks directly to merchants, effective October 2015. Visa's new rules put the responsibility for fraudulent transactions on merchants who had not yet upgraded their payment terminals to accept chip cards, on the theory that chip would have prevented this type of fraud. The shift allowed issuers to simply charge back counterfeit fraud to the merchant—just as they could with suspected fraud at online merchants—giving complete recovery to issuing banks outside of (and far in excess of) the GCAR program.

Given these and other changes as the migration to chip finally progressed in the United States, Visa announced that, effective October 14, 2017, the Fraud Recovery component of GCAR would be eliminated "to simplify program rules and calculations." The current Visa Rules (Rule 10.10.1.1, October 17, 2020) maintain this exclusion of fraud recovery and limit partial expense recovery in card-present environments. As a result, because Visa revised its rules after the events in the present case as part of the completion of its long-delayed U.S. EMV chip rollout, affirming the lower court here will have no future effect on the Fraud Recovery portion of the GCAR program—because it no longer exists.

As for the other piece of the GCAR penalty program, Operating Recovery, the district court's decision will likewise not have any impact on the integrity of the payment card system. As both Visa and their amici acknowledge, before the creation of the GCAR predecessor program in 2006, issuers could and did recover

their documented, actual losses through a Visa-administered program known as a "compliance case."

Moreover, as Visa and its amici also know well, where issuers suffer actual operational losses from data breaches for which merchants have legal liability, they can (and routinely do, see Part II.D, *infra*) institute class action litigation directly against such merchants, seeking to recover such losses. There is no reason to think the invalidation of GCAR will therefore leave card issuers without a remedy for recovering incremental operating expenses when they can show they are entitled to such a remedy following a data breach. Rather, invalidation would merely strip card issuers of their current undeserved windfall recoveries of millions of dollars following a data breach without regard to what, if any, losses they actually suffered from the breach or whether the merchant actually had factual or legal liability for the breach.

Finally, although CUNA asserts the importance of GCAR to small credit unions, they ignore the high levels of concentration in the payments industry. Just the five largest Visa and Mastercard banks (Chase, Citibank, Capital One, Bank of America, and US Bank) alone account for 70 percent of Visa and Mastercard credit card volume.[14] These and other massive banks—who are already collecting

[14] *See* Nilson Report, Issue Nos. 1191 (Feb. 2021) & 1192 (Feb. 2021).

billions in interchange fees from merchants and finance charges from cardholders—are the true beneficiaries of nearly all GCAR recoveries.

In sum, this Court can affirm the district court's decision without fear that it will adversely affect the payment networks, card issuers, cardholders, or small financial institutions—including in the state of Texas. Given the changes that Visa has already made to GCAR, it is clear that the program is not essential to the continuing function of the payment ecosystem; nonetheless, the decision below is essential because it sets a clear legal limit on the types of penalties that Visa can impose on merchants.

D. Alternate Means of Issuer Recovery May Exist Outside the GCAR Mechanism.

In its brief, the ABA makes much of the difficulties financial institutions would face if they had to sue merchants directly for costs arising from a data breach at that merchant. Such difficulties, argues the ABA, relate both to issues of proof and to the "economic loss doctrine," adopted in some states, which precludes tort recoveries for negligence not involving physical harm.[15] ABA Br. at 13-14.

But actions for recovery of such damages have been brought—and successfully so—many times under state law. Many such actions have resulted in settlements benefitting a class of financial institutions. *See, e.g.*, *In re: Arby's*

[15] *See, e.g.*, *LAN/STV v. Martin K. Eby Const. Co.*, 435 S.W.3d 234 (Tex. 2014) (applying economic loss rule).

Rest. Grp., Inc. Litig., 1:17-cv-514-WMR, Dkt. No. 317 (N.D. Ga. Nov. 25, 2020)*; In re Equifax Inc. Customer Data Sec. Breach Litig.*, 1:17-md-02800, Dkt. No. 1193 (N.D. Ga. Nov. 16, 2020); *First Choice Fed. Credit Union v. Wendy's*, 2:16-cv-506, Dkt. No. 191 (W.D. Pa. Nov. 6, 2019); *In re: The Home Depot, Inc., Customer Data Sec. Breach Litig.*, 1:14-md-02583-TWT, Dkt. No. 343 (N.D. Ga. Sept. 22, 2017); *Greater Chautauqua Fed. Credit Union v. KMart Corp.*, 1:15-cv-02228, Dkt. No. 152 (N.D. Ill. June, 16 2017); *In re: Target Corp. Customer Data Sec. Breach Litig.*, 14:2522, Dkt. No. 758, 2016 WL 2757692 (D. Minn. May 12, 2016).

Recently, an Ohio federal district court upheld a negligence claim by several credit unions against a motion to dismiss by a drive-in restaurant under Oklahoma law. *In re Sonic Corp. Customer Data Breach Litig. (Financial Institutions)*, No. 17-md-2807, 2020 WL 3577341 (N.D. Ohio July 1, 2020). That court later certified a class composed of: "All banks, credit unions, and financial institutions in the United States that received notice and took action to reissue credit cards or debit cards or reimbursed a compromised account from any card brand involved with the Sonic Data Breach." *In re Sonic Corp.*, 2020 WL 6701992 (Nov.13, 2020). Notably, the court appointed Fort Worth-based American Airlines Federal Credit Union as one of the four class representatives in that case.

In these cases, of course, the supposedly aggrieved issuing banks must *prove* (1) actual losses (2) proximately caused (3) by the merchant's unlawful conduct. This, of course, is the black letter legal standard that works perfectly well for the rest of America, but that Visa and its issuing banks would prefer to escape through their unlawful GCAR program. Far from undermining the payment system, affirming the lower court's decision to invalidate the GCAR program merely requires the payment system to function the same way the rest of U.S. commerce functions: according to, and subject to, the rule of law—a result that is hardly contrary to public policy.

IV. CONCLUSION

For the reasons set forth above, the district court's opinion should be affirmed and Visa's GCAR program should be held to be an unlawful penalty under California law.

Respectfully submitted this 5th day of May, 2021.

/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

W. Stephen Cannon
DC Bar No. 303727
Pro Hac Vice Application forthcoming
Richard O. Levine
DC Bar No. 203877
Pro Hac Vice Application forthcoming
CONSTANTINE CANNON LLP
1001 Pennsylvania Avenue NW
Suite 1300 North
Washington DC 20004
Telephone: 202-204-3500
Facsimile: 202-204-3501
scannon@constantinecannon.com

Owen Glist
NY Bar No. 4020186
MA Bar No. 651840
Pro Hac Vice Application forthcoming
CONSTANTINE CANNON LLP
335 Madison Avenue
New York, NY 10017
Telephone: 212-350-2700
Facsimile: 212-350-2701
oglist@constantinecannon.com

Deborah White
DC Bar No. 444974
Pro Hac Vice Application forthcoming
President
Retail Litigation Center
99 M Street SE
Suite 700
Washington, DC 20003
Telephone: 202-869-0088
deborah.white@rila.org

Counsel for Amicus Curiae
The Retail Litigation Center, Inc.

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 6,476 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 May 5, 2021, 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