FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

December 23, 2022

The Honorable Raphael G. Warnock
United States Senate
B40D Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Warnock:

Thank you for your letter regarding the efforts of the Federal Communications Commission to combat illegal robocalls. Protecting consumers from illegal robocalls is one of our top consumer protection priorities, and the agency is using all its tools to address this on-going issue. Our approach to this problem has been multi-faceted. We have updated policies, pursued enforcement actions, provided consumers with new tools and education on new scam tactics, championed new technologies, and closed loopholes.

As you note, the Commission took a critical step in May when we updated our policies to address illegal robocall traffic that originates in other countries. This is important because a growing amount of the robocall traffic that we receive now comes from overseas. In fact, one study suggests as many as two-thirds of robocall campaigns may now originate from abroad. That is why we adopted an Order requiring gateway providers—the carriers that serve as the domestic entry point for calls from outside the United States—to use STIR/SHAKEN call authentication technology, register in our Robocall Mitigation Database, and comply with traceback requests from the Commission and law enforcement to help figure out from where these foreign-originated junk calls are originating. I believe these measures will help us identify and tackle the increasing number of international robocalls.

In addition, our Enforcement Bureau continues to investigate and take aggressive action against illegal robocallers. Over the past year, the Bureau's investigations have led to the Commission proposing fines ranging from $5 million to more than $299 million against companies for apparently illegal robocalls under the Telephone Consumer Protection Act.

We have also ordered the rest of the industry to block known scam robocallers. In July, the Enforcement Bureau issued a first of its kind Order directing all voice service providers in the United States to stop carrying traffic from multiple entities responsible for making billions of robocalls marketing automobile warranties. This novel approach is especially noteworthy for two reasons. First, the effort to tell all other carriers to cease taking traffic from those responsible for these warranty calls represented a new approach under our rules. Second, this effort had real impact. YouMail reported that after our action these calls dropped 80 percent from the previous month, and Robokiller said that auto warranty calls fell by over 99 percent in

the months following our action.[1] As a result, we have replicated this approach in other contexts. In particular, in December 2022, we ordered that providers block the entity responsible for an estimated 40 percent of scam student loan robocalls.

It is also worth noting that our action against the auto warranty scam was part of a broader effort at the Commission to work collaboratively with and leverage the work of state enforcement agencies on robocall matters. In the auto warranty case, we coordinated our investigation and efforts with the Ohio Attorney General. The Commission now has Memoranda of Understanding (MOU) with Attorneys General in 43 states, the District of Columbia, and Guam. These MOUs allow us to share information that will assist in efforts to prosecute bad actors behind robocalls under both federal and state law, as was done with the Ohio Attorney General. In addition, the Attorneys General of Colorado, North Carolina, and Tennessee have committed to help work with the Commission to bring their other colleagues in the states on board with this effort. We have put a premium on expanding these kind of partnerships with colleagues inside and outside of government in order to more effectively pursue enforcement actions and broadly raise consumer awareness. To this end, the Consumer and Governmental Affairs Bureau has developed partnerships with non-profit organizations, such as AARP and the National Diversity Coalition, to inform the most vulnerable consumers about common and emerging robocall scams. The Commission is also continuing to build on the consumer education partnership developed with the Federal Trade Commission during our joint spoofing awareness campaign.

Another important partnership involves our coordination with the Industry Traceback Group (ITG). The ITG was created under the TRACED Act. As you note, the ITG uses provider data to traceback and identify the source of illegal robocalls. This information and collaboration is essential to our enforcement efforts. I agree with your suggestion that increased visibility into the traceback process is likely to serve the public interest. Accordingly, I have asked the Commission's Enforcement Bureau to require the ITG to submit on a quarterly basis a unified traceback report that includes (1) an identifier for each traceback that the ITG performed during the prior quarter; (2) the date of the traceback; (3) the identity of the originating/gateway provider (or the provider furthest along in the call path that the ITG was able to identify); and (4) a basic description of the type of robocall (e.g., auto warranty, government impostor, etc.). I believe this approach will improve transparency while also protecting the integrity of our enforcement process, consumer privacy, and commercially-sensitive information that could have an adverse effect on competition if disclosed inappropriately. As you know, the Enforcement Bureau's investigative activities, including identifying potential targets of enforcement actions, benefit from confidentiality until we have collected the underlying data necessary to take public action. This is also consistent with our actions in recent years adopting a targeted approach, under existing law and recently-developed rules, to publicly disclose bad actor originating and gateway providers as sources of illegal robocalls. We have issued over two dozen cease-and-desist letters over the past two years that are designed to do just that. And we used this approach in our recent enforcement efforts against providers responsible for robocalls marketing auto warranties. For the first time, we publicly disclosed the list of providers we believed were

[1] *See* https://blog.youmail.com/2022/07/july-enforcement-achieve-success-in-escalating-the-war-on-robocalls/; Car Warranty Robocalls Plummeted in Late 2022: Here's Why | RoboKiller Blog.

responsible for these calls to put other providers on notice. Then, as noted above, we followed up with a subsequent order telling every other provider to block traffic from the providers tied to the auto warranty and student loan scams.

Finally, although the Commission is using every tool at its disposal, I believe that additional authority from Congress is needed to combat robocalls and robotexts more effectively. In particular, I want to draw your attention to the issues described below.

Fix the definition of autodialer: Because robotexts are neither prerecorded nor artificial voice calls, the Telephone Consumer Protection Act (TCPA) only provides consumers protection from robotexts if they are sent from autodialers. Last year's Supreme Court decision, *Facebook v. Duguid,* narrowed the definition of autodialer under the TCPA, resulting in the law only covering equipment that generates numbers randomly and sequentially. Consequently, equipment that simply uses lists to generate robotexts means that fewer robotexts may be subject to TCPA protections, and as a result, this decision may be responsible for the rise in robotexts over the past year.

Expand tools to catch robocallers: Robocallers often create multiple entities and business relationships to cover their tracks and obscure their involvement. As a result, the Commission would benefit from statutory authority allowing it to access Bank Secrecy Act information. This would allow the agency to identify more quickly the financial records and assets of our investigative targets given the overlap between illegal robocalls and the role they play facilitating schemes to defraud and harm victims financially. In particular, our investigations would benefit from clear authority to access financial reports that institutions are required to produce regarding suspicious activities under the Bank Secrecy Act. This would permit the agency's Enforcement Bureau to access financial information about individual targets without first notifying the targets. By updating the law to allow for administrative subpoenas for all types of non-content customer records, the Commission would be able to obtain evidence that can help identify who is actually responsible for illegal robocall campaigns, and to prevent scam artists from registering new entities under new names after enforcement actions shut them down.

Increase court enforcement of fines: We vigorously pursue robocall violations, spending a great deal of time and effort to gather evidence and issue fines against violators. But when the violators refuse to pay the fines we assess, we have to hand the cases over to our colleagues at the Department of Justice (DOJ) and hope that DOJ has the resources available to pursue these cases in court. If Congress granted the Commission the authority and resources to perform this work ourselves, we could leverage the agency's existing expertise and motivation to enforce our orders.

I hope this is helpful. Please let me know if you have any further questions.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

December 23, 2022

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Wyden:

Thank you for your letter regarding the efforts of the Federal Communications Commission to combat illegal robocalls. Protecting consumers from illegal robocalls is one of our top consumer protection priorities, and the agency is using all its tools to address this on-going issue. Our approach to this problem has been multi-faceted. We have updated policies, pursued enforcement actions, provided consumers with new tools and education on new scam tactics, championed new technologies, and closed loopholes.

As you note, the Commission took a critical step in May when we updated our policies to address illegal robocall traffic that originates in other countries. This is important because a growing amount of the robocall traffic that we receive now comes from overseas. In fact, one study suggests as many as two-thirds of robocall campaigns may now originate from abroad. That is why we adopted an Order requiring gateway providers—the carriers that serve as the domestic entry point for calls from outside the United States—to use STIR/SHAKEN call authentication technology, register in our Robocall Mitigation Database, and comply with traceback requests from the Commission and law enforcement to help figure out from where these foreign-originated junk calls are originating. I believe these measures will help us identify and tackle the increasing number of international robocalls.

In addition, our Enforcement Bureau continues to investigate and take aggressive action against illegal robocallers. Over the past year, the Bureau's investigations have led to the Commission proposing fines ranging from $5 million to more than $299 million against companies for apparently illegal robocalls under the Telephone Consumer Protection Act.

We have also ordered the rest of the industry to block known scam robocallers. In July, the Enforcement Bureau issued a first of its kind Order directing all voice service providers in the United States to stop carrying traffic from multiple entities responsible for making billions of robocalls marketing automobile warranties. This novel approach is especially noteworthy for two reasons. First, the effort to tell all other carriers to cease taking traffic from those responsible for these warranty calls represented a new approach under our rules. Second, this effort had real impact. YouMail reported that after our action these calls dropped 80 percent from the previous month, and Robokiller said that auto warranty calls fell by over 99 percent in

the months following our action.[2] As a result, we have replicated this approach in other contexts. In particular, in December 2022, we ordered that providers block the entity responsible for an estimated 40 percent of scam student loan robocalls.

It is also worth noting that our action against the auto warranty scam was part of a broader effort at the Commission to work collaboratively with and leverage the work of state enforcement agencies on robocall matters. In the auto warranty case, we coordinated our investigation and efforts with the Ohio Attorney General. The Commission now has Memoranda of Understanding (MOU) with Attorneys General in 43 states, the District of Columbia, and Guam. These MOUs allow us to share information that will assist in efforts to prosecute bad actors behind robocalls under both federal and state law, as was done with the Ohio Attorney General. In addition, the Attorneys General of Colorado, North Carolina, and Tennessee have committed to help work with the Commission to bring their other colleagues in the states on board with this effort. We have put a premium on expanding these kind of partnerships with colleagues inside and outside of government in order to more effectively pursue enforcement actions and broadly raise consumer awareness. To this end, the Consumer and Governmental Affairs Bureau has developed partnerships with non-profit organizations, such as AARP and the National Diversity Coalition, to inform the most vulnerable consumers about common and emerging robocall scams. The Commission is also continuing to build on the consumer education partnership developed with the Federal Trade Commission during our joint spoofing awareness campaign.

