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 AMERICAN BANKERS ASSOCIATION IN SUPPORT OF APPELLANT

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

Counsel for Amicus Curiae

TABLE OF CONTENTS

INDEX OF AUTHORITIES

Cases:

Statutes & regulations:

Other authorities:

Other authorities—continued:

STATEMENT OF INTEREST[1]

The American Bankers Association (ABA) is the principal national trade association of the financial services industry in the United States. Founded in 1875, the ABA is the voice for the nation's $13 trillion banking industry and its million employees. ABA members are located in each of the fifty States and the District of Columbia, and include financial institutions of all sizes and types, both large and small. ABA frequently submits amicus curiae briefs in state and federal courts in matters that significantly affect its members and the business of banking.

This is just such a case. Virtually all the ABA's members play some role in card-payment processing networks like Visa's, serving as issuing banks, acquiring banks, or both. ABA therefore has a vested interest in supporting the orderly and secure operation of these processing networks. ABA recognizes the critical role that Visa's Global Compromised Account Recovery Program (GCAR) plays in preserving the integrity of Visa's own network, and the crucial role that similar programs play in protecting competitors' networks. The decision below threatens the vitality of all programs like the

[1] No counsel for any party authored this brief in whole or in part, and no person or entity, other than amicus curiae, its members, or its counsel contributed money to fund the brief's preparation or submission.

GCAR Program, by invalidating its key component—the GCAR Assessment. That presents a threat to Visa's network and every stakeholder associated with it, including the customers of ABA-member banks. The ABA therefore urges the Court to overturn the trial court's decision.

INTRODUCTION AND SUMMARY OF THE ARGUMENT

One of the biggest challenges of modern commerce is protecting debit and credit card data. The 16 digits embossed on a credit or debit card serve to facilitate the vast majority of transactions occurring worldwide, enabling cardholders to purchase—via a single swipe—virtually any good or service over networks that connect to almost every merchant, and every major bank.

Yet the very features that make card numbers so powerful in facilitating commerce also make them one of the most sensitive pieces of data that comprise a person's personal identity. In the wrong hands, those 16 digits could permit thieves to steal thousands of dollars within minutes—by racking up unauthorized charges or draining bank accounts—and could create identity-theft losses lasting a lifetime.

Yet every time a customer uses a card to make a purchase—an event that occurred 44.7 billion times in the past year alone—individuals must expose that sensitive data and turn it over to a merchant for safekeeping. *See*

The Fed. Reserve, *The Federal Reserve Payments Study 2019* (2020), http://bit.ly/3vqLTrm. If even one of those merchants experiences a data breach, card data from every register within a merchant's system could be exposed, allowing bad actors to access the credit-card numbers for thousands—or millions—of the merchant's customers. Accordingly, the benefits and risks of card transactions make the problem of securing card data an issue of pressing concern for every stakeholder in the card-payment system.

Banks and other financial institutions must address these issues because they are subject to a comprehensive set of regulatory and oversight requirements mandated by federal law. But merchants have so far escaped regulation that would bring their links in the chain of data custody up to bank-level standards. As a result, merchants experience card data breaches more than six times as often as financial institutions, despite controlling far less actual card data. Identity Theft Res. Ctr., *2019 End-of-Year Data Breach Report* at 2 (2019).

Yet merchant data security is an attainable goal, as Visa has demonstrated with its GCAR Program. This program protects the physical and financial integrity of Visa's network from the threats posed by merchant

data breaches, while providing protections for every stakeholder within the network. The GCAR Program protects cardholders by requiring acquiring banks to ensure their merchants take commonsense precautions to secure their customers' card numbers—measures that, if followed, virtually eliminate the risk that cardholders will suffer harm from data breaches of merchant card acceptance systems.

The GCAR Program also protects the banks that issue cards. If a merchant fails to take those commonsense steps and a data breach results, the program's liquidated damages provision, the GCAR Assessment, requires the merchant's acquiring bank to compensate the cardholders' issuing banks for the frequently numerous, often immeasurable, and usually unrecoverable costs they incur because of the merchant's failures. And the acquiring banks can—and usually will—pass those costs on to merchants.

Yet the GCAR Assessment also protects the merchants themselves, and their own acquiring banks, by providing a fixed, fair, efficient, and capped mechanism for resolving liability for data breaches. And of course, the program benefits Visa, and supports the value its network extends to end-users, by ensuring its entire card-payment ecosystem continues to function and attracts new cardholders, new issuing banks, new acquiring banks, and

new merchants. The GCAR Program and the GCAR Assessment are thus critical components of Visa's card-payment system.

