The Consumer Finance Observer

A periodic update on legal developments in consumer finance — Fall 2019

IN THIS ISSUE:

Regulators Continue to Focus on the Use of Alternative Data

Michael W. Ross

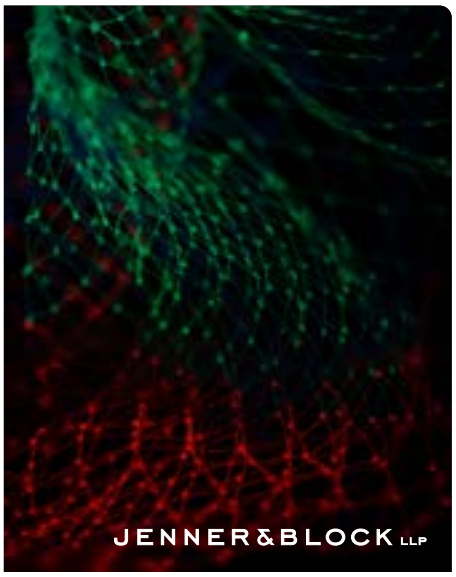
In an article published in the inaugural edition of *The Consumer Finance Observer*, our lawyers highlighted the increasing focus of government enforcement authorities on how companies are using "alternative data" in making consumer credit decisions. For example, the article highlighted that – as stated in a June 2019 fair lending report from the Consumer Finance Protection Bureau (CFPB) – "[t]he use of alternative data and modeling techniques may expand access to credit or lower credit cost and, at the same time, present fair lending risks." Regulators have continued to focus on this area, including on the benefits and risks of using alternative data in lending decisions.

In August 2019, the CFPB posted a widely reported-on blog entry on the benefits of using alternative data in lending decisions. The CFPB blog post provided an update to the public on the agency's first and only no-action letter, issued to Upstart Network, Inc. in 2017. In that letter, the CFPB stated it had no intention of taking action against Upstart under the Equal Credit Opportunity Act (ECOA), which prohibits discrimination in lending, for using certain alternative data sources – particularly information about a borrower's education and employment history – to make credit decisions. To obtain that letter, Upstart committed to implementing a risk management and compliance plan that included a process for analyzing the potential risk that its use of alternative data could lead to impermissible discrimination against protected classes of consumers.

The CFPB's blog post reported on the results of Upstart analyzing almost two years of data from its risk management process. Its data showed that Upstart's model approved 27 percent more applicants than would have been approved by a traditional underwriting model (i.e., one that did not use alternative data and machine learning), and led to 16 percent lower average APRs for approved loans. The CFPB also reported that expansion of credit occurred "across all tested race, ethnicity, and sex segments," and resulted in particular increases in approval among applicants under 25, those with incomes under $50,000, and those with "near prime" credit scores.[1] These results hearken back to a report by the Philadelphia Federal Reserve in 2017 concluding that the use of alternative data in credit decisions (in that case, relying on data from another FinTech lender, Lending Club) expanded access to credit in underserved areas at a lower cost than would otherwise be available.

The news of Upstart's results was widely reported, as the use of alternative data in consumer lending remains a hot topic that regulators and legislators are continuing to watch closely.

[1] Government agencies and legislators also continue to focus on the potential risks of alternative data. In June, for example, Senators Elizabeth Warren and Doug Jones wrote a letter to various government regulators highlighting concerns that using algorithms in underwriting decisions could lead to unlawful discriminatory lending practices.



Five Best Practices to Avoid TCPA Wrong-Number Claims

Amy M. Gallegos

On July 10, 2019, the district court in the Northern District of Illinois preliminarily approved a settlement in which Wells Fargo agreed to pay $17.85 million to settle a nationwide class action alleging violations of the Telephone Consumer Protection Act (TCPA). The complaint alleged that Wells Fargo had sent automated calls and texts that were intended for accountholders to "wrong parties"—i.e., consumers who were not actually the accountholders Wells Fargo was attempting to reach. The settlement class encompasses individuals who received calls from Wells Fargo in connection with collecting or servicing of loans or accounts, or fraud alert notifications, via "any automated dialing technology or artificial or prerecorded voice technology."[1] Notably, the settlement class only includes people who were *not* customers of Wells Fargo at the time of the call.[2]