Another important partnership involves our coordination with the Industry Traceback Group (ITG). The ITG was created under the TRACED Act. As you note, the ITG uses provider data to traceback and identify the source of illegal robocalls. This information and collaboration is essential to our enforcement efforts. I agree with your suggestion that increased visibility into the traceback process is likely to serve the public interest. Accordingly, I have asked the Commission's Enforcement Bureau to require the ITG to submit on a quarterly basis a unified traceback report that includes (1) an identifier for each traceback that the ITG performed during the prior quarter; (2) the date of the traceback; (3) the identity of the originating/gateway provider (or the provider furthest along in the call path that the ITG was able to identify); and (4) a basic description of the type of robocall (e.g., auto warranty, government impostor, etc.). I believe this approach will improve transparency while also protecting the integrity of our enforcement process, consumer privacy, and commercially-sensitive information that could have an adverse effect on competition if disclosed inappropriately. As you know, the Enforcement Bureau's investigative activities, including identifying potential targets of enforcement actions, benefit from confidentiality until we have collected the underlying data necessary to take public action. This is also consistent with our actions in recent years adopting a targeted approach, under existing law and recently-developed rules, to publicly disclose bad actor originating and gateway providers as sources of illegal robocalls. We have issued over two dozen cease-and-desist letters over the past two years that are designed to do just that. And we used this approach in our recent enforcement efforts against providers responsible for robocalls marketing auto warranties. For the first time, we publicly disclosed the list of providers we believed were

[2] *See* https://blog.youmail.com/2022/07/july-enforcement-achieve-success-in-escalating-the-war-on-robocalls/; Car Warranty Robocalls Plummeted in Late 2022: Here's Why | RoboKiller Blog.

responsible for these calls to put other providers on notice. Then, as noted above, we followed up with a subsequent order telling every other provider to block traffic from the providers tied to the auto warranty and student loan scams.

Finally, although the Commission is using every tool at its disposal, I believe that additional authority from Congress is needed to combat robocalls and robotexts more effectively. In particular, I want to draw your attention to the issues described below.

Fix the definition of autodialer: Because robotexts are neither prerecorded nor artificial voice calls, the Telephone Consumer Protection Act (TCPA) only provides consumers protection from robotexts if they are sent from autodialers. Last year's Supreme Court decision, *Facebook v. Duguid,* narrowed the definition of autodialer under the TCPA, resulting in the law only covering equipment that generates numbers randomly and sequentially. Consequently, equipment that simply uses lists to generate robotexts means that fewer robotexts may be subject to TCPA protections, and as a result, this decision may be responsible for the rise in robotexts over the past year.

Expand tools to catch robocallers: Robocallers often create multiple entities and business relationships to cover their tracks and obscure their involvement. As a result, the Commission would benefit from statutory authority allowing it to access Bank Secrecy Act information. This would allow the agency to identify more quickly the financial records and assets of our investigative targets given the overlap between illegal robocalls and the role they play facilitating schemes to defraud and harm victims financially. In particular, our investigations would benefit from clear authority to access financial reports that institutions are required to produce regarding suspicious activities under the Bank Secrecy Act. This would permit the agency's Enforcement Bureau to access financial information about individual targets without first notifying the targets. By updating the law to allow for administrative subpoenas for all types of non-content customer records, the Commission would be able to obtain evidence that can help identify who is actually responsible for illegal robocall campaigns, and to prevent scam artists from registering new entities under new names after enforcement actions shut them down.

Increase court enforcement of fines: We vigorously pursue robocall violations, spending a great deal of time and effort to gather evidence and issue fines against violators. But when the violators refuse to pay the fines we assess, we have to hand the cases over to our colleagues at the Department of Justice (DOJ) and hope that DOJ has the resources available to pursue these cases in court. If Congress granted the Commission the authority and resources to perform this work ourselves, we could leverage the agency's existing expertise and motivation to enforce our orders.

I hope this is helpful. Please let me know if you have any further questions.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

December 23, 2022

The Honorable Brian Schatz
United States Senate
722 Hart Senate Office Building
Washington, DC 20510

Dear Senator Schatz:

Thank you for your letter regarding the efforts of the Federal Communications Commission to combat illegal robocalls. Protecting consumers from illegal robocalls is one of our top consumer protection priorities, and the agency is using all its tools to address this on-going issue. Our approach to this problem has been multi-faceted. We have updated policies, pursued enforcement actions, provided consumers with new tools and education on new scam tactics, championed new technologies, and closed loopholes.

As you note, the Commission took a critical step in May when we updated our policies to address illegal robocall traffic that originates in other countries. This is important because a growing amount of the robocall traffic that we receive now comes from overseas. In fact, one study suggests as many as two-thirds of robocall campaigns may now originate from abroad. That is why we adopted an Order requiring gateway providers—the carriers that serve as the domestic entry point for calls from outside the United States—to use STIR/SHAKEN call authentication technology, register in our Robocall Mitigation Database, and comply with traceback requests from the Commission and law enforcement to help figure out from where these foreign-originated junk calls are originating. I believe these measures will help us identify and tackle the increasing number of international robocalls.

In addition, our Enforcement Bureau continues to investigate and take aggressive action against illegal robocallers. Over the past year, the Bureau's investigations have led to the Commission proposing fines ranging from $5 million to more than $299 million against companies for apparently illegal robocalls under the Telephone Consumer Protection Act.

We have also ordered the rest of the industry to block known scam robocallers. In July, the Enforcement Bureau issued a first of its kind Order directing all voice service providers in the United States to stop carrying traffic from multiple entities responsible for making billions of robocalls marketing automobile warranties. This novel approach is especially noteworthy for two reasons. First, the effort to tell all other carriers to cease taking traffic from those responsible for these warranty calls represented a new approach under our rules. Second, this effort had real impact. YouMail reported that after our action these calls dropped 80 percent from the previous month, and Robokiller said that auto warranty calls fell by over 99 percent in

the months following our action.[3] As a result, we have replicated this approach in other contexts. In particular, in December 2022, we ordered that providers block the entity responsible for an estimated 40 percent of scam student loan robocalls.

It is also worth noting that our action against the auto warranty scam was part of a broader effort at the Commission to work collaboratively with and leverage the work of state enforcement agencies on robocall matters. In the auto warranty case, we coordinated our investigation and efforts with the Ohio Attorney General. The Commission now has Memoranda of Understanding (MOU) with Attorneys General in 43 states, the District of Columbia, and Guam. These MOUs allow us to share information that will assist in efforts to prosecute bad actors behind robocalls under both federal and state law, as was done with the Ohio Attorney General. In addition, the Attorneys General of Colorado, North Carolina, and Tennessee have committed to help work with the Commission to bring their other colleagues in the states on board with this effort. We have put a premium on expanding these kind of partnerships with colleagues inside and outside of government in order to more effectively pursue enforcement actions and broadly raise consumer awareness. To this end, the Consumer and Governmental Affairs Bureau has developed partnerships with non-profit organizations, such as AARP and the National Diversity Coalition, to inform the most vulnerable consumers about common and emerging robocall scams. The Commission is also continuing to build on the consumer education partnership developed with the Federal Trade Commission during our joint spoofing awareness campaign.

Another important partnership involves our coordination with the Industry Traceback Group (ITG). The ITG was created under the TRACED Act. As you note, the ITG uses provider data to traceback and identify the source of illegal robocalls. This information and collaboration is essential to our enforcement efforts. I agree with your suggestion that increased visibility into the traceback process is likely to serve the public interest. Accordingly, I have asked the Commission's Enforcement Bureau to require the ITG to submit on a quarterly basis a unified traceback report that includes (1) an identifier for each traceback that the ITG performed during the prior quarter; (2) the date of the traceback; (3) the identity of the originating/gateway provider (or the provider furthest along in the call path that the ITG was able to identify); and (4) a basic description of the type of robocall (e.g., auto warranty, government impostor, etc.). I believe this approach will improve transparency while also protecting the integrity of our enforcement process, consumer privacy, and commercially-sensitive information that could have an adverse effect on competition if disclosed inappropriately. As you know, the Enforcement Bureau's investigative activities, including identifying potential targets of enforcement actions, benefit from confidentiality until we have collected the underlying data necessary to take public action. This is also consistent with our actions in recent years adopting a targeted approach, under existing law and recently-developed rules, to publicly disclose bad actor originating and gateway providers as sources of illegal robocalls. We have issued over two dozen cease-and-desist letters over the past two years that are designed to do just that. And we used this approach in our recent enforcement efforts against providers responsible for robocalls marketing auto warranties. For the first time, we publicly disclosed the list of providers we believed were

[3] *See* https://blog.youmail.com/2022/07/july-enforcement-achieve-success-in-escalating-the-war-on-robocalls/; Car Warranty Robocalls Plummeted in Late 2022: Here's Why | RoboKiller Blog.

responsible for these calls to put other providers on notice. Then, as noted above, we followed up with a subsequent order telling every other provider to block traffic from the providers tied to the auto warranty and student loan scams.

Finally, although the Commission is using every tool at its disposal, I believe that additional authority from Congress is needed to combat robocalls and robotexts more effectively. In particular, I want to draw your attention to the issues described below.

Fix the definition of autodialer: Because robotexts are neither prerecorded nor artificial voice calls, the Telephone Consumer Protection Act (TCPA) only provides consumers protection from robotexts if they are sent from autodialers. Last year's Supreme Court decision, *Facebook v. Duguid,* narrowed the definition of autodialer under the TCPA, resulting in the law only covering equipment that generates numbers randomly and sequentially. Consequently, equipment that simply uses lists to generate robotexts means that fewer robotexts may be subject to TCPA protections, and as a result, this decision may be responsible for the rise in robotexts over the past year.

Expand tools to catch robocallers: Robocallers often create multiple entities and business relationships to cover their tracks and obscure their involvement. As a result, the Commission would benefit from statutory authority allowing it to access Bank Secrecy Act information. This would allow the agency to identify more quickly the financial records and assets of our investigative targets given the overlap between illegal robocalls and the role they play facilitating schemes to defraud and harm victims financially. In particular, our investigations would benefit from clear authority to access financial reports that institutions are required to produce regarding suspicious activities under the Bank Secrecy Act. This would permit the agency's Enforcement Bureau to access financial information about individual targets without first notifying the targets. By updating the law to allow for administrative subpoenas for all types of non-content customer records, the Commission would be able to obtain evidence that can help identify who is actually responsible for illegal robocall campaigns, and to prevent scam artists from registering new entities under new names after enforcement actions shut them down.

Increase court enforcement of fines: We vigorously pursue robocall violations, spending a great deal of time and effort to gather evidence and issue fines against violators. But when the violators refuse to pay the fines we assess, we have to hand the cases over to our colleagues at the Department of Justice (DOJ) and hope that DOJ has the resources available to pursue these cases in court. If Congress granted the Commission the authority and resources to perform this work ourselves, we could leverage the agency's existing expertise and motivation to enforce our orders.

