No. 17-1705

**In the**
**Supreme Court of the United States**

PDR Network, LLC, *et al.*,
*Petitioners,*

v.

Carlton & Harris Chiropractic, Inc.,
*Respondent.*

**On Writ of Certiorari to the United States Court of Appeals for the Fourth Circuit**

**BRIEF OF**

# AMERICAN BANKERS ASSOCIATION, CONSUMER BANKERS ASSOCIATION AND INDEPENDENT COMMUNITY BANKERS OF AMERICA AS *AMICI CURIAE*

**IN SUPPORT OF RESPONDENT**


VIRGINIA O'NEIL
THOMAS PINDER
JONATHAN THESSIN
AMERICAN BANKERS ASSOCIATION
1120 Connecticut Ave., N.W.
Washington, DC 20036

CHARLES H. KENNEDY
(Counsel of Record)
1050 30th Street, NW
Washington, DC 20007
(202) 250-3704
ckennedy@kennedyonprivacy.com


February 14, 2019

## TABLE OF CONTENTS

*Page*

## TABLE OF CITED AUTHORITIES

*Page*

**Cases**

**Statutes**

**Other Authorities**

## INTERESTS OF *AMICI CURIAE*

American Bankers Association (ABA), Consumer Bankers Association (CBA) and Independent Community Bankers of America (ICBA) (collectively, the Associations) submit this brief as *amici curiae* in support of Respondent Carlton & Harris Chiropractic, Inc. (Respondent).[1]

ABA is an association representing the nation's $17 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard $13 trillion in deposits and extend nearly $10 trillion in loans.[2]

CBA is the trade association for today's leaders in retail banking — banking services geared towards consumers and small businesses. The nation's largest financial institutions, as well as many regional banks, are CBA corporate members, effectively holding two-thirds of the industry's total assets.

[1] Pursuant to Supreme Court Rule 37.6, no counsel for a party authored this brief in whole or in part, no such counsel or a party made a monetary contribution intended to fund the preparation or submission of this brief, and no person other than the *amici curiae* or their members made a monetary contribution to the preparation or submission of the brief.

[2] The Associations have obtained the written consent of the parties to file this *amicus* brief.

ICBA is an association that promotes an environment in which community banks can flourish. With more than 52,000 locations nationwide, community banks constitute 99 percent of all banks, employ more than 760,000 Americans and are the only physical banking presence in one in five U.S. counties.

The Associations' members will be directly affected by the Court's disposition of the issue presented in this case: *i.e.,* whether the Hobbs Act requires district courts to accept the Federal Communications Commission's (FCC) interpretations of the Telephone Consumer Protection Act (TCPA). The Associations' members must comply with TCPA requirements when they alert customers concerning questionable transaction requests, send notices of possible security breaches or engage in other vital customer communications. The Associations also are frequent participants in FCC and judicial proceedings that determine how TCPA requirements will be interpreted and enforced. The ability of the nation's banks to communicate effectively with their millions of customers will be impaired if district courts are empowered, contrary to the Hobbs Act, to adopt a patchwork of conflicting interpretations of TCPA obligations without regard to the authoritative rules issued by the FCC.

## SUMMARY OF ARGUMENT

Efficient, effective communications are essential if banks are to serve their customers and comply with their regulatory obligations. Financial institutions regularly seek to send time-critical, non-telemarketing communications to millions of customers promptly, including suspicious activity alerts, data security breach notifications, alerts to promote fee avoidance, and delinquency notifications. These consumer-protecting messages can be sent most efficiently and in compliance with the TCPA's requirements if financial institutions can design and follow uniform, nationwide compliance programs and have reasonable certainty that the programs will not be upended by a decision from a single federal district court.

The Hobbs Act provides banks and other regulated entities with that certainty. The Act places regulation of interstate telephone communications squarely in the hands of the FCC and prescribes a streamlined process for challenging that agency's final orders. If collateral attacks on FCC orders are permitted outside of the Hobbs Act framework, financial institutions will face perpetual uncertainty concerning their compliance obligations under the TCPA. The result will deprive TCPA regulation of its intended, nationwide uniformity, undermine financial institutions' compliance measures taken in reliance on FCC orders, and discourage vital

communications between financial institutions and their customers.

