



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

June 11, 2024

The Honorable Debbie Dingell
U.S. House of Representatives
116 Cannon House Office Building
Washington, DC 20515

Dear Representative Dingell:

Thank you for your letter regarding scam text messages and inquiring about what specifically can be done to stop those that impersonate financial institutions and put consumer funds and financial security at risk. I agree that when bad actors use telecommunications networks to target the public with these schemes, we should do everything we can to stop these fraudulent messages.

Using the authority it has under current law, the Federal Communications Commission has taken a series of steps to protect consumers from unlawful text messages and the scams that they can often spread.

For example, on March 16, 2023, the Commission adopted an Order that required all carriers to block texts from invalid, unallocated, or unused numbers. These numbers are highly likely to be used for fraud, so blocking them at the network level—before they even reach our phones—helps prevent consumers from engaging with bad actors behind these junk schemes.

In addition, on December 13, 2023, the Commission adopted an Order that required all carriers to block texts from numbers that the agency's Enforcement Bureau has determined are a source of illegal texts. Again, by blocking at the network level, carriers can help consumers avoid scams that depend on reaching consumers through communications. To ensure that carriers truly are blocking these texts, they are required to respond to the Enforcement Bureau certifying that they are blocking texts from the identified numbers. As part of this effort, the agency also encouraged carriers to make "email-to-text" an opt-in service. Email-to-text services, which account for a significant percentage of fraudulent text messages, allow senders to anonymously send text messages from an email account on a computer, rather than from a telephone number. The Commission encouraged providers to make this service opt-in only as a way to curb the influx of such spam text messages.

Because we understand that we will continually need to evolve our policies to stop new scams, on December 13, 2023, we also sought comment on new efforts to help protect consumers from junk texts. These include proposals to strengthen our text message blocking requirements by expanding the requirement to more service providers as well as to explore further options for blocking illegal text messages. The Commission also sought comment on using authentication practices for texting to combat text message spoofing, and on requiring

providers to respond to traceback requests for texting, similar to what we already have in place for voice calls. In addition, we sought comment on requiring providers to make email-to-text an opt-in service. The record in that proceeding closed on March 11, 2024. The staff at the agency is reviewing it now in order to determine how we can continue to take steps to protect consumers while ensuring that legitimate text messages—the ones we want—reach us without difficulty or delay.

These efforts are largely taken pursuant to the Telephone Consumer Protection Act and TRACED Act, both of which amended the Communications Act. It is also important to recognize that under the Communications Act, telecommunications carriers have special responsibilities to protect sensitive personal information. Likewise, their customers have privacy interests in protecting this information from disclosure and dissemination. To this end, Section 222 of the Communications Act requires telecommunications carriers (and interconnected VoIP service providers) to take specific steps to ensure that customer proprietary network information is adequately protected from unauthorized disclosure. As a result, the law makes clear that telecommunications carriers have a duty to protect the privacy of customer proprietary network information as well as the ways a carrier is able to obtain, use, and secure such information.

At the same time, Section 222(d) contains exceptions that allow telecommunications carriers the ability to use, disclose, or share sensitive information for certain purposes. Section 222(d)(2) allows telecommunications carriers to protect consumers from “fraudulent, abusive, or unlawful use” of the services rendered to those consumers.

These scam text messages that masquerade as financial institutions for the purpose of exploiting consumers are the kind of fraudulent, abusive, and unlawful uses of the services provided to consumers that the provisions in Section 222 of the Act were intended to cover. We will continue to strengthen our rules to stop new scams over our networks by using this authority and other tools we have in existing law.

Finally, I want you to know that I share your concerns about the dangers of illegal and fraudulent text messages and assure you that the Commission is always willing to explore options for stopping these messages before they reach consumers. Nonetheless, it is important to recognize that the strongest authority we have to combat junk texts is in the Telephone Consumer Protection Act—a law that dates to 1991. In the years since the passage of this legislation, a lot has changed in the way we communicate and the way bad actors use our connections for fraudulent schemes. For this reason, I welcome discussion of any new legislative proposals you may have on this topic.

Please let me know if I can be of any further assistance.

Sincerely,

A handwritten signature in black ink, appearing to read "Jessica Rosenworcel", with a long horizontal flourish extending to the right.

