NAFCU

3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

January 29, 2020

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street SW
Washington, D.C. 20554

RE: Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor (CG Docket Nos. 17-59 and 17-97)

Dear Ms. Dortch:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), I am writing in regard to the Consumer and Governmental Affairs Bureau of the Federal Communications Commission's (FCC or Commission) Public Notice (Notice) seeking comment for the first staff report on call blocking. NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve nearly 120 million consumers with personal and small business financial service products. NAFCU members have reported a drastic increase in the volume of calls being blocked by Voice Service Providers (Service Providers). NAFCU is alarmed by this trend and, accordingly, recommends the FCC halt Service Providers' aggressive call blocking efforts until the STIR/SHAKEN call authentication framework is fully implemented. Additionally, NAFCU urges the FCC to ensure there is complete transparency and mitigation of blocking for both callers and called parties.

General Comments

The FCC has historically prohibited call blocking by Service Providers;[1] however, in June 2019, the Commission encouraged the implementation of STIR/SHAKEN by proposing a safe harbor from liability under its call completion rules for Service Providers who block calls that are not authenticated under that framework.[2] The Commission also proposed to mandate adoption of STIR/SHAKEN if major Service Providers do not do so voluntarily by December 2019.[3] Moreover, the Commission proposed to create a mechanism to provide information to consumers about the effectiveness of Service Providers' "robocall solutions."[4] Relatedly, in its June 2019 Declaratory Ruling, the Commission authorized Service Providers with broad authority to block

[1] *See* Notice of Proposed Rulemaking and Notice of Inquiry, Advanced Methods to Target and Eliminate Unlawful Robocalls, 82 Fed. Reg. 22,625, 22,626 (May 17, 2017) (referencing the "Commission's historic prohibitions on call blocking").

[2] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, No. CG17-59, 2019 WL 2461905 ¶¶ 51-58 (June 7, 2019) [hereinafter Declaratory Ruling and Further Notice].

[3] *Id*. ¶¶ 71-74.

[4] *Id*. ¶ 83.

calls “based on any reasonable analytics designed to identify unwanted calls.”[5]As a result, Service Providers have rapidly moved to implement call-blocking measures by using their own algorithm as well as the industry-led STIR/SHAKEN call authentication framework.

NAFCU supports the Commission’s goal to eliminate illegal automated calls using a fully tested and effective STIR/SHAKEN framework. However, the STIR/SHAKEN framework must be designed to ensure that important and often time-sensitive calls that legitimate businesses, including credit unions, place to their customers are not blocked. Credit unions, as not-for-profit, member-owned community financial institutions, do not seek to harm their member-owners, but rather provide them with important information about their existing accounts. Credit unions place thousands of calls to their members related to data breach, fraud alerts, loan servicing and collections. It is critical that these calls be completed without delay. Currently, these calls are experiencing delays or not being completed at all due to the unclear and inconsistent call blocking environment.

To minimize the blocking of important calls, NAFCU recommends that the Commission direct Service Providers not to block unsigned calls until the STIR/ SHAKEN framework has been fully implemented. Moreover, once the framework has been fully implemented, the Commission should authorize Service Providers to block only calls that have been properly authenticated (full authentication) under the framework. In addition, for a Service Provider to be protected by the safe harbor, the Commission should require Providers that block calls to notify the calling party and to remove erroneous blocks within 24 hours of learning of the block.

Current Effectiveness of Call Blocking

In June 2019, the Commission suggested that Service Providers should establish procedures to enable callers to correct erroneous blocks. This requirement would implement Congress’s directive in the recently enacted *Telephone Robocall Abuse Criminal Enforcement and Deterrence* (TRACED) *Act* that the Commission not “support blocking or mislabeling calls from legitimate businesses” and that the Commission “should require voice service providers to unblock improperly blocked calls in as timely and efficient a manner as reasonable.”[6] Contrary to the suggestion of the FCC and Congress, evidence suggests that Service Providers are not providing the necessary redress to blocked calls. The current call blocking landscape has created a litany of problems for legitimate businesses seeking to contact their members on important, time-sensitive information.

Following the June 2019 Declaratory Order and Notice on call blocking, providers have swiftly moved to block calls based on analytics and an industry-led call authentication system. Some Service Providers have moved forward in blocking calls without an exhaustive analysis of the impact on their call blocking efforts, resulting in the blockage of hundreds and thousands of legitimate calls, leaving callers and called parties without an appropriate redress. Accordingly,

[5] *See* Declaratory Ruling and Third Notice ¶ 34-35.
[6] S. Rep. No. 116-41, at 15 (2019) (Senate Commerce Committee report on the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act (S. 151, 116th Cong. (2019)).

NAFCU recommends the FCC take a step back and reevaluate call blocking measures to ensure there is rigorous market testing prior to fully deploying the STIR/SHAKEN framework.

Most credit unions do not have the resources to track busy signals and determine which of their outbound calls are blocked from Service Providers. Those credit unions that investigated further realized that the spike in busy signals correlated directly to blocked calls from Service Providers. After analyzing the average percentage of busy signals over a period of time and noticing the significant spike in busy signals in the months following the FCC's Declaratory Order and Notice, one credit union calculated that there were over 100,000 calls blocked by two Service Providers between September 2019 and November 2019. As this was a very conservative assessment, it is reasonable to presume that thousands of more calls were blocked. In the September call blocking incident, the credit union's average busy percentage reached 6% — more than double their average busy rate. Similarly, in the October and November call blocking incidents, the credit union's average busy percentage was over 11% — more than triple the average busy calls they experience.