## ARGUMENT

### I. THE HOBBS ACT ENSURES A STABLE COMPLIANCE ENVIRONMENT THAT ENCOURAGES VITAL COMMUNICATIONS WITH CUSTOMERS OF THE NATION'S BANKS

The Hobbs Act provides an efficient, streamlined process for challenging the final orders of the FCC and certain other agencies. The Act vests the power to overturn such orders exclusively in the federal courts of appeals and confines such challenges to direct review petitions initiated within 60 days of the effective date of the challenged order. Administrative Orders Review Act, 28 U.S.C. §§ 2341-2352 (2012).

Unlike the judge-made *Chevron* doctrine — which requires that courts give deference to an agency's interpretation of a statute it is entrusted to administer — the Hobbs Act does not require the judicial branch to defer to agency action. Instead, the Act reflects Congress's considered view that certain agencies' actions should be accorded deference once an expedited review by a court of appeals has been

completed. This Court should not abrogate Congress's intent by permitting collateral attacks on orders of agencies encompassed within the Hobbs Act's framework. *See Chevron U.S.A., Inc. v. Nat. Res. Def. Council, Inc.,* 467 U.S. 837, 842-43 (1984); *see also United States Telecom Ass'n v. Fed. Commc'n Comm'n,* 855 F.3d 381, 417 (D.C. Cir. 2017) (Kavanaugh, J., dissenting).

By foreclosing perpetual, collateral attacks on orders that have been upheld by an appellate court or that have not been the subject of timely petitions for direct review, the Hobbs Act: (1) promotes judicial efficiency by avoiding multiple adjudications of the validity of the same agency action; (2) allows and gives effect to "uniform, nationwide interpretation of the federal statute by the centralized expert agency;" and (3) protects the legitimate interests of individuals and businesses that have made investment and compliance decisions in reliance upon agency orders. *Mais v. Gulf Coast Collection Bureau, Inc.,* 768 F.3d 1110, 1119 (11th Cir. 2014) (quoting CE Design, Ltd. v. Prism Bus. Media, Inc., 606 F.3d 443, 450 (7th Cir. 2010)); *see also Fla. Power & Light Co. v. Lorion,* 470 U.S. 729, 740 (1985); *cf. Perez v. Mortgage Bankers Ass'n,* 135 S. Ct. 1199, 1209 (2015) (affirming that regulated entities' "serious reliance interests" must be respected during the rulemaking process).

The uniformity and reliance interests protected by the Hobbs Act are especially critical to the efforts of banks to communicate with their customers in compliance with the FCC's orders interpreting the TCPA.

### A. Effective Customer Communications by Banks Require National Regulatory Stability and Uniformity

Of all the institutions with which people must stay connected, their banks are among the most vital. As described in greater detail below, banks send automated informational messages to prevent fraud and identity theft, provide notice of security breaches, provide low-balance and over-limit alerts, and help consumers avoid delinquency, among other purposes. For institutions to reach their customers today, these messages must increasingly be placed to mobile telephone numbers. Over 50% of U.S. households are now "wireless-only," with that percentage rising to over 70% for adults between 25 and 34 years of age. Stephen J. Blumberg & Julian V. Luke, U.S. Dep't of Health & Human Services, Ctr. for Disease Control & Prevention, Nat'l Ctr. for Health Statistics, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, July-December 2017* 5 -6 (2018) (Tables 1 & 2).

Many of the informational communications that banks place to their customers are time-

sensitive. To be valuable to the recipient, these calls must be placed immediately — using automated means, not manual dialing — and must be placed in compliance with the TCPA. That statute prohibits, with limited exceptions, financial institutions and other businesses from placing calls to their customers' mobile devices using specific dialing equipment — an "automatic telephone dialing system" (or autodialer) — unless the institution has the prior express consent of the called party. 47 U.S.C. § 227(b)(1)(A) (2012). The TCPA empowers the FCC to adopt regulations implementing this "prior express consent" requirement, including by delineating the type of automated dialing equipment that comprises an autodialer (and thus will subject a message to the TCPA's restrictions) and by specifying the means by which prior express consent may be obtained. *Id.* § 227(b)(2).