The lower court's judgment in this case strikes at cornerstones of that system. If the lower court is correct, and the GCAR Assessment is an illegal contractual penalty, then merchants can simply delete the GCAR Assessment from their contracts at their pleasure. That will strike a blow to the entire GCAR Program and upset settled expectations of all the players in Visa's payment-processing network. It will make cardholder data less secure. It will force banks, and ultimately their customers, to absorb losses for data breaches they did not cause and could not prevent. It will compel changes to mutually agreed-upon, industry-standard practices that have governed card-payment networks nationwide for nearly a decade. And it could threaten the very integrity of Visa's payment system. Accordingly, it is vital that the Court reverse the lower court's erroneous judgment and restore the GCAR Assessment provision in Sally Beauty's acquiring bank's contract with Visa.

ARGUMENT

I. Visa's GCAR Program, and the GCAR Assessment, provide vital protections to all the stakeholders in Visa's card-payment-processing network.

The judgment of the court below may have limited itself to striking a single contractual provision from a single agreement between a single

acquiring bank and Visa. But the ripples from the lower court's ruling will nonetheless be felt throughout Visa's entire card-payment network, as well as similar networks maintained by Visa's competitors. And those ripples will be experienced by all stakeholders within those networks. That includes the customers who use the cards, the banks that issue the cards, the merchants that accept the cards, and network providers like Visa, which operate the payment networks connecting them all together. *See* CFPB, *The Consumer Credit Card Market* 11, 18 & n.20, 23 (2019), https://bit.ly/3bQKsuv.

These systemic shocks will occur because the contractual provision at issue in this case concerns the GCAR Assessment, an integral part of Visa's GCAR Program, which protects all these constituent interests within Visa's card-payment network. These varied interests are all best served by seeing the GCAR Program, and the GCAR Assessment, left intact.

A. The GCAR Program and the GCAR Assessment benefit cardholders and banks by minimizing and distributing the risk of loss from merchant-level data breaches.

The GCAR Program is Visa's effort to tackle one of the biggest problems in modern commerce: the risk of card fraud resulting when criminals access card number data held by merchants. Merchants obtain that data with every card swipe that occurs during a purchase. And fraudsters frequently manage

to hack into that data by gaining access to merchant's "point of sale" systems—the terminals where the card swipes take place and this data is stored. *Visa Global Account Recovery Program: What Every Merchant Should Know About GCAR* at 2 (2013) (*Visa GCAR Merchant Information*), https://bit.ly/3cBGV2p. Fraudsters might use the card numbers they steal from merchants' machines to create new "counterfeit cards." *Id.* Or they might download them to a computer, thereby obtaining the ability to conduct fraudulent card transactions online or over the phone. *Id.*

In recent years, criminals have used these techniques to accomplish a series of high-profile hackings of some of the country's leading retailers—including names like Home Depot, Target, Neiman Marcus, and P.F. Chang's. *See* Robin Sidel, *Home Depot's 56 Million Card Breach Bigger than Target's*, Wall St. J., Sept. 18, 2014, http://on.wsj.com/2OVnaL7. Through these hacks, experts estimate that over 160 million consumers had their credit-card numbers exposed. BridgeForce Special Report, *Combating Fraud and Data Breaches: End-to-end strategic management insights*, at 1 (2015), https://bit.ly/314BPGG.

And the losses from credit card fraud can be devastating. The Federal Trade Commission recently reported that card fraud is the most common type

of identity theft. FTC, Consumer Sentinel Network, *Data Book 2019*, at 4 (Jan. 2020), https://bit.ly/3bQzVjj. Last year, losses due to card fraud amounted to $9.62 billion. Nilson Report at 5 (Issue No. 1187, Dec. 2020), http://bit.ly/3eE8TgQ.