Jessica Rosenworcel



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

June 11, 2024

The Honorable Andrew R. Garbarino
U.S. House of Representatives
2344 Rayburn House Office Building
Washington, DC 20515

Dear Representative Garbarino:

Thank you for your letter regarding scam text messages and inquiring about what specifically can be done to stop those that impersonate financial institutions and put consumer funds and financial security at risk. I agree that when bad actors use telecommunications networks to target the public with these schemes, we should do everything we can to stop these fraudulent messages.

Using the authority it has under current law, the Federal Communications Commission has taken a series of steps to protect consumers from unlawful text messages and the scams that they can often spread.

For example, on March 16, 2023, the Commission adopted an Order that required all carriers to block texts from invalid, unallocated, or unused numbers. These numbers are highly likely to be used for fraud, so blocking them at the network level—before they even reach our phones—helps prevent consumers from engaging with bad actors behind these junk schemes.

In addition, on December 13, 2023, the Commission adopted an Order that required all carriers to block texts from numbers that the agency's Enforcement Bureau has determined are a source of illegal texts. Again, by blocking at the network level, carriers can help consumers avoid scams that depend on reaching consumers through communications. To ensure that carriers truly are blocking these texts, they are required to respond to the Enforcement Bureau certifying that they are blocking texts from the identified numbers. As part of this effort, the agency also encouraged carriers to make "email-to-text" an opt-in service. Email-to-text services, which account for a significant percentage of fraudulent text messages, allow senders to anonymously send text messages from an email account on a computer, rather than from a telephone number. The Commission encouraged providers to make this service opt-in only as a way to curb the influx of such spam text messages.

Because we understand that we will continually need to evolve our policies to stop new scams, on December 13, 2023, we also sought comment on new efforts to help protect consumers from junk texts. These include proposals to strengthen our text message blocking requirements by expanding the requirement to more service providers as well as to explore further options for blocking illegal text messages. The Commission also sought comment on using authentication practices for texting to combat text message spoofing, and on requiring

providers to respond to traceback requests for texting, similar to what we already have in place for voice calls. In addition, we sought comment on requiring providers to make email-to-text an opt-in service. The record in that proceeding closed on March 11, 2024. The staff at the agency is reviewing it now in order to determine how we can continue to take steps to protect consumers while ensuring that legitimate text messages—the ones we want—reach us without difficulty or delay.

These efforts are largely taken pursuant to the Telephone Consumer Protection Act and TRACED Act, both of which amended the Communications Act. It is also important to recognize that under the Communications Act, telecommunications carriers have special responsibilities to protect sensitive personal information. Likewise, their customers have privacy interests in protecting this information from disclosure and dissemination. To this end, Section 222 of the Communications Act requires telecommunications carriers (and interconnected VoIP service providers) to take specific steps to ensure that customer proprietary network information is adequately protected from unauthorized disclosure. As a result, the law makes clear that telecommunications carriers have a duty to protect the privacy of customer proprietary network information as well as the ways a carrier is able to obtain, use, and secure such information.

At the same time, Section 222(d) contains exceptions that allow telecommunications carriers the ability to use, disclose, or share sensitive information for certain purposes. Section 222(d)(2) allows telecommunications carriers to protect consumers from “fraudulent, abusive, or unlawful use” of the services rendered to those consumers.

These scam text messages that masquerade as financial institutions for the purpose of exploiting consumers are the kind of fraudulent, abusive, and unlawful uses of the services provided to consumers that the provisions in Section 222 of the Act were intended to cover. We will continue to strengthen our rules to stop new scams over our networks by using this authority and other tools we have in existing law.

Finally, I want you to know that I share your concerns about the dangers of illegal and fraudulent text messages and assure you that the Commission is always willing to explore options for stopping these messages before they reach consumers. Nonetheless, it is important to recognize that the strongest authority we have to combat junk texts is in the Telephone Consumer Protection Act—a law that dates to 1991. In the years since the passage of this legislation, a lot has changed in the way we communicate and the way bad actors use our connections for fraudulent schemes. For this reason, I welcome discussion of any new legislative proposals you may have on this topic.

Please let me know if I can be of any further assistance.

Sincerely,

A handwritten signature in black ink, appearing to read "Jessica Rosenworcel", with a long horizontal line extending to the right.