Wrong-party calls are a thorn in the side of even the most scrupulous TCPA compliance programs. Reassigned numbers are a significant problem: According to the FCC, approximately 35 million numbers are disconnected and made available for reassignment to new consumers each year. Yet, historically, there has been no comprehensive and timely way for callers to determine whether a number has been reassigned. Wrong number calls can be the result of innocent mistakes—a consumer accidentally types the wrong number into an online form or forgets to update all of his accounts when he changes numbers. Consumers with delinquent debts may change their numbers to dodge creditors, sticking the new owners of those numbers with their debt-collection calls. Professional plaintiffs have developed strategies to draw wrong number calls, in hopes of collecting the $500 to $1,500 per call penalties available under the TCPA. Maintaining accurate records of wrong numbers can be challenging as well. In the debt collection context, for example, it is not unusual for the debtor to falsely tell the caller that he has the wrong number. Many consumers do not answer calls from numbers they do not recognize and do not bother to opt out of text messages they did not request, meaning that businesses can accidently send multiple calls or texts to the wrong party without ever having a reason to suspect that the number being dialed is incorrect.

The FCC has stepped in to address this problem—but help is still a ways away. In December 2018, the FCC issued an order creating a single, comprehensive database that will contain reassigned number information from providers in North America. The order also created a safe harbor for callers who relied upon the database. Once the database becomes operational, callers who wish to avail themselves of the safe harbor must demonstrate that they appropriately checked the most recent update of the database and the database reported "No" when given either the date they contacted that consumer or the date on which the caller could be confident that the consumer could still be reached at that number. The safe harbor would then shield the caller from liability should the database return an inaccurate result. The database is in the process of being implemented and there is no established completion date.

For a long time, the conventional wisdom among TCPA practitioners was that protection against wrong-party TCPA class actions was best found in Rule 23. A "wrong number" class could not be certified, the reasoning went, because there would be no feasible way to identify the class members—i.e., the people on the other end of the line of a business's wrong-number calls. Individual inquiries would be required to identify wrong number calls and determine who received them, running afoul of Rule 23's predominance requirement and/or some circuits' requirements that a class be "ascertainable." However, although most courts still refuse to certify wrong-party classes, over the past few years, a few courts have become more receptive, blessing complex schemes to identify class members that involve hunting down call recipients using the caller's phone records, subpoenas to cellular and wireless carriers, reverse-lookup services, and class member affidavits. Moreover, as more and more companies have shored up their consent regimes, securing and documenting consent from their customers and account holders to receive autodialed calls and texts, wrong party calls are likely now perceived to be more lucrative by the plaintiffs' bar since most wrong parties will not have provided consent.

Contineud on page 3

As the Wells Fargo settlement illustrates, it is now more important than ever for businesses to ensure that their TCPA compliance programs include measures to avoid wrong-number calls. So what steps should businesses consider taking to accomplish this seemingly impossible task?

1. ***IMPLEMENT PROCEDURES FOR LOGGING AND DEACTIVATING WRONG NUMBERS.*** Repeat calls to wrong numbers create terrible optics in TCPA litigation. Courts are less likely to certify a wrong-party class if the evidence shows that the caller took reasonable steps to avoid wrong-party calls and stopped dialing numbers they knew or had reason to know were wrong. It is critical for companies to implement recordkeeping systems that allow for the logging and automatic deactivation of wrong numbers. Of course, there is no way to guarantee that a person who answers the phone and informs the caller he has the wrong number is telling the truth. However, given the high cost of TCPA exposure, it will in most cases make sense to take the consumer at his word.

2. ***REQUIRE CUSTOMERS TO PROVIDE A VERIFIED PHONE NUMBER AS A CONDITION OF OPENING AN ACCOUNT OR ACCESSING SERVICES AND BUILD NUMBER VERIFICATION INTO MULTIPLE CUSTOMER CONTACT POINTS.*** Businesses can ensure that customers provide accurate telephone numbers by requiring a verified telephone number as a condition of opening an account or accessing a service. Many lenders, banks, and other service providers are already requiring a verified phone number due to the rise of to-factor authentication. Companies can then maximize their ability to capture updated data by confirming contact information whenever they communicate with the customer. For example, businesses that interact with customers via call centers could instruct representatives to confirm or update the customer's contact information on every call. Businesses like financial institutions or retailers that offer services online should consider asking that customers confirm or update their contact information upon login. Email can be used to confirm customers' contact information and request updates. Reminding customers to keep their contact information up to date will reduce the risk that consumers will forget to update their contact information when they change phone numbers.

3. ***INCORPORATE EASY OPT-OUT OPTIONS FOR CALLS AND TEXTS.*** Make it easy for recipients of wrong party calls to opt out of future communications. Businesses that send texts to consumers should include in each message a notification that the recipient can opt out of future clicks by responding "STOP." Businesses that deliver prerecorded messages to consumers—for example, pharmacies informing consumers about prescription status or service providers warning consumers about late payments—should consider incorporating an option allowing call recipients to opt out of future calls via an IVR system.