I hope this is helpful. Please let me know if you have any further questions.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

December 23, 2022

The Honorable Edward J. Markey
United States Senate
255 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Markey:

Thank you for your letter regarding the efforts of the Federal Communications Commission to combat illegal robocalls. Protecting consumers from illegal robocalls is one of our top consumer protection priorities, and the agency is using all its tools to address this on-going issue. Our approach to this problem has been multi-faceted. We have updated policies, pursued enforcement actions, provided consumers with new tools and education on new scam tactics, championed new technologies, and closed loopholes.

As you note, the Commission took a critical step in May when we updated our policies to address illegal robocall traffic that originates in other countries. This is important because a growing amount of the robocall traffic that we receive now comes from overseas. In fact, one study suggests as many as two-thirds of robocall campaigns may now originate from abroad. That is why we adopted an Order requiring gateway providers—the carriers that serve as the domestic entry point for calls from outside the United States—to use STIR/SHAKEN call authentication technology, register in our Robocall Mitigation Database, and comply with traceback requests from the Commission and law enforcement to help figure out from where these foreign-originated junk calls are originating. I believe these measures will help us identify and tackle the increasing number of international robocalls.

In addition, our Enforcement Bureau continues to investigate and take aggressive action against illegal robocallers. Over the past year, the Bureau's investigations have led to the Commission proposing fines ranging from $5 million to more than $299 million against companies for apparently illegal robocalls under the Telephone Consumer Protection Act.

We have also ordered the rest of the industry to block known scam robocallers. In July, the Enforcement Bureau issued a first of its kind Order directing all voice service providers in the United States to stop carrying traffic from multiple entities responsible for making billions of robocalls marketing automobile warranties. This novel approach is especially noteworthy for two reasons. First, the effort to tell all other carriers to cease taking traffic from those responsible for these warranty calls represented a new approach under our rules. Second, this effort had real impact. YouMail reported that after our action these calls dropped 80 percent from the previous month, and Robokiller said that auto warranty calls fell by over 99 percent in

the months following our action.[4] As a result, we have replicated this approach in other contexts. In particular, in December 2022, we ordered that providers block the entity responsible for an estimated 40 percent of scam student loan robocalls.

It is also worth noting that our action against the auto warranty scam was part of a broader effort at the Commission to work collaboratively with and leverage the work of state enforcement agencies on robocall matters. In the auto warranty case, we coordinated our investigation and efforts with the Ohio Attorney General. The Commission now has Memoranda of Understanding (MOU) with Attorneys General in 43 states, the District of Columbia, and Guam. These MOUs allow us to share information that will assist in efforts to prosecute bad actors behind robocalls under both federal and state law, as was done with the Ohio Attorney General. In addition, the Attorneys General of Colorado, North Carolina, and Tennessee have committed to help work with the Commission to bring their other colleagues in the states on board with this effort. We have put a premium on expanding these kind of partnerships with colleagues inside and outside of government in order to more effectively pursue enforcement actions and broadly raise consumer awareness. To this end, the Consumer and Governmental Affairs Bureau has developed partnerships with non-profit organizations, such as AARP and the National Diversity Coalition, to inform the most vulnerable consumers about common and emerging robocall scams. The Commission is also continuing to build on the consumer education partnership developed with the Federal Trade Commission during our joint spoofing awareness campaign.

Another important partnership involves our coordination with the Industry Traceback Group (ITG). The ITG was created under the TRACED Act. As you note, the ITG uses provider data to traceback and identify the source of illegal robocalls. This information and collaboration is essential to our enforcement efforts. I agree with your suggestion that increased visibility into the traceback process is likely to serve the public interest. Accordingly, I have asked the Commission's Enforcement Bureau to require the ITG to submit on a quarterly basis a unified traceback report that includes (1) an identifier for each traceback that the ITG performed during the prior quarter; (2) the date of the traceback; (3) the identity of the originating/gateway provider (or the provider furthest along in the call path that the ITG was able to identify); and (4) a basic description of the type of robocall (e.g., auto warranty, government impostor, etc.). I believe this approach will improve transparency while also protecting the integrity of our enforcement process, consumer privacy, and commercially-sensitive information that could have an adverse effect on competition if disclosed inappropriately. As you know, the Enforcement Bureau's investigative activities, including identifying potential targets of enforcement actions, benefit from confidentiality until we have collected the underlying data necessary to take public action. This is also consistent with our actions in recent years adopting a targeted approach, under existing law and recently-developed rules, to publicly disclose bad actor originating and gateway providers as sources of illegal robocalls. We have issued over two dozen cease-and-desist letters over the past two years that are designed to do just that. And we used this approach in our recent enforcement efforts against providers responsible for robocalls marketing auto warranties. For the first time, we publicly disclosed the list of providers we believed were

[4] *See* https://blog.youmail.com/2022/07/july-enforcement-achieve-success-in-escalating-the-war-on-robocalls/; Car Warranty Robocalls Plummeted in Late 2022: Here's Why | RoboKiller Blog.

responsible for these calls to put other providers on notice. Then, as noted above, we followed up with a subsequent order telling every other provider to block traffic from the providers tied to the auto warranty and student loan scams.

Finally, although the Commission is using every tool at its disposal, I believe that additional authority from Congress is needed to combat robocalls and robotexts more effectively. In particular, I want to draw your attention to the issues described below.

Fix the definition of autodialer: Because robotexts are neither prerecorded nor artificial voice calls, the Telephone Consumer Protection Act (TCPA) only provides consumers protection from robotexts if they are sent from autodialers. Last year's Supreme Court decision, *Facebook v. Duguid,* narrowed the definition of autodialer under the TCPA, resulting in the law only covering equipment that generates numbers randomly and sequentially. Consequently, equipment that simply uses lists to generate robotexts means that fewer robotexts may be subject to TCPA protections, and as a result, this decision may be responsible for the rise in robotexts over the past year.

Expand tools to catch robocallers: Robocallers often create multiple entities and business relationships to cover their tracks and obscure their involvement. As a result, the Commission would benefit from statutory authority allowing it to access Bank Secrecy Act information. This would allow the agency to identify more quickly the financial records and assets of our investigative targets given the overlap between illegal robocalls and the role they play facilitating schemes to defraud and harm victims financially. In particular, our investigations would benefit from clear authority to access financial reports that institutions are required to produce regarding suspicious activities under the Bank Secrecy Act. This would permit the agency's Enforcement Bureau to access financial information about individual targets without first notifying the targets. By updating the law to allow for administrative subpoenas for all types of non-content customer records, the Commission would be able to obtain evidence that can help identify who is actually responsible for illegal robocall campaigns, and to prevent scam artists from registering new entities under new names after enforcement actions shut them down.

Increase court enforcement of fines: We vigorously pursue robocall violations, spending a great deal of time and effort to gather evidence and issue fines against violators. But when the violators refuse to pay the fines we assess, we have to hand the cases over to our colleagues at the Department of Justice (DOJ) and hope that DOJ has the resources available to pursue these cases in court. If Congress granted the Commission the authority and resources to perform this work ourselves, we could leverage the agency's existing expertise and motivation to enforce our orders.

I hope this is helpful. Please let me know if you have any further questions.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

December 23, 2022

The Honorable Angus King
United States Senate
133 Hart Senate Office Building
Washington, DC 20510

Dear Senator King:

Thank you for your letter regarding the efforts of the Federal Communications Commission to combat illegal robocalls. Protecting consumers from illegal robocalls is one of our top consumer protection priorities, and the agency is using all its tools to address this on-going issue. Our approach to this problem has been multi-faceted. We have updated policies, pursued enforcement actions, provided consumers with new tools and education on new scam tactics, championed new technologies, and closed loopholes.

As you note, the Commission took a critical step in May when we updated our policies to address illegal robocall traffic that originates in other countries. This is important because a growing amount of the robocall traffic that we receive now comes from overseas. In fact, one study suggests as many as two-thirds of robocall campaigns may now originate from abroad. That is why we adopted an Order requiring gateway providers—the carriers that serve as the domestic entry point for calls from outside the United States—to use STIR/SHAKEN call authentication technology, register in our Robocall Mitigation Database, and comply with traceback requests from the Commission and law enforcement to help figure out from where these foreign-originated junk calls are originating. I believe these measures will help us identify and tackle the increasing number of international robocalls.

In addition, our Enforcement Bureau continues to investigate and take aggressive action against illegal robocallers. Over the past year, the Bureau's investigations have led to the Commission proposing fines ranging from $5 million to more than $299 million against companies for apparently illegal robocalls under the Telephone Consumer Protection Act.

We have also ordered the rest of the industry to block known scam robocallers. In July, the Enforcement Bureau issued a first of its kind Order directing all voice service providers in the United States to stop carrying traffic from multiple entities responsible for making billions of robocalls marketing automobile warranties. This novel approach is especially noteworthy for two reasons. First, the effort to tell all other carriers to cease taking traffic from those responsible for these warranty calls represented a new approach under our rules. Second, this effort had real impact. YouMail reported that after our action these calls dropped 80 percent from the previous month, and Robokiller said that auto warranty calls fell by over 99 percent in

the months following our action.[5] As a result, we have replicated this approach in other contexts. In particular, in December 2022, we ordered that providers block the entity responsible for an estimated 40 percent of scam student loan robocalls.

It is also worth noting that our action against the auto warranty scam was part of a broader effort at the Commission to work collaboratively with and leverage the work of state enforcement agencies on robocall matters. In the auto warranty case, we coordinated our investigation and efforts with the Ohio Attorney General. The Commission now has Memoranda of Understanding (MOU) with Attorneys General in 43 states, the District of Columbia, and Guam. These MOUs allow us to share information that will assist in efforts to prosecute bad actors behind robocalls under both federal and state law, as was done with the Ohio Attorney General. In addition, the Attorneys General of Colorado, North Carolina, and Tennessee have committed to help work with the Commission to bring their other colleagues in the states on board with this effort. We have put a premium on expanding these kind of partnerships with colleagues inside and outside of government in order to more effectively pursue enforcement actions and broadly raise consumer awareness. To this end, the Consumer and Governmental Affairs Bureau has developed partnerships with non-profit organizations, such as AARP and the National Diversity Coalition, to inform the most vulnerable consumers about common and emerging robocall scams. The Commission is also continuing to build on the consumer education partnership developed with the Federal Trade Commission during our joint spoofing awareness campaign.