Jessica Rosenworcel



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

June 11, 2024

The Honorable Josh Gottheimer
U.S. House of Representatives
203 Cannon House Office Building
Washington, DC 20515

Dear Representative Gottheimer:

Thank you for your letter regarding scam text messages and inquiring about what specifically can be done to stop those that impersonate financial institutions and put consumer funds and financial security at risk. I agree that when bad actors use telecommunications networks to target the public with these schemes, we should do everything we can to stop these fraudulent messages.

Using the authority it has under current law, the Federal Communications Commission has taken a series of steps to protect consumers from unlawful text messages and the scams that they can often spread.

For example, on March 16, 2023, the Commission adopted an Order that required all carriers to block texts from invalid, unallocated, or unused numbers. These numbers are highly likely to be used for fraud, so blocking them at the network level—before they even reach our phones—helps prevent consumers from engaging with bad actors behind these junk schemes.

In addition, on December 13, 2023, the Commission adopted an Order that required all carriers to block texts from numbers that the agency's Enforcement Bureau has determined are a source of illegal texts. Again, by blocking at the network level, carriers can help consumers avoid scams that depend on reaching consumers through communications. To ensure that carriers truly are blocking these texts, they are required to respond to the Enforcement Bureau certifying that they are blocking texts from the identified numbers. As part of this effort, the agency also encouraged carriers to make "email-to-text" an opt-in service. Email-to-text services, which account for a significant percentage of fraudulent text messages, allow senders to anonymously send text messages from an email account on a computer, rather than from a telephone number. The Commission encouraged providers to make this service opt-in only as a way to curb the influx of such spam text messages.

Because we understand that we will continually need to evolve our policies to stop new scams, on December 13, 2023, we also sought comment on new efforts to help protect consumers from junk texts. These include proposals to strengthen our text message blocking requirements by expanding the requirement to more service providers as well as to explore further options for blocking illegal text messages. The Commission also sought comment on using authentication practices for texting to combat text message spoofing, and on requiring

providers to respond to traceback requests for texting, similar to what we already have in place for voice calls. In addition, we sought comment on requiring providers to make email-to-text an opt-in service. The record in that proceeding closed on March 11, 2024. The staff at the agency is reviewing it now in order to determine how we can continue to take steps to protect consumers while ensuring that legitimate text messages—the ones we want—reach us without difficulty or delay.

These efforts are largely taken pursuant to the Telephone Consumer Protection Act and TRACED Act, both of which amended the Communications Act. It is also important to recognize that under the Communications Act, telecommunications carriers have special responsibilities to protect sensitive personal information. Likewise, their customers have privacy interests in protecting this information from disclosure and dissemination. To this end, Section 222 of the Communications Act requires telecommunications carriers (and interconnected VoIP service providers) to take specific steps to ensure that customer proprietary network information is adequately protected from unauthorized disclosure. As a result, the law makes clear that telecommunications carriers have a duty to protect the privacy of customer proprietary network information as well as the ways a carrier is able to obtain, use, and secure such information.

At the same time, Section 222(d) contains exceptions that allow telecommunications carriers the ability to use, disclose, or share sensitive information for certain purposes. Section 222(d)(2) allows telecommunications carriers to protect consumers from “fraudulent, abusive, or unlawful use” of the services rendered to those consumers.

These scam text messages that masquerade as financial institutions for the purpose of exploiting consumers are the kind of fraudulent, abusive, and unlawful uses of the services provided to consumers that the provisions in Section 222 of the Act were intended to cover. We will continue to strengthen our rules to stop new scams over our networks by using this authority and other tools we have in existing law.

Finally, I want you to know that I share your concerns about the dangers of illegal and fraudulent text messages and assure you that the Commission is always willing to explore options for stopping these messages before they reach consumers. Nonetheless, it is important to recognize that the strongest authority we have to combat junk texts is in the Telephone Consumer Protection Act—a law that dates to 1991. In the years since the passage of this legislation, a lot has changed in the way we communicate and the way bad actors use our connections for fraudulent schemes. For this reason, I welcome discussion of any new legislative proposals you may have on this topic.

Please let me know if I can be of any further assistance.

Sincerely,

A handwritten signature in black ink, appearing to read "Jessica Rosenworcel", with a long horizontal flourish extending to the right.