4. ***USE A SERVICE TO UPDATE CONTACT INFORMATION AND SCRUB FOR REASSIGNED NUMBERS.*** A number of vendors such as LexisNexis and TransUnion offer services to update and verify consumer data. Some vendors offer reassigned number scrubbing, though it is unclear how effective these tools are in practice. Of course, there is always a risk that third party-provided data may be inacccurate that has to be weighed against the risk that the consumer-provided numbers have been reassigned or are otherwise inaccurate.

5. ***CONSIDER MANUALLY CALLING HARD-TO-REACH CONSUMERS.*** If practicable, in cases where the same number has been called numerous times without achieving right-party contact, consider dialing the number manually. Manual dial will allow the agent to listen to the voice mail to see if the name in the voicemail matches the consumer the company is trying to reach.

All of these options will not work for every business. However, as the Wells Fargo settlement illustrates, the risk of TCPA liability for wrong-party call is real and substantial. The best way to mitigate that risk is with a strong TCPA compliance program.

This article was first published by Law360 on July 30, 2019.

DC Court Again Dismisses Challenge to OCC's FinTech Charter

William S. C. Goldstein

On September 3, 2019, a federal district court in the District of Columbia dismissed, for the second time, a lawsuit brought by the Conference of State Bank Supervisors (CSBS) seeking to block the Office of the Comptroller of the Currency (OCC) from issuing national bank charters to certain non-bank financial technology (FinTech) companies. *Conference of State Bank Supervisors v. Office of the Comptroller of the Currency*, No. 18-cv-2449, 2019 WL 4194541 (D.D.C. Sept. 3, 2019) (*CSBS II*). CSBS's earlier suit, brought in 2017, was previously dismissed by Judge Dabney Friedrich as premature: Because OCC had not yet finalized its procedure for accepting FinTech charter applications, let alone received any applications, Judge Friedrich found that CSBS's claims were unripe and alleged no injury sufficient for standing. *CSBS v. OCC*, 313 F. Supp. 3d 285, 296-301 (D.D.C. 2018). In October 2018, CSBS brought suit again—this time after OCC had finalized its procedures for accepting FinTech charter applications, albeit before OCC had actually received any applications. *CSBS II*, 2019 WL 4194541, at *1. Judge Friedrich held that neither this change nor the Senate's confirmation of Joseph Otting as Comptroller of the Currency, another change in the facts highlighted by CSBS, "cure[s] the original jurisdictional deficiency." *Id*. (alteration in original; citation omitted). The court pointedly explained that "it will lack jurisdiction over CSBS's claims at least until a Fintech applies for a charter." *Id*. at 3.

In dismissing CSBS's suit for lack of standing, Judge Friedrich found herself in disagreement with Judge Victor Marrero of the Southern District of New York. Judge Marrero held in May of this year, on a very similar record, that the New York State Department of Financial Services (DFS) had standing to challenge OCC's FinTech plans—and that DFS was right on the merits, essentially blocking OCC from issuing FinTech charters. *See Vullo v. OCC*, 378 F. Supp. 3d 271 (S.D.N.Y. 2019). Judge Friedrich "respectfully disagree[d] with *Vullo*, to the extent that its reasoning conflicts with either this opinion or *CSBS I*." *CSBS II*, 2019 WL 4194541, at *1 n.2. The heart of the divergence seems to be Judge Friedrich's conclusion that there could be no jurisdiction at least until OCC received a charter application. *Id*. at *3. Judge Marrero, by contrast, found that OCC "has the clear expectation of issuing [FinTech] charters" and thus that "DFS has demonstrated a 'substantial risk that harm will occur.'" *Vullo*, 378 F. Supp. 3d at 288 (citation omitted). Due to that difference of opinions, CSBS will have to wait at least until a FinTech company applies for a charter before filing again. Such an application may not be forthcoming, as the SDNY's ruling may keep any FinTech companies from applying for a charter in the near future, given the legal uncertainty. The parties in Vullo submitted competing proposals for the language of a final judgment, presumably in order to allow for OCC to take an appeal to the Second Circuit; the court adopted DFS's proposal and issued a final judgment on October 23, 2019. See Amended Final Judgment, Lacewell v. OCC, No. 18-cv-8377 (S.D.N.Y. Oct. 23, 2019), ECF No. 45; see also ECF Nos. 39-41.