The stability and uniformity of the FCC's TCPA regulations are critical to ensuring that banks can place consumer-benefitting informational calls in a cost-efficient manner. If district courts are free to reject FCC regulations and substitute their own judgment for that of the agency, the nationwide regulatory uniformity mandated by the Hobbs Act and the TCPA will be lost. The resulting, fractured compliance environment will complicate and frustrate the efforts of financial institutions to convey

important information to their customers as efficiently as possible and in compliance with the TCPA. These vital communications include the following types of messages.

**a. Messages that Protect Consumers from Fraud and Identity Theft**

Protecting customers from fraud and identity theft is a high priority of the financial services industry. Financial institutions have made significant investments in fraud monitoring to identify suspicious activities and transactions and to respond with timely messages to customers that might be at risk. Among the activities and risk factors financial institutions monitor for these purposes are: (1) customer purchases that are unusual in kind for the customer, such as purchases in amounts, or in geographic areas or at types of merchants, that depart from the customer's established buying patterns; (2) sizes and types of transaction authorization requests that present a high likelihood of fraud, such as high-dollar transactions, ATM withdrawals and purchases of goods that can readily be converted to cash; (3) transaction requests involving geographic areas, merchants or merchant types that recently have experienced unusual levels of fraud; and (4) suspicious non-monetary activities, such as changes of address closely accompanied by requests for new payment cards, and requests for new online

credentials, coupled with evidence of malware or phishing attacks.[3]

The volume of these required notifications, which average 300,000 to 400,000 messages per month for one large bank alone, cannot be accomplished at all, much less with acceptable speed, unless the process is automated. Manual calls placed in these circumstances would come too late to prevent harm to the customer, and probably would not even be attempted because of their sheer impracticality.

Financial institutions also are required, under the Fair Credit Reporting Act, to verify a customer's identity before authorizing the establishment of any new credit plan or extension of credit where a fraud alert has been placed on the customer's credit reporting agency file. Fair Credit Reporting Act § 605A, 15 U.S.C. § 1681c-1 (2012). Financial institutions rely on the efficiency of automated dialers and other automation technologies to contact these customers quickly, with the goal of verifying identity and immediately accommodating the customer's

[3] The Red Flags Rule, adopted by the Federal Trade Commission and other federal regulators of financial institutions, prohibits a card issuer from complying with a request for an additional or replacement card that follows less than 30 days after an address change, until it has notified the cardholder of the request. *See, e.g.,* 16 C.F.R. § 681.3 (2018).

request. For those customers who can most efficiently be contacted at mobile telephone numbers, the institution's inability to use automated calling methods is likely to delay the bank in contacting the customer or member, resulting in embarrassment — or worse — for those individuals.

**b. Data Security Breach Notifications**

Section 501(b) of the Gramm-Leach-Bliley Act, as well as the data security breach notification statutes of the 50 states and the District of Columbia, require financial institutions to establish response and customer notification programs to be implemented following any unauthorized access to customers' personal information. Gramm-Leach-Bliley Financial Services Modernization Act of 1999, Pub. L. No. 106-102, § 501(b), 113 Stat. 1338, 1436-37 (1999); *see, e.g.,* Cal. Civ. Code § 1798.29 (West); 815 Ill. Comp. Stat. Ann. 530/10(a) (West); N.Y. Gen. Bus. Law § 899-aa (McKinney); N.C. Gen. Stat. Ann. § 75-65 (West); Wash. Rev. Code Ann. § 19.255.010 (West). Those statutes permit the required notifications to be made by telephonic or electronic means. *See* Ark. Code Ann. § 4-110-105 (West); Conn. Gen. Stat. Ann. § 36a-701 (West); Del. Code Ann. tit. 6, § 12B-102(a) (West); Ga. Code Ann. § 10-1-912 (West); Haw. Rev. Stat. Ann. § 487N-2 (West); Idaho Code Ann. § 28-51-105 (West); 815 Ill. Comp. Stat. Ann. 530/10(a) (West);

La. Stat. Ann. § 51:3074; Minn. Stat. § 13.055; Mont. Code Ann. § 30-14-704; N.J. Stat. Ann. § 56:8-163 (West).