Jessica Rosenworcel



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

June 11, 2024

The Honorable Jay Obernolte
U.S. House of Representatives
1091 Longworth House Office Building
Washington, DC 20515

Dear Representative Obernolte:

Thank you for your letter regarding scam text messages and inquiring about what specifically can be done to stop those that impersonate financial institutions and put consumer funds and financial security at risk. I agree that when bad actors use telecommunications networks to target the public with these schemes, we should do everything we can to stop these fraudulent messages.

Using the authority it has under current law, the Federal Communications Commission has taken a series of steps to protect consumers from unlawful text messages and the scams that they can often spread.

For example, on March 16, 2023, the Commission adopted an Order that required all carriers to block texts from invalid, unallocated, or unused numbers. These numbers are highly likely to be used for fraud, so blocking them at the network level—before they even reach our phones—helps prevent consumers from engaging with bad actors behind these junk schemes.

In addition, on December 13, 2023, the Commission adopted an Order that required all carriers to block texts from numbers that the agency's Enforcement Bureau has determined are a source of illegal texts. Again, by blocking at the network level, carriers can help consumers avoid scams that depend on reaching consumers through communications. To ensure that carriers truly are blocking these texts, they are required to respond to the Enforcement Bureau certifying that they are blocking texts from the identified numbers. As part of this effort, the agency also encouraged carriers to make "email-to-text" an opt-in service. Email-to-text services, which account for a significant percentage of fraudulent text messages, allow senders to anonymously send text messages from an email account on a computer, rather than from a telephone number. The Commission encouraged providers to make this service opt-in only as a way to curb the influx of such spam text messages.

Because we understand that we will continually need to evolve our policies to stop new scams, on December 13, 2023, we also sought comment on new efforts to help protect consumers from junk texts. These include proposals to strengthen our text message blocking requirements by expanding the requirement to more service providers as well as to explore further options for blocking illegal text messages. The Commission also sought comment on using authentication practices for texting to combat text message spoofing, and on requiring

providers to respond to traceback requests for texting, similar to what we already have in place for voice calls. In addition, we sought comment on requiring providers to make email-to-text an opt-in service. The record in that proceeding closed on March 11, 2024. The staff at the agency is reviewing it now in order to determine how we can continue to take steps to protect consumers while ensuring that legitimate text messages—the ones we want—reach us without difficulty or delay.

These efforts are largely taken pursuant to the Telephone Consumer Protection Act and TRACED Act, both of which amended the Communications Act. It is also important to recognize that under the Communications Act, telecommunications carriers have special responsibilities to protect sensitive personal information. Likewise, their customers have privacy interests in protecting this information from disclosure and dissemination. To this end, Section 222 of the Communications Act requires telecommunications carriers (and interconnected VoIP service providers) to take specific steps to ensure that customer proprietary network information is adequately protected from unauthorized disclosure. As a result, the law makes clear that telecommunications carriers have a duty to protect the privacy of customer proprietary network information as well as the ways a carrier is able to obtain, use, and secure such information.

At the same time, Section 222(d) contains exceptions that allow telecommunications carriers the ability to use, disclose, or share sensitive information for certain purposes. Section 222(d)(2) allows telecommunications carriers to protect consumers from “fraudulent, abusive, or unlawful use” of the services rendered to those consumers.

These scam text messages that masquerade as financial institutions for the purpose of exploiting consumers are the kind of fraudulent, abusive, and unlawful uses of the services provided to consumers that the provisions in Section 222 of the Act were intended to cover. We will continue to strengthen our rules to stop new scams over our networks by using this authority and other tools we have in existing law.

Finally, I want you to know that I share your concerns about the dangers of illegal and fraudulent text messages and assure you that the Commission is always willing to explore options for stopping these messages before they reach consumers. Nonetheless, it is important to recognize that the strongest authority we have to combat junk texts is in the Telephone Consumer Protection Act—a law that dates to 1991. In the years since the passage of this legislation, a lot has changed in the way we communicate and the way bad actors use our connections for fraudulent schemes. For this reason, I welcome discussion of any new legislative proposals you may have on this topic.

Please let me know if I can be of any further assistance.

Sincerely,

A handwritten signature in black ink, appearing to read "Jessica Rosenworcel", with a long horizontal flourish extending to the right.

Jessica Rosenworcel