Another important partnership involves our coordination with the Industry Traceback Group (ITG). The ITG was created under the TRACED Act. As you note, the ITG uses provider data to traceback and identify the source of illegal robocalls. This information and collaboration is essential to our enforcement efforts. I agree with your suggestion that increased visibility into the traceback process is likely to serve the public interest. Accordingly, I have asked the Commission's Enforcement Bureau to require the ITG to submit on a quarterly basis a unified traceback report that includes (1) an identifier for each traceback that the ITG performed during the prior quarter; (2) the date of the traceback; (3) the identity of the originating/gateway provider (or the provider furthest along in the call path that the ITG was able to identify); and (4) a basic description of the type of robocall (e.g., auto warranty, government impostor, etc.). I believe this approach will improve transparency while also protecting the integrity of our enforcement process, consumer privacy, and commercially-sensitive information that could have an adverse effect on competition if disclosed inappropriately. As you know, the Enforcement Bureau's investigative activities, including identifying potential targets of enforcement actions, benefit from confidentiality until we have collected the underlying data necessary to take public action. This is also consistent with our actions in recent years adopting a targeted approach, under existing law and recently-developed rules, to publicly disclose bad actor originating and gateway providers as sources of illegal robocalls. We have issued over two dozen cease-and-desist letters over the past two years that are designed to do just that. And we used this approach in our recent enforcement efforts against providers responsible for robocalls marketing auto warranties. For the first time, we publicly disclosed the list of providers we believed were

[5] *See* https://blog.youmail.com/2022/07/july-enforcement-achieve-success-in-escalating-the-war-on-robocalls/; Car Warranty Robocalls Plummeted in Late 2022: Here's Why | RoboKiller Blog.

responsible for these calls to put other providers on notice. Then, as noted above, we followed up with a subsequent order telling every other provider to block traffic from the providers tied to the auto warranty and student loan scams.

Finally, although the Commission is using every tool at its disposal, I believe that additional authority from Congress is needed to combat robocalls and robotexts more effectively. In particular, I want to draw your attention to the issues described below.

Fix the definition of autodialer: Because robotexts are neither prerecorded nor artificial voice calls, the Telephone Consumer Protection Act (TCPA) only provides consumers protection from robotexts if they are sent from autodialers. Last year's Supreme Court decision, *Facebook v. Duguid,* narrowed the definition of autodialer under the TCPA, resulting in the law only covering equipment that generates numbers randomly and sequentially. Consequently, equipment that simply uses lists to generate robotexts means that fewer robotexts may be subject to TCPA protections, and as a result, this decision may be responsible for the rise in robotexts over the past year.

Expand tools to catch robocallers: Robocallers often create multiple entities and business relationships to cover their tracks and obscure their involvement. As a result, the Commission would benefit from statutory authority allowing it to access Bank Secrecy Act information. This would allow the agency to identify more quickly the financial records and assets of our investigative targets given the overlap between illegal robocalls and the role they play facilitating schemes to defraud and harm victims financially. In particular, our investigations would benefit from clear authority to access financial reports that institutions are required to produce regarding suspicious activities under the Bank Secrecy Act. This would permit the agency's Enforcement Bureau to access financial information about individual targets without first notifying the targets. By updating the law to allow for administrative subpoenas for all types of non-content customer records, the Commission would be able to obtain evidence that can help identify who is actually responsible for illegal robocall campaigns, and to prevent scam artists from registering new entities under new names after enforcement actions shut them down.

Increase court enforcement of fines: We vigorously pursue robocall violations, spending a great deal of time and effort to gather evidence and issue fines against violators. But when the violators refuse to pay the fines we assess, we have to hand the cases over to our colleagues at the Department of Justice (DOJ) and hope that DOJ has the resources available to pursue these cases in court. If Congress granted the Commission the authority and resources to perform this work ourselves, we could leverage the agency's existing expertise and motivation to enforce our orders.

I hope this is helpful. Please let me know if you have any further questions.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

December 23, 2022

The Honorable John W. Hickenlooper
United States Senate
B85 Russell Senate Office Building
Washington, DC 20510

Dear Senator Hickenlooper:

Thank you for your letter regarding the efforts of the Federal Communications Commission to combat illegal robocalls. Protecting consumers from illegal robocalls is one of our top consumer protection priorities, and the agency is using all its tools to address this on-going issue. Our approach to this problem has been multi-faceted. We have updated policies, pursued enforcement actions, provided consumers with new tools and education on new scam tactics, championed new technologies, and closed loopholes.

As you note, the Commission took a critical step in May when we updated our policies to address illegal robocall traffic that originates in other countries. This is important because a growing amount of the robocall traffic that we receive now comes from overseas. In fact, one study suggests as many as two-thirds of robocall campaigns may now originate from abroad. That is why we adopted an Order requiring gateway providers—the carriers that serve as the domestic entry point for calls from outside the United States—to use STIR/SHAKEN call authentication technology, register in our Robocall Mitigation Database, and comply with traceback requests from the Commission and law enforcement to help figure out from where these foreign-originated junk calls are originating. I believe these measures will help us identify and tackle the increasing number of international robocalls.

In addition, our Enforcement Bureau continues to investigate and take aggressive action against illegal robocallers. Over the past year, the Bureau's investigations have led to the Commission proposing fines ranging from $5 million to more than $299 million against companies for apparently illegal robocalls under the Telephone Consumer Protection Act.

We have also ordered the rest of the industry to block known scam robocallers. In July, the Enforcement Bureau issued a first of its kind Order directing all voice service providers in the United States to stop carrying traffic from multiple entities responsible for making billions of robocalls marketing automobile warranties. This novel approach is especially noteworthy for two reasons. First, the effort to tell all other carriers to cease taking traffic from those responsible for these warranty calls represented a new approach under our rules. Second, this effort had real impact. YouMail reported that after our action these calls dropped 80 percent from the previous month, and Robokiller said that auto warranty calls fell by over 99 percent in

the months following our action.[6] As a result, we have replicated this approach in other contexts. In particular, in December 2022, we ordered that providers block the entity responsible for an estimated 40 percent of scam student loan robocalls.

It is also worth noting that our action against the auto warranty scam was part of a broader effort at the Commission to work collaboratively with and leverage the work of state enforcement agencies on robocall matters. In the auto warranty case, we coordinated our investigation and efforts with the Ohio Attorney General. The Commission now has Memoranda of Understanding (MOU) with Attorneys General in 43 states, the District of Columbia, and Guam. These MOUs allow us to share information that will assist in efforts to prosecute bad actors behind robocalls under both federal and state law, as was done with the Ohio Attorney General. In addition, the Attorneys General of Colorado, North Carolina, and Tennessee have committed to help work with the Commission to bring their other colleagues in the states on board with this effort. We have put a premium on expanding these kind of partnerships with colleagues inside and outside of government in order to more effectively pursue enforcement actions and broadly raise consumer awareness. To this end, the Consumer and Governmental Affairs Bureau has developed partnerships with non-profit organizations, such as AARP and the National Diversity Coalition, to inform the most vulnerable consumers about common and emerging robocall scams. The Commission is also continuing to build on the consumer education partnership developed with the Federal Trade Commission during our joint spoofing awareness campaign.

Another important partnership involves our coordination with the Industry Traceback Group (ITG). The ITG was created under the TRACED Act. As you note, the ITG uses provider data to traceback and identify the source of illegal robocalls. This information and collaboration is essential to our enforcement efforts. I agree with your suggestion that increased visibility into the traceback process is likely to serve the public interest. Accordingly, I have asked the Commission's Enforcement Bureau to require the ITG to submit on a quarterly basis a unified traceback report that includes (1) an identifier for each traceback that the ITG performed during the prior quarter; (2) the date of the traceback; (3) the identity of the originating/gateway provider (or the provider furthest along in the call path that the ITG was able to identify); and (4) a basic description of the type of robocall (e.g., auto warranty, government impostor, etc.). I believe this approach will improve transparency while also protecting the integrity of our enforcement process, consumer privacy, and commercially-sensitive information that could have an adverse effect on competition if disclosed inappropriately. As you know, the Enforcement Bureau's investigative activities, including identifying potential targets of enforcement actions, benefit from confidentiality until we have collected the underlying data necessary to take public action. This is also consistent with our actions in recent years adopting a targeted approach, under existing law and recently-developed rules, to publicly disclose bad actor originating and gateway providers as sources of illegal robocalls. We have issued over two dozen cease-and-desist letters over the past two years that are designed to do just that. And we used this approach in our recent enforcement efforts against providers responsible for robocalls marketing auto warranties. For the first time, we publicly disclosed the list of providers we believed were

[6] *See* https://blog.youmail.com/2022/07/july-enforcement-achieve-success-in-escalating-the-war-on-robocalls/; Car Warranty Robocalls Plummeted in Late 2022: Here's Why | RoboKiller Blog.

responsible for these calls to put other providers on notice. Then, as noted above, we followed up with a subsequent order telling every other provider to block traffic from the providers tied to the auto warranty and student loan scams.

Finally, although the Commission is using every tool at its disposal, I believe that additional authority from Congress is needed to combat robocalls and robotexts more effectively. In particular, I want to draw your attention to the issues described below.

Fix the definition of autodialer: Because robotexts are neither prerecorded nor artificial voice calls, the Telephone Consumer Protection Act (TCPA) only provides consumers protection from robotexts if they are sent from autodialers. Last year's Supreme Court decision, *Facebook v. Duguid,* narrowed the definition of autodialer under the TCPA, resulting in the law only covering equipment that generates numbers randomly and sequentially. Consequently, equipment that simply uses lists to generate robotexts means that fewer robotexts may be subject to TCPA protections, and as a result, this decision may be responsible for the rise in robotexts over the past year.

Expand tools to catch robocallers: Robocallers often create multiple entities and business relationships to cover their tracks and obscure their involvement. As a result, the Commission would benefit from statutory authority allowing it to access Bank Secrecy Act information. This would allow the agency to identify more quickly the financial records and assets of our investigative targets given the overlap between illegal robocalls and the role they play facilitating schemes to defraud and harm victims financially. In particular, our investigations would benefit from clear authority to access financial reports that institutions are required to produce regarding suspicious activities under the Bank Secrecy Act. This would permit the agency's Enforcement Bureau to access financial information about individual targets without first notifying the targets. By updating the law to allow for administrative subpoenas for all types of non-content customer records, the Commission would be able to obtain evidence that can help identify who is actually responsible for illegal robocall campaigns, and to prevent scam artists from registering new entities under new names after enforcement actions shut them down.

Increase court enforcement of fines: We vigorously pursue robocall violations, spending a great deal of time and effort to gather evidence and issue fines against violators. But when the violators refuse to pay the fines we assess, we have to hand the cases over to our colleagues at the Department of Justice (DOJ) and hope that DOJ has the resources available to pursue these cases in court. If Congress granted the Commission the authority and resources to perform this work ourselves, we could leverage the agency's existing expertise and motivation to enforce our orders.