Over 1,244 data security breaches were publicly reported in the United States in 2018 alone, compromising the security of 446,515,334 personal records — an increase in the number of records breached of 126 percent over the number of records breached in 2017. Identity Theft Resource Center, 2018 End-of-Year Data Breach Report, https://www.idtheftcenter.org/2018-end-of-year-data-breach-report (last visited Feb. 7, 2019).

The banking, credit, and financial industry accounted for only 11% of all reported breaches during 2018. *Id.* Although most data breaches occur at entities far removed from the banking sector, financial institutions recognize that it is their customers who must be protected. Accordingly, upon learning of any data breach at a retailer, healthcare provider or other organization that potentially affects an institution's customers, the financial institution immediately seeks to contact customers to notify them of the breach and of any remedial action to be taken.

As a result, financial institutions deal in a high volume of data security breach notifications. A single financial institution might be responsible for 50,000

to 60,000 or more potential data security breach notifications per month.

Like fraud and identity theft alerts, breach notification alerts must be timely and reliable. As with fraud and identity theft alerts, the volume of data security breach notifications — both in terms of the numbers of reportable incidents and the numbers of affected customers that must be notified — necessitates the use of automated dialing if the required notices are to be sent in timely and effective fashion.

**c. Remediation Messages**

Closely related to data security breach notification messages are notices to customers concerning measures they may take to prevent identity theft resulting from a breach, such as placing fraud alerts on their credit reports and subscribing to credit monitoring services. In many notable security breach cases, affected institutions have offered to cover the costs of such services for consumers.

**d. Calls to Distressed and Delinquent Borrowers**

Banks seek to place calls to distressed or delinquent mortgage, credit card, or other borrowers. These calls are consumer-protecting communications designed to establish live contact with the borrower.

It is well-established that the earlier a creditor is able to communicate with a financially distressed borrower, the more likely the creditor will be able to offer the borrower a loan modification, interest rate reduction, forbearance on interest and fees during a temporary hardship or disaster, or other alternative that will help limit avoidable late fees, interest charges, negative credit reports, and, where appropriate, repossession of the collateral or foreclosure. *See* Bureau of Consumer Financial Protection, Comment Letter on FCC's Interpretation of the Telephone Consumer Protection Act 1 (June 13, 2018), https://ecfsapi.fcc.gov/file/10613092630663/BCFP%20comment%20to%20FCC%20on%20TCPA.pdf. ("Consumers benefit from communications with consumer financial products providers in many contexts, including . . . notifications about their accounts.") Mortgage servicing regulations, which require that servicers place calls with prescribed frequencies, reflect the well-established public policy goal of initiating conversations with financially distressed borrowers early in the delinquency in order to prevent foreclosure. Truth in Lending (Regulation Z), 12 C.F.R. pt. 1024 (2018).

### B. Banks Have Instituted Costly and Extensive Compliance Procedures based upon the Hobbs Act Framework

As described above, the Hobbs Act channels judicial oversight of FCC orders into a defined process with a clear end point. In so doing, the Act permits affected parties to invest with reasonable confidence in measures designed to comply with those orders. As this Court has recognized, protection of such reliance interests is a legitimate goal of the regulatory process. *Perez v. Mortg. Bankers Ass'n,* 135 S. Ct. 1199, 1209 (2015); *Fed. Commc'n Comm'n v. Fox Television Stations,* 556 U.S. 502, 515 (2009).

In the 28 years since the TCPA was enacted, the FCC has issued a substantial body of regulations, orders and declaratory rulings that implement and interpret the TCPA's requirements. Relying upon the regulatory stability ensured by the Hobbs Act, financial institutions have made investment and compliance decisions based upon FCC orders that were not overturned pursuant to timely petitions for review.