The recent rise of ineffective call blocking efforts has had a significant impact on the ability of credit unions to reach their members and resulted in a direct failure to notify consumers regarding critical account information. Credit unions that investigated blocked calls submitted a form to each respective Service Provider to inquire on call blocking efforts; however, credit unions were met with conflicting responses from Service Providers. While one Service Provider was able to white-list the numbers so that they do not experience further blockage, another Service Provider, was unable to resolve the issue long-term by white-listing the legitimate numbers. As a result, credit unions could further experience blockage of thousands of more calls to their members in the near future.

The types of factors Service Providers use to block suspicious calls under their analytics-based blocking is unclear. For example, under the June 2019 FCC Declaratory Order and Notice, Service Providers were permitted to block calls for a variety of reasons, including high volume of short duration calls originating from a toll-free number. The problem is that legitimate calls may share some of the same analytical tendencies resulting in the blocking of wanted calls, such as credit card fraud notifications and other critical, time-sensitive calls. There is currently no uniform standard for Service Providers to follow during their call blocking measures. Consequently, Service Providers have different approaches for redress for blocked calls, which continues to cause great confusion for both the callers and the called party.

Moreover, some Service Providers may provide redress to callers for payment, which creates an unfair landscape for legitimate callers seeking to reach their customers. For example, one Service Provider, through its supplier provides businesses with the option to register their phone numbers and access data analytics of registered numbers for outbound calls. The supplier offers businesses a thirty-day trial period, after which, the supplier (acting as an agent of the Service Provider), offers businesses to elect to license subscription services on a paid subscription basis. This type of treatment of callers breeds further distrust of the current call blocking efforts.

The combination of an uncertain call analytics system and a partially implemented STIR/SHAKEN framework has raised concerns that a significant number of legitimate messages will not be delivered as Service Providers may block messages using vague or shifting standards. In a STIR/SHAKEN environment, calls are signed or not signed; if calls are signed, then there is a validation process at the terminating carrier. If the call is validated, then the next step is the level of attestation. One problem under a partially implemented call authentication system is that calls originating from conventional (older) time-division multiple access telephone networks will not be signed. As a result, once interworked with a voice over internet protocol (VoIP), those calls may be passed unsigned. Alternatively, if the call is interworked at a gateway, the call may be given a level of gateway attestation. If such calls are blocked, then VoIP subscribers may be blocking calls from other U.S. subscribers in rural areas. That is why it is critical for the STIR/SHAKEN authentication framework to be thoroughly tested and fully implemented before calls are blocked.

Fully Authenticated Calls Should Not Be Blocked Using Analytics

As call authentication is deployed, Service Providers should not have to use the malleable "reasonable analytics" standard to block calls. Once a call is fully authenticated under a well-tested and fully operational STIR/SHAKEN standard, there should be a presumption that the call is legal. Service Providers should have a procedure to investigate suspicious calls before triggering analytics to block a call. Once a Service Provider suspects that one of their customers is generating illegal calls, the next step should be to investigate the caller, not to simply apply analytics, which has a great probability of also sweeping in legitimate calls (e.g., high volume calls). Consequently, if Service Providers presume all calls that fall under the "reasonable analytics" are illegal, then consumers will miss out on important and time-sensitive information. Ultimately, a fully operational call authentication framework is the best remedy to combat illegal automated calls.

Callers and Consumers Need Complete Transparency and Means of Redress for Blocked Calls

The TRACED Act requires the Commission to develop rules to ensure transparency and encourage the mitigation of blocking for callers and called parties alike. Specifically, the Act instructs the FCC to promulgate rules to establish a process to allow redress for callers who are being blocked. The TRACED Act also provides a safe harbor for Service Providers that block calls under the call authentication framework. However, Service Providers should be required to notify callers and call recipients of blocked calls, as well as remove erroneous blocks expeditiously in order to receive safe harbor protection under the FCC's interpretation of the TRACED Act.

Service Providers have a variety of options to notify callers regarding blocked calls, including the use of an intercept message or special information tone to convey that the call has been blocked. These notifications should provide the necessary information to effectively address blocked calls (i.e., a phone number or website address for the caller to seek information about why the call was blocked and how to prevent such blocking in the future). Any intercept process should identify the Service Provider that has blocked the call and provide a means for the caller to contact that Service

Provider. Moreover, Service Providers should remove an erroneous block within 24 hours of learning of the block, at no charge to the caller. Subsequently, these procedures will mitigate the harm caused to our members and consumers by an erroneous block and ensure consumers do not miss important, time-sensitive informational calls.

Conclusion

NAFCU greatly appreciates the opportunity to comment on this Notice and supports the Commission's effort to gather feedback on the effectiveness of the current call blocking efforts. We look forward to continuing to work with the Commission on combating illegal robocalls while ensuring consumers continue to receive critical information. If you have any question or concerns, please do not hesitate to contact me at (703) 842-2222 or mmakonnen@nafcu.org.

Sincerely,

Mahlet Makonnen
Regulatory Affairs Counsel