I hope this is helpful. Please let me know if you have any further questions.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

December 23, 2022

The Honorable Richard Blumenthal
United States Senate
706 Hart Senate Office Building
Washington, DC 20510

Dear Senator Blumenthal:

Thank you for your letter regarding the efforts of the Federal Communications Commission to combat illegal robocalls. Protecting consumers from illegal robocalls is one of our top consumer protection priorities, and the agency is using all its tools to address this on-going issue. Our approach to this problem has been multi-faceted. We have updated policies, pursued enforcement actions, provided consumers with new tools and education on new scam tactics, championed new technologies, and closed loopholes.

As you note, the Commission took a critical step in May when we updated our policies to address illegal robocall traffic that originates in other countries. This is important because a growing amount of the robocall traffic that we receive now comes from overseas. In fact, one study suggests as many as two-thirds of robocall campaigns may now originate from abroad. That is why we adopted an Order requiring gateway providers—the carriers that serve as the domestic entry point for calls from outside the United States—to use STIR/SHAKEN call authentication technology, register in our Robocall Mitigation Database, and comply with traceback requests from the Commission and law enforcement to help figure out from where these foreign-originated junk calls are originating. I believe these measures will help us identify and tackle the increasing number of international robocalls.

In addition, our Enforcement Bureau continues to investigate and take aggressive action against illegal robocallers. Over the past year, the Bureau's investigations have led to the Commission proposing fines ranging from $5 million to more than $299 million against companies for apparently illegal robocalls under the Telephone Consumer Protection Act.

We have also ordered the rest of the industry to block known scam robocallers. In July, the Enforcement Bureau issued a first of its kind Order directing all voice service providers in the United States to stop carrying traffic from multiple entities responsible for making billions of robocalls marketing automobile warranties. This novel approach is especially noteworthy for two reasons. First, the effort to tell all other carriers to cease taking traffic from those responsible for these warranty calls represented a new approach under our rules. Second, this effort had real impact. YouMail reported that after our action these calls dropped 80 percent from the previous month, and Robokiller said that auto warranty calls fell by over 99 percent in

the months following our action.[7] As a result, we have replicated this approach in other contexts. In particular, in December 2022, we ordered that providers block the entity responsible for an estimated 40 percent of scam student loan robocalls.

It is also worth noting that our action against the auto warranty scam was part of a broader effort at the Commission to work collaboratively with and leverage the work of state enforcement agencies on robocall matters. In the auto warranty case, we coordinated our investigation and efforts with the Ohio Attorney General. The Commission now has Memoranda of Understanding (MOU) with Attorneys General in 43 states, the District of Columbia, and Guam. These MOUs allow us to share information that will assist in efforts to prosecute bad actors behind robocalls under both federal and state law, as was done with the Ohio Attorney General. In addition, the Attorneys General of Colorado, North Carolina, and Tennessee have committed to help work with the Commission to bring their other colleagues in the states on board with this effort. We have put a premium on expanding these kind of partnerships with colleagues inside and outside of government in order to more effectively pursue enforcement actions and broadly raise consumer awareness. To this end, the Consumer and Governmental Affairs Bureau has developed partnerships with non-profit organizations, such as AARP and the National Diversity Coalition, to inform the most vulnerable consumers about common and emerging robocall scams. The Commission is also continuing to build on the consumer education partnership developed with the Federal Trade Commission during our joint spoofing awareness campaign.

Another important partnership involves our coordination with the Industry Traceback Group (ITG). The ITG was created under the TRACED Act. As you note, the ITG uses provider data to traceback and identify the source of illegal robocalls. This information and collaboration is essential to our enforcement efforts. I agree with your suggestion that increased visibility into the traceback process is likely to serve the public interest. Accordingly, I have asked the Commission's Enforcement Bureau to require the ITG to submit on a quarterly basis a unified traceback report that includes (1) an identifier for each traceback that the ITG performed during the prior quarter; (2) the date of the traceback; (3) the identity of the originating/gateway provider (or the provider furthest along in the call path that the ITG was able to identify); and (4) a basic description of the type of robocall (e.g., auto warranty, government impostor, etc.). I believe this approach will improve transparency while also protecting the integrity of our enforcement process, consumer privacy, and commercially-sensitive information that could have an adverse effect on competition if disclosed inappropriately. As you know, the Enforcement Bureau's investigative activities, including identifying potential targets of enforcement actions, benefit from confidentiality until we have collected the underlying data necessary to take public action. This is also consistent with our actions in recent years adopting a targeted approach, under existing law and recently-developed rules, to publicly disclose bad actor originating and gateway providers as sources of illegal robocalls. We have issued over two dozen cease-and-desist letters over the past two years that are designed to do just that. And we used this approach in our recent enforcement efforts against providers responsible for robocalls marketing auto warranties. For the first time, we publicly disclosed the list of providers we believed were

[7] *See* https://blog.youmail.com/2022/07/july-enforcement-achieve-success-in-escalating-the-war-on-robocalls/; Car Warranty Robocalls Plummeted in Late 2022: Here's Why | RoboKiller Blog.

responsible for these calls to put other providers on notice. Then, as noted above, we followed up with a subsequent order telling every other provider to block traffic from the providers tied to the auto warranty and student loan scams.

Finally, although the Commission is using every tool at its disposal, I believe that additional authority from Congress is needed to combat robocalls and robotexts more effectively. In particular, I want to draw your attention to the issues described below.

Fix the definition of autodialer: Because robotexts are neither prerecorded nor artificial voice calls, the Telephone Consumer Protection Act (TCPA) only provides consumers protection from robotexts if they are sent from autodialers. Last year's Supreme Court decision, *Facebook v. Duguid,* narrowed the definition of autodialer under the TCPA, resulting in the law only covering equipment that generates numbers randomly and sequentially. Consequently, equipment that simply uses lists to generate robotexts means that fewer robotexts may be subject to TCPA protections, and as a result, this decision may be responsible for the rise in robotexts over the past year.

Expand tools to catch robocallers: Robocallers often create multiple entities and business relationships to cover their tracks and obscure their involvement. As a result, the Commission would benefit from statutory authority allowing it to access Bank Secrecy Act information. This would allow the agency to identify more quickly the financial records and assets of our investigative targets given the overlap between illegal robocalls and the role they play facilitating schemes to defraud and harm victims financially. In particular, our investigations would benefit from clear authority to access financial reports that institutions are required to produce regarding suspicious activities under the Bank Secrecy Act. This would permit the agency's Enforcement Bureau to access financial information about individual targets without first notifying the targets. By updating the law to allow for administrative subpoenas for all types of non-content customer records, the Commission would be able to obtain evidence that can help identify who is actually responsible for illegal robocall campaigns, and to prevent scam artists from registering new entities under new names after enforcement actions shut them down.

Increase court enforcement of fines: We vigorously pursue robocall violations, spending a great deal of time and effort to gather evidence and issue fines against violators. But when the violators refuse to pay the fines we assess, we have to hand the cases over to our colleagues at the Department of Justice (DOJ) and hope that DOJ has the resources available to pursue these cases in court. If Congress granted the Commission the authority and resources to perform this work ourselves, we could leverage the agency's existing expertise and motivation to enforce our orders.

I hope this is helpful. Please let me know if you have any further questions.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

December 23, 2022

The Honorable Chris Van Hollen
United States Senate
110 Hart Senate Office Building
Washington, DC 20510

Dear Senator Van Hollen:

Thank you for your letter regarding the efforts of the Federal Communications Commission to combat illegal robocalls. Protecting consumers from illegal robocalls is one of our top consumer protection priorities, and the agency is using all its tools to address this on-going issue. Our approach to this problem has been multi-faceted. We have updated policies, pursued enforcement actions, provided consumers with new tools and education on new scam tactics, championed new technologies, and closed loopholes.

As you note, the Commission took a critical step in May when we updated our policies to address illegal robocall traffic that originates in other countries. This is important because a growing amount of the robocall traffic that we receive now comes from overseas. In fact, one study suggests as many as two-thirds of robocall campaigns may now originate from abroad. That is why we adopted an Order requiring gateway providers—the carriers that serve as the domestic entry point for calls from outside the United States—to use STIR/SHAKEN call authentication technology, register in our Robocall Mitigation Database, and comply with traceback requests from the Commission and law enforcement to help figure out from where these foreign-originated junk calls are originating. I believe these measures will help us identify and tackle the increasing number of international robocalls.

In addition, our Enforcement Bureau continues to investigate and take aggressive action against illegal robocallers. Over the past year, the Bureau's investigations have led to the Commission proposing fines ranging from $5 million to more than $299 million against companies for apparently illegal robocalls under the Telephone Consumer Protection Act.

We have also ordered the rest of the industry to block known scam robocallers. In July, the Enforcement Bureau issued a first of its kind Order directing all voice service providers in the United States to stop carrying traffic from multiple entities responsible for making billions of robocalls marketing automobile warranties. This novel approach is especially noteworthy for two reasons. First, the effort to tell all other carriers to cease taking traffic from those responsible for these warranty calls represented a new approach under our rules. Second, this effort had real impact. YouMail reported that after our action these calls dropped 80 percent from the previous month, and Robokiller said that auto warranty calls fell by over 99 percent in

the months following our action.[8] As a result, we have replicated this approach in other contexts. In particular, in December 2022, we ordered that providers block the entity responsible for an estimated 40 percent of scam student loan robocalls.

It is also worth noting that our action against the auto warranty scam was part of a broader effort at the Commission to work collaboratively with and leverage the work of state enforcement agencies on robocall matters. In the auto warranty case, we coordinated our investigation and efforts with the Ohio Attorney General. The Commission now has Memoranda of Understanding (MOU) with Attorneys General in 43 states, the District of Columbia, and Guam. These MOUs allow us to share information that will assist in efforts to prosecute bad actors behind robocalls under both federal and state law, as was done with the Ohio Attorney General. In addition, the Attorneys General of Colorado, North Carolina, and Tennessee have committed to help work with the Commission to bring their other colleagues in the states on board with this effort. We have put a premium on expanding these kind of partnerships with colleagues inside and outside of government in order to more effectively pursue enforcement actions and broadly raise consumer awareness. To this end, the Consumer and Governmental Affairs Bureau has developed partnerships with non-profit organizations, such as AARP and the National Diversity Coalition, to inform the most vulnerable consumers about common and emerging robocall scams. The Commission is also continuing to build on the consumer education partnership developed with the Federal Trade Commission during our joint spoofing awareness campaign.