A notable example of financial institutions' reliance on FCC orders that have withstood the Hobbs Act review process is the FCC's rule concerning how consumers may provide prior express consent to receive autodialed communications on their mobile

devices. Because the TCPA requires "prior express consent" but does not specify the means by which that consent may be given, banks and other businesses faced uncertainty in their early efforts to comply. In an order entered in 1992, the FCC held that "persons who knowingly release their phone numbers have in effect given their invitation or permission to be called at the number which they have given, absent instructions to the contrary;" and that, accordingly, callers "will not violate our rules by calling a number which was provided as one at which the called party wishes to be reached." *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991,* 7 F.C.C. Rcd. 8752, 8769 (1992).

This "provided-number" rule, which the FCC has reaffirmed in subsequent orders, has guided banks in their documentation of many millions of consumer accounts over the decades since the rule was adopted.[4] In reliance on that rule, financial

[4] *See In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, Request of ACA International for Clarification and Declaratory Ruling*, 23 F.C.C. Rcd. 559, 563 (2008). In a later decision, the FCC found that autodialed marketing – as opposed to informational – calls placed to mobile devices may be placed only with the prior express *written* consent of the called party. *In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, 27 F.C.C. Rcd. 1830, 1840 (2012). However, the FCC has not changed its rule concerning the form by which prior express consent may be provided for autodialed informational calls placed to mobile numbers.

institutions have asked account applicants to furnish contact telephone numbers, and have used those contact numbers to send suspicious transaction alerts, data security breach notifications and other informational communications over the course of those account relationships. One large bank reports that its cost to build a centralized infrastructure to capture and store customers' prior express consents in compliance with the TCPA is approximately $6 million, and that its annual expenditures to maintain that infrastructure and process are approximately $7.2 million. Other financial institutions have made investments and incurred expenses of similar magnitude, varying with their size and the scope of their operations.

Financial institutions also have trained millions of customer support, call center and marketing personnel on the TCPA and the institution's compliance procedures. The bank referenced above reports that it spends between $1.1 million and $1.5 million annually to train its employees in TCPA compliance. Each of the Associations' members incur such TCPA training costs.

The Hobbs Act has protected these reliance interests against collateral attack. For example, in 2008 a district court rejected the FCC's provided-number rule, concluding that a customer's act of

furnishing a mobile contact number to a creditor did not support the creditor's subsequent collection calls to that number. In a later order, the court vacated its decision on the ground that the Hobbs Act did not permit it to "enjoin, set aside, suspend . . . or determine the validity of" the FCC's final order adopting the provided-number rule. *Leckler v. Cashcall, Inc.,* 554 F.Supp. 2d 1025 (N.D. Cal. 2008), *vacated*, No. C 07-04002 SI, 2008 WL 5000528, *1 (N.D. Cal. Nov. 21, 2008). More recent court decisions also have applied the Hobbs Act to reject collateral attacks on the provided-number rule. *See Mais v. Gulf Coast Collection Bureau, Inc.,* No. 11-61936-Civ, 2013 WL 11941572, at *1 (S.D. Fla. May 23, 2013), *rev'd,* 786 F.3d 1110 (11th Cir. 2014).

A second example of actions taken in reliance on the FCC's TCPA rules involves the definition of an autodialer, the use of which requires prior express consent if a call is placed to a mobile number. 47 U.S.C. § 227(a)(1) (2012). The FCC has adopted a number of orders interpreting the statute's autodialer definition, and banks have invested many millions of dollars in equipment purchases and employee training in reliance on those orders. *See, e.g., In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991,* 30 F.C.C. Rcd. 7961, 7971-78 (2015) (interpreting the statutory definition of an autodialer). Many financial institutions have disagreed with the FCC's interpretation of the

autodialer definition, which was rejected in a 2018 decision of the United States Court of Appeals for the District of Columbia Circuit (following Hobbs Act procedures) and is the subject of a pending FCC remand proceeding. *ACA Int'l v. Fed. Commc'n Comm'n,* 885 F.3d 687 (D.C. Cir. 2018). However, financial institutions continue to rely upon the stability of the Hobbs Act process to ensure that any changes to the FCC's interpretation of the statutory definition will have the finality needed to support investment and compliance decisions taken in the future.