Yet the burdens from merchant-data fraud losses are not naturally distributed evenly within Visa's network. Those losses are initially suffered by the cardholders alone. It is their card numbers that are exposed when a merchant data breach occurs. It is also their bank accounts that are drained, and credit lines maxed out, when a thief obtains the card numbers and uses them to create unauthorized charges. And while, for customers, these disruptions will definitely be alarming, sometimes be time-consuming, and certainly be inconvenient, most of the financial losses will eventually be transferred to the banks because federal law and bank policies limit customers' liability for unauthorized charges, placing most of the risk onto the issuing bank. *See* Fair Credit Billing Act, 15 U.S.C. § 1666(e) (limiting credit card holders' liability to $50 in most cases); *see also* Electronic Fund Transfer Act, 15 U.S.C. § 1693 *et seq.*. & Regulation E (12 C.F.R. § 205.6) (limiting liability of consumers for unauthorized wire transfers to $50 in most cases).

Accordingly, the banks and their customers suffer virtually all the harm

from merchant-level data breaches. And that harm can be ruinous, especially for small, community banks. For them, the simple cost of providing a replacement card to every one of their customers could prove crippling. If forced to absorb millions of dollars in fraudulent charges that occur in the average data breach, many would probably be driven out of business. *See* IBM Security, *Cost of a Data Breach Report*, at 5 (2020) (*IBM Security Report*).

But the banks and their customers have virtually no power to prevent breaches of card data held by merchants. No matter how careful customers might be in keeping tabs on their cards, and no matter how vigilant the banks might be in securing card data within their own systems, banks and cardholders lose all control when a customer turns that data over to a merchant during a card swipe. At that point, if the merchant fails to protect the customer's card data, then the data enjoys no protection at all. The system is truly only as strong as its weakest link.

Visa's GCAR Program exists to correct this basic mismatch between the cardholders and banks that bear the risk of loss from a merchant-level breach, and the merchants that actually control whether a breach occurs. The program requires merchants in Visa's network to take measures to protect customer card data. Specifically, the program mandates that merchants follow an

industry-wide security standard, embodied in the "Payment Card Industry Data Security Standard" (PCI-DSS), which virtually eliminates any risk from damaging breaches of a merchant's card data. *See Visa GCAR Merchant Information*, *supra* at 1 (citing www.pcisecuritystandards.org).

The PCI-DSS requires merchants to maintain a variety of security features and protocols, including firewalls, anti-virus software, strong access control measures, and system testing. These measures ensure that unauthorized persons can never obtain access to customers' card data. Richard Rohena, *PCI-DSS: The Six Major Principles*, GlobalPayments Integrated Blog, http://bit.ly/38KtV9O; *see also* Elavon, *Data Compromise Management*, at 6 (2010), https://bit.ly/3bTe7U7.

But even if a criminal manages to thwart all these security measures and gains access to merchant card data, the PCI-DSS contain failsafe measures that protect the data despite the breach. The PCI-DSS requires that merchants eliminate storage of cardholder data whenever possible, thereby minimizing the number of card numbers that might be disclosed during a breach. Rohena, *supra;* Elavon, *supra* at 6. The PCI-DSS also requires merchants to encode card data during storage, and encrypt it during transmittal over public networks, so that any would-be thief who actually

obtains access to the card data would not be able to use it. Accordingly, the PCI-DSS imposed through the GCAR Program ensure that the merchants—the only stakeholders in Visa's payment network capable of stopping merchant-level card data breaches—actually take steps to stop those breaches. And if merchants follow the PCI-DSS as Visa requires, there is extraordinarily little risk that a damaging merchant-level data breach will occur. Rohena, *supra;* Elavon, *supra* at 6.

Yet if merchants in the Visa network fail to follow the PCI-DSS, dangerous breaches could result. This is where the GCAR Program steps in to ensure that banks and their customers are not required to bear losses from those breaches on their own—through the GCAR Assessment. It "enables issuers to recover a portion of the costs" they experience because of merchant-level data breaches, often by obtaining compensation from the merchants themselves. *Visa GCAR Merchant Information*, *supra* at 1. When a merchant's failure to follow PCI-DSS results in a data breach, the merchant must typically compensate the banks that suffer fraud-related losses as the result of that breach. The payment amount is determined by a standardized formula representing an estimate of the fraud-related losses that the banks likely suffered. The formula also includes an allowance for recovery "of the

associated operating expenses" likely to arise after a breach, *id.*, such as the "costs of replacing compromised cards" or "increased account monitoring," *Paymentech, LLC v. Landry's Inc.*, No. CV H-18-1622, 2020 WL 1671075, at *1 (S.D. Tex. Feb. 10, 2020). The formula is not meant to provide the banks complete compensation, but it does ensure that merchants and their acquirers are required to share the fraud-related costs that their security-related failures create for banks and their customers.