Another important partnership involves our coordination with the Industry Traceback Group (ITG). The ITG was created under the TRACED Act. As you note, the ITG uses provider data to traceback and identify the source of illegal robocalls. This information and collaboration is essential to our enforcement efforts. I agree with your suggestion that increased visibility into the traceback process is likely to serve the public interest. Accordingly, I have asked the Commission's Enforcement Bureau to require the ITG to submit on a quarterly basis a unified traceback report that includes (1) an identifier for each traceback that the ITG performed during the prior quarter; (2) the date of the traceback; (3) the identity of the originating/gateway provider (or the provider furthest along in the call path that the ITG was able to identify); and (4) a basic description of the type of robocall (e.g., auto warranty, government impostor, etc.). I believe this approach will improve transparency while also protecting the integrity of our enforcement process, consumer privacy, and commercially-sensitive information that could have an adverse effect on competition if disclosed inappropriately. As you know, the Enforcement Bureau's investigative activities, including identifying potential targets of enforcement actions, benefit from confidentiality until we have collected the underlying data necessary to take public action. This is also consistent with our actions in recent years adopting a targeted approach, under existing law and recently-developed rules, to publicly disclose bad actor originating and gateway providers as sources of illegal robocalls. We have issued over two dozen cease-and-desist letters over the past two years that are designed to do just that. And we used this approach in our recent enforcement efforts against providers responsible for robocalls marketing auto warranties. For the first time, we publicly disclosed the list of providers we believed were

[8] *See* https://blog.youmail.com/2022/07/july-enforcement-achieve-success-in-escalating-the-war-on-robocalls/; Car Warranty Robocalls Plummeted in Late 2022: Here's Why | RoboKiller Blog.

responsible for these calls to put other providers on notice. Then, as noted above, we followed up with a subsequent order telling every other provider to block traffic from the providers tied to the auto warranty and student loan scams.

Finally, although the Commission is using every tool at its disposal, I believe that additional authority from Congress is needed to combat robocalls and robotexts more effectively. In particular, I want to draw your attention to the issues described below.

Fix the definition of autodialer: Because robotexts are neither prerecorded nor artificial voice calls, the Telephone Consumer Protection Act (TCPA) only provides consumers protection from robotexts if they are sent from autodialers. Last year's Supreme Court decision, *Facebook v. Duguid,* narrowed the definition of autodialer under the TCPA, resulting in the law only covering equipment that generates numbers randomly and sequentially. Consequently, equipment that simply uses lists to generate robotexts means that fewer robotexts may be subject to TCPA protections, and as a result, this decision may be responsible for the rise in robotexts over the past year.

Expand tools to catch robocallers: Robocallers often create multiple entities and business relationships to cover their tracks and obscure their involvement. As a result, the Commission would benefit from statutory authority allowing it to access Bank Secrecy Act information. This would allow the agency to identify more quickly the financial records and assets of our investigative targets given the overlap between illegal robocalls and the role they play facilitating schemes to defraud and harm victims financially. In particular, our investigations would benefit from clear authority to access financial reports that institutions are required to produce regarding suspicious activities under the Bank Secrecy Act. This would permit the agency's Enforcement Bureau to access financial information about individual targets without first notifying the targets. By updating the law to allow for administrative subpoenas for all types of non-content customer records, the Commission would be able to obtain evidence that can help identify who is actually responsible for illegal robocall campaigns, and to prevent scam artists from registering new entities under new names after enforcement actions shut them down.

Increase court enforcement of fines: We vigorously pursue robocall violations, spending a great deal of time and effort to gather evidence and issue fines against violators. But when the violators refuse to pay the fines we assess, we have to hand the cases over to our colleagues at the Department of Justice (DOJ) and hope that DOJ has the resources available to pursue these cases in court. If Congress granted the Commission the authority and resources to perform this work ourselves, we could leverage the agency's existing expertise and motivation to enforce our orders.

I hope this is helpful. Please let me know if you have any further questions.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

December 23, 2022

The Honorable Martin Heinrich
United States Senate
303 Hart Senate Office Building
Washington, DC 20510

Dear Senator Heinrich:

Thank you for your letter regarding the efforts of the Federal Communications Commission to combat illegal robocalls. Protecting consumers from illegal robocalls is one of our top consumer protection priorities, and the agency is using all its tools to address this on-going issue. Our approach to this problem has been multi-faceted. We have updated policies, pursued enforcement actions, provided consumers with new tools and education on new scam tactics, championed new technologies, and closed loopholes.

As you note, the Commission took a critical step in May when we updated our policies to address illegal robocall traffic that originates in other countries. This is important because a growing amount of the robocall traffic that we receive now comes from overseas. In fact, one study suggests as many as two-thirds of robocall campaigns may now originate from abroad. That is why we adopted an Order requiring gateway providers—the carriers that serve as the domestic entry point for calls from outside the United States—to use STIR/SHAKEN call authentication technology, register in our Robocall Mitigation Database, and comply with traceback requests from the Commission and law enforcement to help figure out from where these foreign-originated junk calls are originating. I believe these measures will help us identify and tackle the increasing number of international robocalls.

In addition, our Enforcement Bureau continues to investigate and take aggressive action against illegal robocallers. Over the past year, the Bureau's investigations have led to the Commission proposing fines ranging from $5 million to more than $299 million against companies for apparently illegal robocalls under the Telephone Consumer Protection Act.

We have also ordered the rest of the industry to block known scam robocallers. In July, the Enforcement Bureau issued a first of its kind Order directing all voice service providers in the United States to stop carrying traffic from multiple entities responsible for making billions of robocalls marketing automobile warranties. This novel approach is especially noteworthy for two reasons. First, the effort to tell all other carriers to cease taking traffic from those responsible for these warranty calls represented a new approach under our rules. Second, this effort had real impact. YouMail reported that after our action these calls dropped 80 percent from the previous month, and Robokiller said that auto warranty calls fell by over 99 percent in

the months following our action.[9] As a result, we have replicated this approach in other contexts. In particular, in December 2022, we ordered that providers block the entity responsible for an estimated 40 percent of scam student loan robocalls.

It is also worth noting that our action against the auto warranty scam was part of a broader effort at the Commission to work collaboratively with and leverage the work of state enforcement agencies on robocall matters. In the auto warranty case, we coordinated our investigation and efforts with the Ohio Attorney General. The Commission now has Memoranda of Understanding (MOU) with Attorneys General in 43 states, the District of Columbia, and Guam. These MOUs allow us to share information that will assist in efforts to prosecute bad actors behind robocalls under both federal and state law, as was done with the Ohio Attorney General. In addition, the Attorneys General of Colorado, North Carolina, and Tennessee have committed to help work with the Commission to bring their other colleagues in the states on board with this effort. We have put a premium on expanding these kind of partnerships with colleagues inside and outside of government in order to more effectively pursue enforcement actions and broadly raise consumer awareness. To this end, the Consumer and Governmental Affairs Bureau has developed partnerships with non-profit organizations, such as AARP and the National Diversity Coalition, to inform the most vulnerable consumers about common and emerging robocall scams. The Commission is also continuing to build on the consumer education partnership developed with the Federal Trade Commission during our joint spoofing awareness campaign.

Another important partnership involves our coordination with the Industry Traceback Group (ITG). The ITG was created under the TRACED Act. As you note, the ITG uses provider data to traceback and identify the source of illegal robocalls. This information and collaboration is essential to our enforcement efforts. I agree with your suggestion that increased visibility into the traceback process is likely to serve the public interest. Accordingly, I have asked the Commission's Enforcement Bureau to require the ITG to submit on a quarterly basis a unified traceback report that includes (1) an identifier for each traceback that the ITG performed during the prior quarter; (2) the date of the traceback; (3) the identity of the originating/gateway provider (or the provider furthest along in the call path that the ITG was able to identify); and (4) a basic description of the type of robocall (e.g., auto warranty, government impostor, etc.). I believe this approach will improve transparency while also protecting the integrity of our enforcement process, consumer privacy, and commercially-sensitive information that could have an adverse effect on competition if disclosed inappropriately. As you know, the Enforcement Bureau's investigative activities, including identifying potential targets of enforcement actions, benefit from confidentiality until we have collected the underlying data necessary to take public action. This is also consistent with our actions in recent years adopting a targeted approach, under existing law and recently-developed rules, to publicly disclose bad actor originating and gateway providers as sources of illegal robocalls. We have issued over two dozen cease-and-desist letters over the past two years that are designed to do just that. And we used this approach in our recent enforcement efforts against providers responsible for robocalls marketing auto warranties. For the first time, we publicly disclosed the list of providers we believed were

[9] *See* https://blog.youmail.com/2022/07/july-enforcement-achieve-success-in-escalating-the-war-on-robocalls/; Car Warranty Robocalls Plummeted in Late 2022: Here's Why | RoboKiller Blog.

responsible for these calls to put other providers on notice. Then, as noted above, we followed up with a subsequent order telling every other provider to block traffic from the providers tied to the auto warranty and student loan scams.

Finally, although the Commission is using every tool at its disposal, I believe that additional authority from Congress is needed to combat robocalls and robotexts more effectively. In particular, I want to draw your attention to the issues described below.

Fix the definition of autodialer: Because robotexts are neither prerecorded nor artificial voice calls, the Telephone Consumer Protection Act (TCPA) only provides consumers protection from robotexts if they are sent from autodialers. Last year's Supreme Court decision, *Facebook v. Duguid,* narrowed the definition of autodialer under the TCPA, resulting in the law only covering equipment that generates numbers randomly and sequentially. Consequently, equipment that simply uses lists to generate robotexts means that fewer robotexts may be subject to TCPA protections, and as a result, this decision may be responsible for the rise in robotexts over the past year.

Expand tools to catch robocallers: Robocallers often create multiple entities and business relationships to cover their tracks and obscure their involvement. As a result, the Commission would benefit from statutory authority allowing it to access Bank Secrecy Act information. This would allow the agency to identify more quickly the financial records and assets of our investigative targets given the overlap between illegal robocalls and the role they play facilitating schemes to defraud and harm victims financially. In particular, our investigations would benefit from clear authority to access financial reports that institutions are required to produce regarding suspicious activities under the Bank Secrecy Act. This would permit the agency's Enforcement Bureau to access financial information about individual targets without first notifying the targets. By updating the law to allow for administrative subpoenas for all types of non-content customer records, the Commission would be able to obtain evidence that can help identify who is actually responsible for illegal robocall campaigns, and to prevent scam artists from registering new entities under new names after enforcement actions shut them down.

Increase court enforcement of fines: We vigorously pursue robocall violations, spending a great deal of time and effort to gather evidence and issue fines against violators. But when the violators refuse to pay the fines we assess, we have to hand the cases over to our colleagues at the Department of Justice (DOJ) and hope that DOJ has the resources available to pursue these cases in court. If Congress granted the Commission the authority and resources to perform this work ourselves, we could leverage the agency's existing expertise and motivation to enforce our orders.