## II. REMOVAL OF HOBBS ACT CONSTRAINTS WILL ADVERSELY AFFECT MILLIONS OF BANK CUSTOMERS NATIONWIDE

The importance of the Hobbs Act to TCPA compliance can be measured against the backdrop of the constant, crushing volume of TCPA class-action complaints. TCPA litigation increased by 46% in the 17 months since the FCC issued its 2015 Declaratory Ruling and Order interpreting the autodialer definition, as compared with the preceding 17-month period. U.S. Chamber of Commerce Institute of Legal Reform, *TCPA Litigation Sprawl: A Study of the Sources and Targets of Recent TCPA Lawsuits* 2 (Aug. 2017), https://www.instituteforlegalreform.com/research/tcp

a-litigation-sprawl-a-study-of-the-sources-and-targets-of-recent-tcpa-lawsuits. Between 2010 and 2016, there was a 1,273% increase in TCPA litigants. Josh Adams, ACA Int'l, *Unintended Consequences of an Outdated Statute: How the TCPA Fails to Keep Pace with Shifting Consumer Trends* 2 (May 2017) (emphasis omitted). These complaints invariably seek statutory damages of $1,500 per alleged violation rather than compensation for actual harm. *See Bais Yaakov of Spring Valley v. Fed. Commc'n Comm'n,* 852 F.3d 1078 (D.C. Cir. 2017) (Kavanaugh, J.), *cert. denied,* 138 S. Ct. 1043 (2018).

At any given time, hundreds of such lawsuits are working their way through the district courts, and the merits of those claims often hinge upon the application of FCC orders to the alleged facts. For example, plaintiffs may claim not to have given prior express consent to receive autodialed calls or argue that the equipment used to place a disputed call met the definition of an autodialer under the TCPA. Some parties to these lawsuits continue to argue that the district court should substitute its own judgment for that of the FCC, and that the court should reject FCC regulations and orders that otherwise would provide a clear path to resolution of the questions presented. A decision for the petitioner in this case would open the flood gates to district court second-guessing of the expert agency charged by Congress with implementation and enforcement of the TCPA. The

inevitable result would be to harm the interests of millions of financial institution customers. Faced with the loss of stable FCC rules concerning their TCPA compliance obligations, and threatened with vexatious lawsuits based upon a patchwork of conflicting district court decisions, financial institutions might have no choice but to cease sending many of the millions of automated informational alerts that customers have come to expect.

Substitution of manual communication methods would impose extensive costs as well as degradation in customer service. For example, one large institution reports that it sent 760,788,302 automated customer text messages in 2018, and that sending those messages manually rather than by automated means would have raised the cost of those communications by an estimated $287,577,978.

A community bank reports that communications involving 120,000 to 180,000 customer accounts would be adversely affected if automated fraud prevention messages could not be sent in reliance upon current FCC rules. Between 50% and 80% of that bank's accounts have mobile telephone numbers recorded as the customers' preferred mode of contact. The bank currently is investing in a program of text messaging to report suspicious transaction requests, according to which the bank would send a code that the customer could

return to the bank as confirmation of the request. If the bank no longer could use the customer's act of providing a mobile contact number as the basis for those messages, the program could not go forward except after a long and costly process of obtaining new consents, or by sending the texts manually at enormous cost and loss of efficiency. The bank reports that this prospect likely would require this valuable customer-protection program to be abandoned.

As these examples show, loss of the regulatory stability afforded by the Hobbs Act inevitably would raise customers' costs of banking services, and degrade or prevent valuable communications, with no offsetting customer benefit.

## CONCLUSION

The Hobbs Act is an indispensable source of regulatory stability for those affected by decisions of the agencies to which it applies, and particularly for those subject to the TCPA and the implementing

orders of the FCC. The Court should reject Petitioners' suggestion that district courts are free to ignore the Hobbs Act and may entertain perpetual, collateral attacks on final agency orders.

VIRGINIA O'NEIL
THOMAS PINDER
JONATHAN THESSIN
AMERICAN BANKERS ASSOCIATION
1120 Connecticut Ave., N.W.
Washington, DC 20036

CHARLES H. KENNEDY
(Counsel of Record)
1050 30th Street, NW
Washington, DC 20007
(202) 250-3704
ckennedy@kennedyonprivacy.com

February 14, 2019