FTC Monitoring of Class Action Settlements

Joseph L. Noga

The Federal Trade Commission (FTC) and its Class Action Fairness Project regularly monitor and analyze class actions and class action settlements with a view toward whether appropriate benefits are provided to consumers. In September, the staff issued "Consumers and Class Actions: A Retrospective and Analysis of Settlement Campaigns," a report which analyzed 140 consumer class action settlements handled by large class action administrators and the results from an internet-based consumer research study conducted by the staff to explore consumer understanding of class action notices (particularly certain phrasing and language provided by email). *See* ftc.gov/reports/consumers-class-actions-retrospective-analysis-settlement-campaigns. In the study of class administrator data, it was noted that the median calculated claims rate for settlements was nine percent; 86 percent of claims were approved and objection and exclusion rates were "miniscule." In the consumer research study, the staff found that the phrasing of email subject lines and other information may help notice campaigns reach more class members and should be the subject of further research. The staff report concluded by stating that there may simply be a need for broad-based consumer education about the potential monetary benefits of opting-in to a settlement class.

The FTC continued the discussion on these issues at a workshop on October 29, 2019, at the Constitution Center in Washington, DC that was open to the public and webcasted live. *See ftc.gov/news-events/audio-video/video/consumers-class-action-notices-ftc-workshop*. Through November 22, 2019, interested parties may submit public comments, either through Regulations.gov, or by mail to Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue N.W., Suite CC-5610 (Annex B), Washington, DC 20580. The re line should be "Class Action Notices, Project No. P024210."

Second Circuit Addresses Cross-Jurisdictional Class Action Tolling

Gabriel K. Gillett and Katherine Rosoff

On August 7, 2019, the Second Circuit certified two questions to the New York Court of Appeals with broad implications for multi-jurisdictional class actions. First, "whether New York recognizes 'cross-jurisdictional class action tolling,' i.e., tolling of a New York statute of limitations by the pendency of a class action in another jurisdiction." *Chavez v. Occidental Chem. Corp.*, -- F.3d. --, 2019 WL 3673190, *1 (2d Cir. Aug. 7, 2019). Second, "whether non-merits dismissal of class certification can terminate class action tolling" when dismissal included a "return jurisdiction" clause allowing the plaintiffs to renew their claims if they were unable to find an adequate forum in their home countries. *Id*.

The case was brought by agricultural workers from Costa Rica, Ecuador and Panama, alleging they suffered adverse health effects from a pesticide used on banana plantations. The parties agree that their claims accrued no later than August 1993 and are subject to New York's three-year statute of limitations in personal injury actions. However, the parties dispute whether plaintiffs' claims were tolled by related actions filed in other jurisdictions.

Judge Sack, writing for Judges Raggi and Carney, found no clear case law on whether New York State would recognize cross-jurisdictional class action tolling. The panel explained that, although New York has adopted the federal rule from *American Pipe Construction Co. v. Utah*, 414 U.S. 538 (1974) that allows for class-action tolling, New York state courts have not determined whether New York would apply that rule to class actions in other jurisdictions. Courts within the Second Circuit that have been tasked with predicting New York's ruling on the issue are split. *See, e.g., Chavez*, 2019 WL 3673190, at *7 n.5. So too, the Second Circuit recognized, are courts in other states that have faced the same issue. *Id*.

Faced with a thorny question of state law, the Second Circuit asked the New York Court of Appeals to weigh in. *See* Second Circuit Local Rule 27.2; 22 NYCRR § 500.27. On August 29, the Court of Appeals accepted the Second Circuit's questions and ordered the parties to brief and argue the case. At present, the issues are scheduled to be fully briefed by the end of January and argument will occur thereafter.