I hope this is helpful. Please let me know if you have any further questions.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

December 23, 2022

The Honorable Jack Reed
United States Senate
728 Hart Senate Office Building
Washington, DC 20510

Dear Senator Reed:

Thank you for your letter regarding the efforts of the Federal Communications Commission to combat illegal robocalls. Protecting consumers from illegal robocalls is one of our top consumer protection priorities, and the agency is using all its tools to address this on-going issue. Our approach to this problem has been multi-faceted. We have updated policies, pursued enforcement actions, provided consumers with new tools and education on new scam tactics, championed new technologies, and closed loopholes.

As you note, the Commission took a critical step in May when we updated our policies to address illegal robocall traffic that originates in other countries. This is important because a growing amount of the robocall traffic that we receive now comes from overseas. In fact, one study suggests as many as two-thirds of robocall campaigns may now originate from abroad. That is why we adopted an Order requiring gateway providers—the carriers that serve as the domestic entry point for calls from outside the United States—to use STIR/SHAKEN call authentication technology, register in our Robocall Mitigation Database, and comply with traceback requests from the Commission and law enforcement to help figure out from where these foreign-originated junk calls are originating. I believe these measures will help us identify and tackle the increasing number of international robocalls.

In addition, our Enforcement Bureau continues to investigate and take aggressive action against illegal robocallers. Over the past year, the Bureau's investigations have led to the Commission proposing fines ranging from $5 million to more than $299 million against companies for apparently illegal robocalls under the Telephone Consumer Protection Act.

We have also ordered the rest of the industry to block known scam robocallers. In July, the Enforcement Bureau issued a first of its kind Order directing all voice service providers in the United States to stop carrying traffic from multiple entities responsible for making billions of robocalls marketing automobile warranties. This novel approach is especially noteworthy for two reasons. First, the effort to tell all other carriers to cease taking traffic from those responsible for these warranty calls represented a new approach under our rules. Second, this effort had real impact. YouMail reported that after our action these calls dropped 80 percent from the previous month, and Robokiller said that auto warranty calls fell by over 99 percent in

the months following our action.[10] As a result, we have replicated this approach in other contexts. In particular, in December 2022, we ordered that providers block the entity responsible for an estimated 40 percent of scam student loan robocalls.

It is also worth noting that our action against the auto warranty scam was part of a broader effort at the Commission to work collaboratively with and leverage the work of state enforcement agencies on robocall matters. In the auto warranty case, we coordinated our investigation and efforts with the Ohio Attorney General. The Commission now has Memoranda of Understanding (MOU) with Attorneys General in 43 states, the District of Columbia, and Guam. These MOUs allow us to share information that will assist in efforts to prosecute bad actors behind robocalls under both federal and state law, as was done with the Ohio Attorney General. In addition, the Attorneys General of Colorado, North Carolina, and Tennessee have committed to help work with the Commission to bring their other colleagues in the states on board with this effort. We have put a premium on expanding these kind of partnerships with colleagues inside and outside of government in order to more effectively pursue enforcement actions and broadly raise consumer awareness. To this end, the Consumer and Governmental Affairs Bureau has developed partnerships with non-profit organizations, such as AARP and the National Diversity Coalition, to inform the most vulnerable consumers about common and emerging robocall scams. The Commission is also continuing to build on the consumer education partnership developed with the Federal Trade Commission during our joint spoofing awareness campaign.

Another important partnership involves our coordination with the Industry Traceback Group (ITG). The ITG was created under the TRACED Act. As you note, the ITG uses provider data to traceback and identify the source of illegal robocalls. This information and collaboration is essential to our enforcement efforts. I agree with your suggestion that increased visibility into the traceback process is likely to serve the public interest. Accordingly, I have asked the Commission's Enforcement Bureau to require the ITG to submit on a quarterly basis a unified traceback report that includes (1) an identifier for each traceback that the ITG performed during the prior quarter; (2) the date of the traceback; (3) the identity of the originating/gateway provider (or the provider furthest along in the call path that the ITG was able to identify); and (4) a basic description of the type of robocall (e.g., auto warranty, government impostor, etc.). I believe this approach will improve transparency while also protecting the integrity of our enforcement process, consumer privacy, and commercially-sensitive information that could have an adverse effect on competition if disclosed inappropriately. As you know, the Enforcement Bureau's investigative activities, including identifying potential targets of enforcement actions, benefit from confidentiality until we have collected the underlying data necessary to take public action. This is also consistent with our actions in recent years adopting a targeted approach, under existing law and recently-developed rules, to publicly disclose bad actor originating and gateway providers as sources of illegal robocalls. We have issued over two dozen cease-and-desist letters over the past two years that are designed to do just that. And we used this approach in our recent enforcement efforts against providers responsible for robocalls marketing auto warranties. For the first time, we publicly disclosed the list of providers we believed were

[10] *See* https://blog.youmail.com/2022/07/july-enforcement-achieve-success-in-escalating-the-war-on-robocalls/; Car Warranty Robocalls Plummeted in Late 2022: Here's Why | RoboKiller Blog.

responsible for these calls to put other providers on notice. Then, as noted above, we followed up with a subsequent order telling every other provider to block traffic from the providers tied to the auto warranty and student loan scams.

Finally, although the Commission is using every tool at its disposal, I believe that additional authority from Congress is needed to combat robocalls and robotexts more effectively. In particular, I want to draw your attention to the issues described below.

Fix the definition of autodialer: Because robotexts are neither prerecorded nor artificial voice calls, the Telephone Consumer Protection Act (TCPA) only provides consumers protection from robotexts if they are sent from autodialers. Last year's Supreme Court decision, *Facebook v. Duguid,* narrowed the definition of autodialer under the TCPA, resulting in the law only covering equipment that generates numbers randomly and sequentially. Consequently, equipment that simply uses lists to generate robotexts means that fewer robotexts may be subject to TCPA protections, and as a result, this decision may be responsible for the rise in robotexts over the past year.

Expand tools to catch robocallers: Robocallers often create multiple entities and business relationships to cover their tracks and obscure their involvement. As a result, the Commission would benefit from statutory authority allowing it to access Bank Secrecy Act information. This would allow the agency to identify more quickly the financial records and assets of our investigative targets given the overlap between illegal robocalls and the role they play facilitating schemes to defraud and harm victims financially. In particular, our investigations would benefit from clear authority to access financial reports that institutions are required to produce regarding suspicious activities under the Bank Secrecy Act. This would permit the agency's Enforcement Bureau to access financial information about individual targets without first notifying the targets. By updating the law to allow for administrative subpoenas for all types of non-content customer records, the Commission would be able to obtain evidence that can help identify who is actually responsible for illegal robocall campaigns, and to prevent scam artists from registering new entities under new names after enforcement actions shut them down.

Increase court enforcement of fines: We vigorously pursue robocall violations, spending a great deal of time and effort to gather evidence and issue fines against violators. But when the violators refuse to pay the fines we assess, we have to hand the cases over to our colleagues at the Department of Justice (DOJ) and hope that DOJ has the resources available to pursue these cases in court. If Congress granted the Commission the authority and resources to perform this work ourselves, we could leverage the agency's existing expertise and motivation to enforce our orders.

I hope this is helpful. Please let me know if you have any further questions.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

December 23, 2022

The Honorable Ben Ray Lujan
United States Senate
498 Russell Senate Office Building
Washington, DC 20510

Dear Chairman Lujan:

Thank you for your letter regarding the efforts of the Federal Communications Commission to combat illegal robocalls. Protecting consumers from illegal robocalls is one of our top consumer protection priorities, and the agency is using all its tools to address this on-going issue. Our approach to this problem has been multi-faceted. We have updated policies, pursued enforcement actions, provided consumers with new tools and education on new scam tactics, championed new technologies, and closed loopholes.

As you note, the Commission took a critical step in May when we updated our policies to address illegal robocall traffic that originates in other countries. This is important because a growing amount of the robocall traffic that we receive now comes from overseas. In fact, one study suggests as many as two-thirds of robocall campaigns may now originate from abroad. That is why we adopted an Order requiring gateway providers—the carriers that serve as the domestic entry point for calls from outside the United States—to use STIR/SHAKEN call authentication technology, register in our Robocall Mitigation Database, and comply with traceback requests from the Commission and law enforcement to help figure out from where these foreign-originated junk calls are originating. I believe these measures will help us identify and tackle the increasing number of international robocalls.

In addition, our Enforcement Bureau continues to investigate and take aggressive action against illegal robocallers. Over the past year, the Bureau's investigations have led to the Commission proposing fines ranging from $5 million to more than $299 million against companies for apparently illegal robocalls under the Telephone Consumer Protection Act.

We have also ordered the rest of the industry to block known scam robocallers. In July, the Enforcement Bureau issued a first of its kind Order directing all voice service providers in the United States to stop carrying traffic from multiple entities responsible for making billions of robocalls marketing automobile warranties. This novel approach is especially noteworthy for two reasons. First, the effort to tell all other carriers to cease taking traffic from those responsible for these warranty calls represented a new approach under our rules. Second, this effort had real impact. YouMail reported that after our action these calls dropped 80 percent from the previous month, and Robokiller said that auto warranty calls fell by over 99 percent in

the months following our action.[11] As a result, we have replicated this approach in other contexts. In particular, in December 2022, we ordered that providers block the entity responsible for an estimated 40 percent of scam student loan robocalls.

It is also worth noting that our action against the auto warranty scam was part of a broader effort at the Commission to work collaboratively with and leverage the work of state enforcement agencies on robocall matters. In the auto warranty case, we coordinated our investigation and efforts with the Ohio Attorney General. The Commission now has Memoranda of Understanding (MOU) with Attorneys General in 43 states, the District of Columbia, and Guam. These MOUs allow us to share information that will assist in efforts to prosecute bad actors behind robocalls under both federal and state law, as was done with the Ohio Attorney General. In addition, the Attorneys General of Colorado, North Carolina, and Tennessee have committed to help work with the Commission to bring their other colleagues in the states on board with this effort. We have put a premium on expanding these kind of partnerships with colleagues inside and outside of government in order to more effectively pursue enforcement actions and broadly raise consumer awareness. To this end, the Consumer and Governmental Affairs Bureau has developed partnerships with non-profit organizations, such as AARP and the National Diversity Coalition, to inform the most vulnerable consumers about common and emerging robocall scams. The Commission is also continuing to build on the consumer education partnership developed with the Federal Trade Commission during our joint spoofing awareness campaign.