The GCAR Assessment also provides banks with an efficient, equitable means of recouping fraud-related expenses that they would have difficulty recovering through litigation. Attempting to pursue litigation against the card fraudsters who actually steal cardholder data is usually a non-starter. And the option of pursuing litigation against the merchant who facilitates the theft is a fraught path full of uncertainty, difficulty, and great expense.

One of the greatest uncertainties in data-breach litigation can be establishing the requisite connection between a cardholder's fraud-related losses and a merchant's data breach. It can be difficult—and costly—simply to establish whether a data breach has occurred. Even when a merchant leaves a customer's card data out in the open, that does not necessarily mean a criminal has accessed it. Many data-breach cases fail simply because the plaintiff

cannot establish this crucial causal link. *See, e.g.*, *Guin v. Brazos Higher Educ. Servs.*, No. Civ. 05-668 RHK/JSM, 2006 WL 288483, at *4 (D. Minn. Feb. 7, 2006) (dismissing data-breach claims related to a stolen laptop where the customer could not prove data on the laptop had been accessed by outsiders).

And a bank may still have difficulty proving causation even when it can establish that a criminal accessed its customer's card information, because it is always hard to establish the requisite connection between the criminal's access and a customer's fraud-related losses. That requires demonstrating the data taken during the breach was the same data used to commit fraud—a showing that requires tracing the data's path through the electronic criminal underworld. But stolen data frequently disappears into a web of criminal activity that can be hard to untangle. Often it falls into the depths of the "dark web," where it can be bought cheaply by anonymous sources and combined with other data in ways that can often be impossible to trace. Brian Stack, Experian Blog, *Here's How Much Your Personal Information Is Selling for on the Dark Web* (Dec. 6, 2017), http://bit.ly/3eAjzgk. Accordingly, it will frequently be hard for a bank to prove that a particular data breach was associated with a particular fraud.

This 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." Michael Hooker, *Have We Reached the Tipping Point? Emerging Causation Issues in Data-Breach Litigation*, Fla. Bar J. (May/June 2020). And that will make it difficult to determine *which* breach, if any, led to a customer's losses. Indeed, some experts believe the country is reaching a "tipping point," "where it will be virtually impossible to determine whether a particular data breach was the proximate cause of subsequent related harm if the claimant's" private data "was previously disclosed in one or more other data breaches." *Id.*

Other legal barriers besides causation may also prevent a bank from recovering fraud-related losses from a merchant. Depending upon the court, and depending upon the claim, matters such as standing and the "economic loss" doctrine can stand in the way of recovery. *See, e.g.*, *Banknorth, N.A. v. BJ's Wholesale Club, Inc.*, 442 F. Supp. 2d 206 (M.D. Pa. 2006); *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 427 F. Supp. 2d 526 (M.D. Pa. 2006), *aff'd in part, rev'd in part*, 533 F.3d 162 (3d Cir. 2008) (dismissing bank's contract claims against merchant because the bank was not a third-party beneficiary to the contract between the merchant and the merchant's bank, and dismissing tort claims under the "economic loss" doctrine).

Finally, even if a bank manages to clear all these hurdles along the path to recovery, success remains uncertain because "[p]roving damages in data breach cases is almost as difficult as establishing sufficient harm exists to bring a case in the first place." CQ Roll Call Washington Data Privacy Briefing, *Data breach cases don't need an actual data breach, Edelson and Meal agree*, 2017 WL 1404112 (April 20, 2017). Some of the losses from card fraud are intangible, and therefore hard to measure with certainty. Some of the losses are consequential, and therefore difficult to predict in advance. And some are indeterminate by nature because they concern future risks of harms that may never arise or involve "long-tail" exposures that have costs that continue years after a data breach. *IBM Security Report*, *supra* at 58. All these factors can make it difficult to establish damages with any precision. And a bank's likelihood of obtaining a recovery can be made still more uncertain by the significant litigation expenses incurred in pursuing it—expenses that often swamp the losses themselves. The GCAR Assessment avoids all these pitfalls, and all of litigation's uncertainty and expense, thereby providing a fair, equitable, and efficient means of establishing fraud-related losses without litigation.