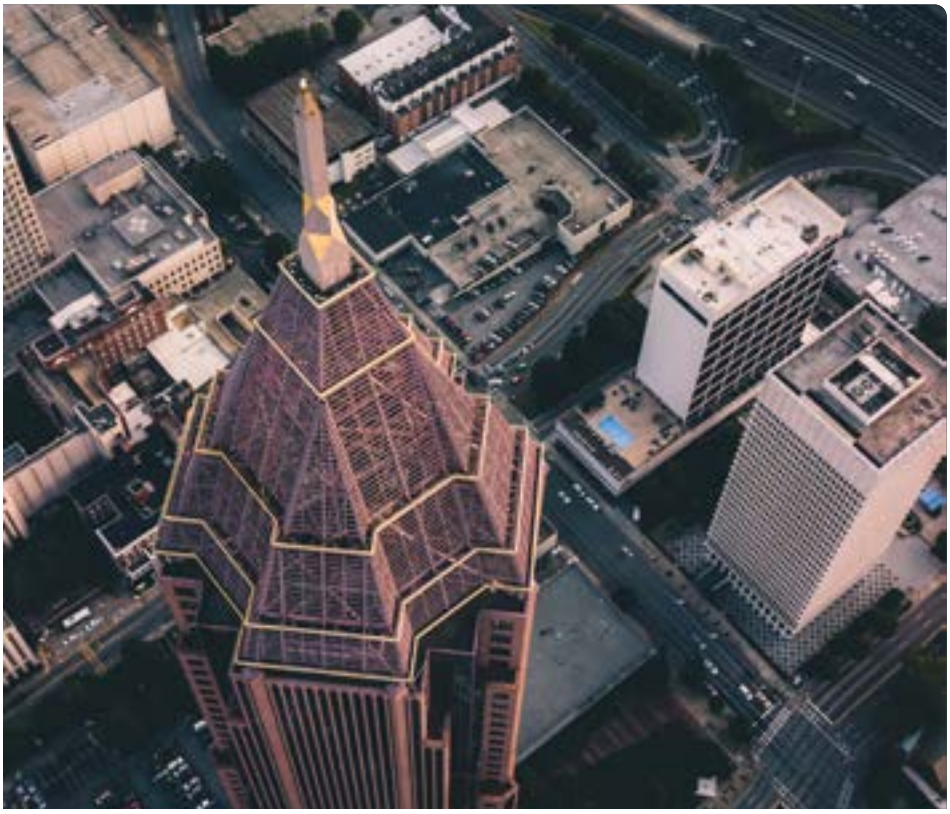
Eleventh Circuit Rules in TCPA Case

Olivia Hoffman

The Eleventh Circuit recently decided a case that raised the bar for pleading injury under the Telephone Consumer Privacy Act (TCPA), 47 U.S.C. § 227, noting its disagreement with an earlier decision from the Ninth Circuit on the same issue and creating a possible roadblock for future plaintiff classes seeking to assert claims under the TCPA.

In *Salcedo v. Hanna*, the Eleventh Circuit held that "receiving a single unsolicited text message" in violation of the TCPA was not a "concrete injury" sufficient to confer standing on the plaintiff.[1] The case arose out of a text message that plaintiff John Salcedo received from his former lawyer, defendant Alex Hanna, offering Salcedo a discount on Hanna's services. According to Salcedo, receiving the text message "caused [him] to waste his time answering or otherwise addressing the message" and "resulted in an invasion of [his] privacy and right to enjoy the full utility of his cellular device."[2] Salcedo filed a class action complaint in the Southern District of Florida on behalf of a class of former clients of Hanna who had received similar unsolicited text messages. Salcedo demanded statutory damages of $500 per text message and treble damages of $1,500 per text message for knowing or willful violations of the statute.

The case went up to the Eleventh Circuit on interlocutory appeal. The court held that Salcedo's receipt of a single unwanted text message from his former lawyer was not a concrete injury for the purpose of Article III. It distinguished other unsolicited, one-off communications that have sufficed to confer standing, such as a junk fax—which, the court noted, rendered the plaintiff's fax machine "unavailable for legitimate business messages" for "a full minute" and also used the plaintiff's paper and ink.[3] Here, by contrast, Salcedo had failed to allege that the text message cost him any money or interfered with his use of his cellular phone for a specific amount of time. The court also observed that not only is the TCPA silent on text messages, but "the receipt of a single text message is qualitatively different from the kinds of things Congress was concerned about when it enacted the TCPA," which involved more serious privacy and nuisance issues.[4] Ultimately, the court concluded that the receipt of a single text message, while perhaps "[a]nnoying," was "not a basis for invoking the jurisdiction of the federal courts."[5]



In reaching this conclusion, the Eleventh Circuit explicitly rejected the reasoning of the Ninth Circuit—the only other circuit to directly address the issue of whether receipt of a text message, on its own, constitutes injury under the TCPA—in a similar case. Indeed, in *Van Patten v. Vertical Fitness Group, LLC*, the Ninth Circuit held that unwanted text messages implicate the same kinds of concerns as unsolicited calls, reasoning that the receipt of unwanted telemarketing text messages "present[s] the precise harm and infringe[s] the same privacy interests Congress sought to protect in enacting the TCPA."[6]

The Eleventh Circuit's opinion in *Salcedo* does not impose a *per se* bar on TCPA claims based on the receipt of unsolicited text messages. Rather, it requires plaintiffs pleading claims under the TCPA to allege a "particular loss of opportunity," or to allege "specifically" that the defendant's text message cost them money or deprived them of the use of their device for a period of time.[7] Under this framework, the question of whether an individual has suffered a concrete injury sufficient to confer standing is a highly individualized and fact-specific inquiry. As a result, as some commentators have noted, plaintiffs seeking to assert claims under the TCPA on behalf of a class may struggle to establish, for example, that the questions of law or fact common to the class members predominate, or that a class action is a superior vehicle for resolving the dispute.[8]

[1] *Salcedo v. Hanna*, No. 17-14077, 2019 WL 4050424, at *1 (11th Cir. Aug. 28, 2019).