Another important partnership involves our coordination with the Industry Traceback Group (ITG). The ITG was created under the TRACED Act. As you note, the ITG uses provider data to traceback and identify the source of illegal robocalls. This information and collaboration is essential to our enforcement efforts. I agree with your suggestion that increased visibility into the traceback process is likely to serve the public interest. Accordingly, I have asked the Commission's Enforcement Bureau to require the ITG to submit on a quarterly basis a unified traceback report that includes (1) an identifier for each traceback that the ITG performed during the prior quarter; (2) the date of the traceback; (3) the identity of the originating/gateway provider (or the provider furthest along in the call path that the ITG was able to identify); and (4) a basic description of the type of robocall (e.g., auto warranty, government impostor, etc.). I believe this approach will improve transparency while also protecting the integrity of our enforcement process, consumer privacy, and commercially-sensitive information that could have an adverse effect on competition if disclosed inappropriately. As you know, the Enforcement Bureau's investigative activities, including identifying potential targets of enforcement actions, benefit from confidentiality until we have collected the underlying data necessary to take public action. This is also consistent with our actions in recent years adopting a targeted approach, under existing law and recently-developed rules, to publicly disclose bad actor originating and gateway providers as sources of illegal robocalls. We have issued over two dozen cease-and-desist letters over the past two years that are designed to do just that. And we used this approach in our recent enforcement efforts against providers responsible for robocalls marketing auto warranties. For the first time, we publicly disclosed the list of providers we believed were

[11] *See* https://blog.youmail.com/2022/07/july-enforcement-achieve-success-in-escalating-the-war-on-robocalls/; Car Warranty Robocalls Plummeted in Late 2022: Here's Why | RoboKiller Blog.

responsible for these calls to put other providers on notice. Then, as noted above, we followed up with a subsequent order telling every other provider to block traffic from the providers tied to the auto warranty and student loan scams.

Finally, although the Commission is using every tool at its disposal, I believe that additional authority from Congress is needed to combat robocalls and robotexts more effectively. In particular, I want to draw your attention to the issues described below.

Fix the definition of autodialer: Because robotexts are neither prerecorded nor artificial voice calls, the Telephone Consumer Protection Act (TCPA) only provides consumers protection from robotexts if they are sent from autodialers. Last year's Supreme Court decision, *Facebook v. Duguid,* narrowed the definition of autodialer under the TCPA, resulting in the law only covering equipment that generates numbers randomly and sequentially. Consequently, equipment that simply uses lists to generate robotexts means that fewer robotexts may be subject to TCPA protections, and as a result, this decision may be responsible for the rise in robotexts over the past year.

Expand tools to catch robocallers: Robocallers often create multiple entities and business relationships to cover their tracks and obscure their involvement. As a result, the Commission would benefit from statutory authority allowing it to access Bank Secrecy Act information. This would allow the agency to identify more quickly the financial records and assets of our investigative targets given the overlap between illegal robocalls and the role they play facilitating schemes to defraud and harm victims financially. In particular, our investigations would benefit from clear authority to access financial reports that institutions are required to produce regarding suspicious activities under the Bank Secrecy Act. This would permit the agency's Enforcement Bureau to access financial information about individual targets without first notifying the targets. By updating the law to allow for administrative subpoenas for all types of non-content customer records, the Commission would be able to obtain evidence that can help identify who is actually responsible for illegal robocall campaigns, and to prevent scam artists from registering new entities under new names after enforcement actions shut them down.

Increase court enforcement of fines: We vigorously pursue robocall violations, spending a great deal of time and effort to gather evidence and issue fines against violators. But when the violators refuse to pay the fines we assess, we have to hand the cases over to our colleagues at the Department of Justice (DOJ) and hope that DOJ has the resources available to pursue these cases in court. If Congress granted the Commission the authority and resources to perform this work ourselves, we could leverage the agency's existing expertise and motivation to enforce our orders.

I hope this is helpful. Please let me know if you have any further questions.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

December 23, 2022

The Honorable Tammy Duckworth
United States Senate
524 Hart Senate Office Building
Washington, DC 20510

Dear Senator Duckworth:

Thank you for your letter regarding the efforts of the Federal Communications Commission to combat illegal robocalls. Protecting consumers from illegal robocalls is one of our top consumer protection priorities, and the agency is using all its tools to address this on-going issue. Our approach to this problem has been multi-faceted. We have updated policies, pursued enforcement actions, provided consumers with new tools and education on new scam tactics, championed new technologies, and closed loopholes.

As you note, the Commission took a critical step in May when we updated our policies to address illegal robocall traffic that originates in other countries. This is important because a growing amount of the robocall traffic that we receive now comes from overseas. In fact, one study suggests as many as two-thirds of robocall campaigns may now originate from abroad. That is why we adopted an Order requiring gateway providers—the carriers that serve as the domestic entry point for calls from outside the United States—to use STIR/SHAKEN call authentication technology, register in our Robocall Mitigation Database, and comply with traceback requests from the Commission and law enforcement to help figure out from where these foreign-originated junk calls are originating. I believe these measures will help us identify and tackle the increasing number of international robocalls.

In addition, our Enforcement Bureau continues to investigate and take aggressive action against illegal robocallers. Over the past year, the Bureau's investigations have led to the Commission proposing fines ranging from $5 million to more than $299 million against companies for apparently illegal robocalls under the Telephone Consumer Protection Act.

We have also ordered the rest of the industry to block known scam robocallers. In July, the Enforcement Bureau issued a first of its kind Order directing all voice service providers in the United States to stop carrying traffic from multiple entities responsible for making billions of robocalls marketing automobile warranties. This novel approach is especially noteworthy for two reasons. First, the effort to tell all other carriers to cease taking traffic from those responsible for these warranty calls represented a new approach under our rules. Second, this effort had real impact. YouMail reported that after our action these calls dropped 80 percent from the previous month, and Robokiller said that auto warranty calls fell by over 99 percent in

the months following our action.[12] As a result, we have replicated this approach in other contexts. In particular, in December 2022, we ordered that providers block the entity responsible for an estimated 40 percent of scam student loan robocalls.

It is also worth noting that our action against the auto warranty scam was part of a broader effort at the Commission to work collaboratively with and leverage the work of state enforcement agencies on robocall matters. In the auto warranty case, we coordinated our investigation and efforts with the Ohio Attorney General. The Commission now has Memoranda of Understanding (MOU) with Attorneys General in 43 states, the District of Columbia, and Guam. These MOUs allow us to share information that will assist in efforts to prosecute bad actors behind robocalls under both federal and state law, as was done with the Ohio Attorney General. In addition, the Attorneys General of Colorado, North Carolina, and Tennessee have committed to help work with the Commission to bring their other colleagues in the states on board with this effort. We have put a premium on expanding these kind of partnerships with colleagues inside and outside of government in order to more effectively pursue enforcement actions and broadly raise consumer awareness. To this end, the Consumer and Governmental Affairs Bureau has developed partnerships with non-profit organizations, such as AARP and the National Diversity Coalition, to inform the most vulnerable consumers about common and emerging robocall scams. The Commission is also continuing to build on the consumer education partnership developed with the Federal Trade Commission during our joint spoofing awareness campaign.

Another important partnership involves our coordination with the Industry Traceback Group (ITG). The ITG was created under the TRACED Act. As you note, the ITG uses provider data to traceback and identify the source of illegal robocalls. This information and collaboration is essential to our enforcement efforts. I agree with your suggestion that increased visibility into the traceback process is likely to serve the public interest. Accordingly, I have asked the Commission's Enforcement Bureau to require the ITG to submit on a quarterly basis a unified traceback report that includes (1) an identifier for each traceback that the ITG performed during the prior quarter; (2) the date of the traceback; (3) the identity of the originating/gateway provider (or the provider furthest along in the call path that the ITG was able to identify); and (4) a basic description of the type of robocall (e.g., auto warranty, government impostor, etc.). I believe this approach will improve transparency while also protecting the integrity of our enforcement process, consumer privacy, and commercially-sensitive information that could have an adverse effect on competition if disclosed inappropriately. As you know, the Enforcement Bureau's investigative activities, including identifying potential targets of enforcement actions, benefit from confidentiality until we have collected the underlying data necessary to take public action. This is also consistent with our actions in recent years adopting a targeted approach, under existing law and recently-developed rules, to publicly disclose bad actor originating and gateway providers as sources of illegal robocalls. We have issued over two dozen cease-and-desist letters over the past two years that are designed to do just that. And we used this approach in our recent enforcement efforts against providers responsible for robocalls marketing auto warranties. For the first time, we publicly disclosed the list of providers we believed were

[12] *See* https://blog.youmail.com/2022/07/july-enforcement-achieve-success-in-escalating-the-war-on-robocalls/; Car Warranty Robocalls Plummeted in Late 2022: Here's Why | RoboKiller Blog.

responsible for these calls to put other providers on notice. Then, as noted above, we followed up with a subsequent order telling every other provider to block traffic from the providers tied to the auto warranty and student loan scams.

Finally, although the Commission is using every tool at its disposal, I believe that additional authority from Congress is needed to combat robocalls and robotexts more effectively. In particular, I want to draw your attention to the issues described below.

Fix the definition of autodialer: Because robotexts are neither prerecorded nor artificial voice calls, the Telephone Consumer Protection Act (TCPA) only provides consumers protection from robotexts if they are sent from autodialers. Last year's Supreme Court decision, *Facebook v. Duguid,* narrowed the definition of autodialer under the TCPA, resulting in the law only covering equipment that generates numbers randomly and sequentially. Consequently, equipment that simply uses lists to generate robotexts means that fewer robotexts may be subject to TCPA protections, and as a result, this decision may be responsible for the rise in robotexts over the past year.

Expand tools to catch robocallers: Robocallers often create multiple entities and business relationships to cover their tracks and obscure their involvement. As a result, the Commission would benefit from statutory authority allowing it to access Bank Secrecy Act information. This would allow the agency to identify more quickly the financial records and assets of our investigative targets given the overlap between illegal robocalls and the role they play facilitating schemes to defraud and harm victims financially. In particular, our investigations would benefit from clear authority to access financial reports that institutions are required to produce regarding suspicious activities under the Bank Secrecy Act. This would permit the agency's Enforcement Bureau to access financial information about individual targets without first notifying the targets. By updating the law to allow for administrative subpoenas for all types of non-content customer records, the Commission would be able to obtain evidence that can help identify who is actually responsible for illegal robocall campaigns, and to prevent scam artists from registering new entities under new names after enforcement actions shut them down.

Increase court enforcement of fines: We vigorously pursue robocall violations, spending a great deal of time and effort to gather evidence and issue fines against violators. But when the violators refuse to pay the fines we assess, we have to hand the cases over to our colleagues at the Department of Justice (DOJ) and hope that DOJ has the resources available to pursue these cases in court. If Congress granted the Commission the authority and resources to perform this work ourselves, we could leverage the agency's existing expertise and motivation to enforce our orders.

I hope this is helpful. Please let me know if you have any further questions.

Sincerely,

Jessica Rosenworcel