That makes the GCAR Assessment the classic liquidated damages

provision—a means of providing a definite recovery, negotiated in advance, to compensate for what would otherwise be an "indeterminate loss." Reply Br. 4. This assessment should not be dismissed as benefitting outsiders to Sally Beauty Supply's contractual relationship with Fifth Third, or Fifth Third's contractual relationship with Visa. The banks that will receive the Assessment in this case are no outsiders: They are stakeholders in the same network of relationships in Visa's payment network as Sally Beauty Supply and Fifth Third themselves. And the GCAR Program, together with the GCAR Assessment, undergird that entire network of relationships.

B. The GCAR Program and the GCAR Assessment also benefit the other stakeholders in Visa's card-payment network.

The GCAR Assessment does much more than simply provide compensation for the banks in Visa's networks and their customers. "Having fair and predictable rules that allocate responsibility for the financial impact of an account data compromise" protects *all* "stakeholders in the Visa payment system." *Visa GCAR Merchant Information*, *supra* at 1.

That of course includes Visa, because the GCAR Assessment plays a crucial role in protecting the network itself. The value of Visa's services depends on "the number of participants" in the network. *Ohio v. Am. Express Co.*, 138 S. Ct. 2274, 2281 (2018); *see also* CR61–62; 1SuppCR13; Visa Br. 44–

46. And providing adequate compensation for banks and their customers is critical to keep banks in the network and entice new banks to join. Accordingly, the strength of Visa's network rests on the assurance that the GCAR Assessment provides.

And even the merchants forced to pay the assessment obtain some benefits from it. The GCAR Assessment formula caps a merchant's liability, limiting not only the ultimate amount the merchant might be forced to pay, but also "limit[ing] liability … to a maximum window of time." *Visa GCAR Merchant Information*, *supra* at 1. The Assessment also "caps losses associated with operating expenses and catastrophic liability losses," further limiting merchant's liability. *Id.* And just as the Assessment saves banks the costs associated with data-breach litigation, it affords that same advantage to merchants too, allowing them to obtain a quick, efficient, and cost-effective settlement of their breach-related liabilities. Accordingly, the GCAR Program and the GCAR Assessment provide critical protections for everyone in Visa's network—merchants included.

II. Invalidating the GCAR Assessment will harm all stakeholders in Visa's card-payment-processing network.

By contrast, upholding the lower court's ruling invalidating the GCAR Assessment would present a serious, multi-faceted threat to Visa's payment

network. That result would dramatically increase the administrative burden on all participants within Visa's payment system and disrupt practices within the payment network that have continued for nearly a decade.

The issuing banks will have to trade the fairness and efficiency of the Assessment for the uncertainty and expense of litigation. That will mean the banks will be forced to pay more to recover less, and will be forced to absorb more unrecoverable losses from fraud. Those harms will drive issuing banks out of Visa's network, and will drive away potential cardholders too, when they find themselves unhappy with the remaining options for issuing banks.

Ultimately, all these harms will eventually trickle down to consumers. It will be consumers who are forced to absorb the unrecoverable losses from the bank's fraud-related losses—because banks' expenses are all eventually born by their customers and shareholders. It will be consumers who suffer the increased risk of card fraud that will result when merchants are no longer incentivized to follow good data management practices out of fear of paying a large assessment if they fail to do so. And it will be consumers who experience the diminished options and increased cost of credit and deposit accounts that will result if the Assessment is not restored.

These potential harms provide compelling reason to overturn the

invalidation of the GCAR assessment, and to reverse the trial court's judgment.

CONCLUSION

The Court should reverse the trial court's judgment.

Respectfully submitted,

/s/ J. Carl Cecere

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

Counsel for Amicus Curiae

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 3,809 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 2013 in 14-point Century Expanded BT font (and 13 point for footnotes).

/s/ J. Carl Cecere

J. Carl Cecere

CERTIFICATE OF SERVICE

I hereby certify that, on March 23, 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

CLYDE M. SIEBMAN
SIEBMAN FORREST BURG & SMITH LLP
Federal Courthouse Square
300 N. Travis
Sherman, Texas 75090
clydesiebman@siebman.com

SETH HARRINGTON
ORRICK, HERRINGTON & SUTCLIFFE LLP
222 Berkeley Street, Suite 2000
Boston, Massachusetts 02116
sharrington@orrick.com

CLAUDIA WILSON FROST
ORRICK, HERRINGTON & SUTCLIFFE LLP
609 Main Street, 40th Floor
Houston, Texas 77002
cfrost@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

/s/ J. Carl Cecere

J. Carl Cecere