[2] *Id*. at *3.

[3] *Id*. at *3-*4.

[4] *Id*. at *4.

[5] *Id*. at *7.

[6] 847 F.3d 1037, 1043 (9th Cir. 2017).

[7] 2019 WL 4050424, at *3-*4.

[8] See Fed. R. Civ. P. 23.

A Quick Look at HUD's FHA Lender Annual Certification Statements

Damon Y. Smith

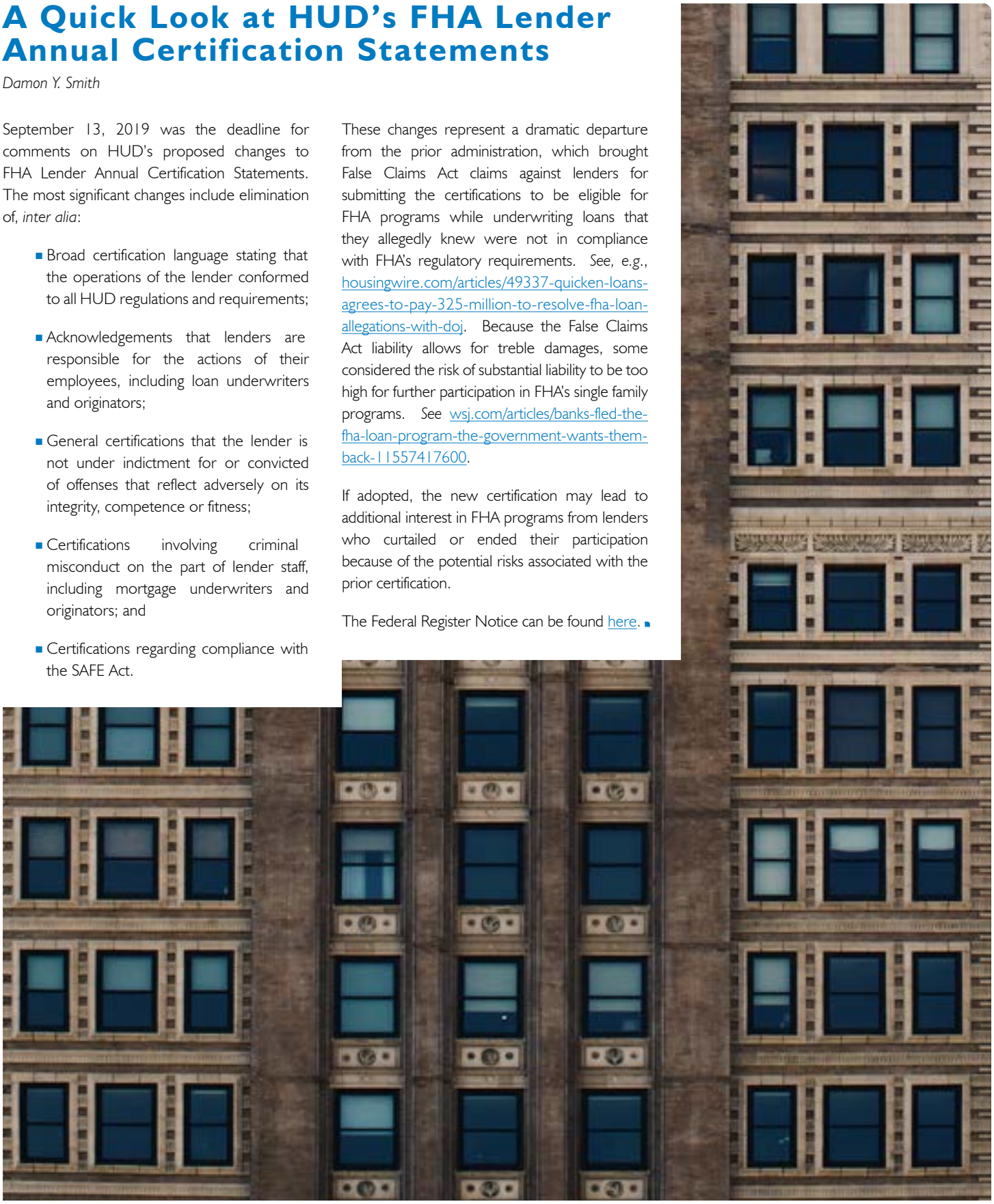
September 13, 2019 was the deadline for comments on HUD's proposed changes to FHA Lender Annual Certification Statements. The most significant changes include elimination of, *inter alia*:

- Broad certification language stating that the operations of the lender conformed to all HUD regulations and requirements;
- Acknowledgements that lenders are responsible for the actions of their employees, including loan underwriters and originators;
- General certifications that the lender is not under indictment for or convicted of offenses that reflect adversely on its integrity, competence or fitness;
- Certifications involving criminal misconduct on the part of lender staff, including mortgage underwriters and originators; and
- Certifications regarding compliance with the SAFE Act.

These changes represent a dramatic departure from the prior administration, which brought False Claims Act claims against lenders for submitting the certifications to be eligible for FHA programs while underwriting loans that they allegedly knew were not in compliance with FHA's regulatory requirements. *See, e.g.*, housingwire.com/articles/49337-quicken-loans-agrees-to-pay-325-million-to-resolve-fha-loan-allegations-with-doj. Because the False Claims Act liability allows for treble damages, some considered the risk of substantial liability to be too high for further participation in FHA's single family programs. *See* wsj.com/articles/banks-fled-the-fha-loan-program-the-government-wants-them-back-11557417600.

If adopted, the new certification may lead to additional interest in FHA programs from lenders who curtailed or ended their participation because of the potential risks associated with the prior certification.

The Federal Register Notice can be found here.



FinCen Issues Report on Business Email Scams

David P. Saunders

At the risk of stating the obvious, everyone uses email. It has become a central component of both our daily lives and, of course, our businesses. As we transform into a fully digital, corporate world, there are those who have sought to exploit the growing reliance on email. Spammers, hackers, and of course, phishers. No, not the people who go to those really long concerts; we are talking about email scammers who purport to tell you that your UPS package has arrived, but all you need to do is click a link and enter some information. These scams can cripple a business, and trying to prevent these scams is difficult because in many ways, the solution relies on removing human error.

Enter the Financial Crimes Enforcement Network (FinCEN), a bureau of the US Treasury Department that collects and analyzes information about financial transactions in order to combat domestic and international money laundering, terrorist financing, and other financial crimes. FinCEN recently held a forum aimed at discussing ways to identify and curtail business email scammers. The forum, held in New York City, analyzed the trends in business email scams. At the forum, FinCEN released a report indicating that reporting of business email scams had more than doubled between 2016 and 2018. The report also detailed that fake invoice scams grew as a methodology and that manufacturing and construction businesses were top targets.

While knowledge and preparation are critical to defending a business from email scams, the reality of today's world is that it is inevitable that a scam will succeed from time to time. And that is where FinCEN's Rapid Response Program comes in. The program was established in 2014 to assist businesses seeking to report and attempt to recover the loss of funds resulting from, among other things, email scams. It has helped to recover more than $500 million in funds. According to FinCEN, "[u]nder the program, when US law enforcement receives a [scamming] complaint from a victim or a financial institution, the relevant information is forwarded to FinCEN, which moves quickly to track and recover the funds. The program utilizes FinCEN's ability to rapidly share information with counterpart Financial Intelligence Units (FIU) in more than 164 jurisdictions, and leverages these relationships to encourage foreign authorities to intercede and hold funds or reverse wire transfers." See fincen.gov/news/news-releases/fincen-exchange-forum-counters-business-email-compromise-scams. This is an important tool in a business' toolbox when it comes to remediating the harm of an email scam. For information about the program, businesses can contact RRPinfo@fincen.gov.

A Brief History of the CFPB Payday Lending Rule

Alexander N. Ghantous

Between 2013 and 2016, the Consumer Financial Protection Bureau (CFPB) issued no fewer than six white papers or reports relating to payday loan protections.[1] On the date of the last report, June 2, 2016, the CFPB issued a proposed rule[2]. On October 5, 2017, the CFPB issued a final rule that addresses payday loans, auto title loans, and other loans that require the entire loan balance, or the majority of a loan balance, be repaid at once.[3] The rule's stated objective was to eliminate "payday debt traps" by, among other things, addressing underwriting through establishing "ability-to-repay" protections that vary by loan type.[4]

Under the final rule, for payday loans, auto title loans, and other loans comprising lengthier terms and balloon payments, the CFPB would require a "'full-payment test" to establish that borrowers can afford to pay back the loan and also limits the quantity of loans taken "in quick succession" to only three.[5] The rule also lays out two instances when the "full-payment test" is not required: (1) borrowing up to $500 when the loan balance can be repaid at a more gradual pace; and (2) taking loans that are less risky, such as personal loans taken in smaller amounts.[6] The rule would also establish a "debit attempt cutoff," which requires lenders to obtain renewed authorization from a borrower after two consecutive unsuccessful debits on a borrower's account.[7] The rule was scheduled to become effective one year and nine months after being published by the Federal Register, which was last month[8] (the rule was published on November 17, 2017[9]).

However, on February 6, 2019, the CFPB announced that it was proposing to issue a new rule to rescind the underwriting provisions of the prior rule, namely, the requirements for payday loans, auto title loans, and other loans comprising lengthier terms and balloon payments.[10] According to the CFPB's preliminary findings, overturning the requirements would make credit more readily available to consumers.[11] That same day, the CFPB also proposed pushing the rule's compliance date from August 19, 2019, to November 19, 2020.[12]

On June 6, 2019, the CFPB issued a final rule to delay the compliance date for the mandatory underwriting provisions of the 2017 final rule to November 19, 2020, in order to provide additional time to permit an orderly conclusion to its separate rulemaking process to reconsider the mandatory underwriting provisions.[13] Note that the payment provisions of the final rule, which address withdrawing payments from accounts, have not been delayed by rulemaking, and the CFPB has made no move to rescind those provisions.[14] However, the CFPB also has not opposed the compliance date for those provisions being stayed through at least December 6, 2019, in connection with a lawsuit in the Western District of Texas that challenges the rulemaking.[15]

Thus, the earliest that any part of the rule will go into effect is December 2019.

[1] Consumer Fin. Prot. Bureau, consumerfinance.gov/payday-rule/. (last visited Sept. 18, 2019).

[2] Consumer Fin. Prot. Bureau, consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-proposes-rule-end-payday-debt-traps/. (June 2, 2016).

[3] Consumer Fin. Prot. Bureau, consumerfinance.gov/about-us/newsroom/cfpb-finalizes-rule-stop-payday-debt-traps/ (Oct. 5, 2017).

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] Payday, Vehicle Title, and Certain High-Cost Installment Loans, 82 FR 54472-01

[10] Consumer Fin. Prot. Bureau, consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-releases-notices-proposed-rulemaking-payday-lending/ (Feb. 6, 2019).

[11] *Id.*

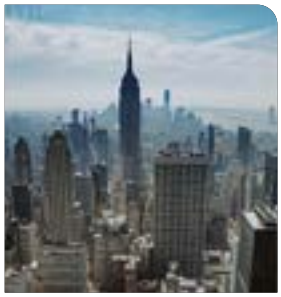
[12] *Id.*

[13] Consumer Fin. Prot. Bureau, consumerfinance.gov/policy-compliance/rulemaking/final-rules/payday-vehicle-title-and-certain-high-cost-installment-loans-delay-compliance-date-correcting-amendments/ (last visited Sept. 18, 2019).

[14] Consumer Fin. Prot. Bureau, consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-releases-notices-proposed-rulemaking-payday-lending/ (Feb. 6, 2019).

[15] *Cmty. Fin. Servs. Ass'n of Am., Ltd. v. Consumer Fin. Prot. Bureau*, No. 1:18-cv-00295-LY (Tex. Dist. Aug. 6, 2019) (order staying litigation and compliance date).




Contributors

Alexander N. Ghantous

Gabriel K. Gillett

William S. C. Goldstein

Olivia Hoffman

Katherine Rosoff

Contacts

AMY M. GALLEGOS
PARTNER

Los Angeles | 213 239-2208
agallegos@jenner.com

MICHAEL W. ROSS
PARTNER

New York | 212 891-1669
mross@jenner.com

DAMON Y. SMITH
PARTNER

Washington, DC | 202 639-6008
dsmith@jenner.com

JOSEPH L. NOGA
PARTNER

New York | 212 891-1676
jnoga@jenner.com

DAVID P. SAUNDERS
PARTNER

Chicago | 312 923-8388
dsaunders@jenner.com

© 2019 Jenner & Block LLP. **Attorney Advertising**. Jenner & Block is an Illinois Limited Liability Partnership including professional corporations. This publication is not intended to provide legal advice but to provide information on legal matters and firm news of interest to our clients and colleagues. Readers should seek specific legal advice before taking any action with respect to matters mentioned in this publication. The attorney responsible for this publication is Brent E. Kidwell, Jenner & Block LLP, 353 N. Clark Street, Chicago, IL 60654-3456. Prior results do not guarantee a similar outcome.