FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

April 23, 2024

The Honorable Kat Cammack
U.S. House of Representatives
2421 Rayburn House Office Building
Washington, DC 20515

Dear Representative Cammack:

Thank you for your letter regarding the *Data Breach Reporting Requirements* proceeding at the Federal Communications Commission. On December 13, 2023, the agency adopted an order updating its data breach policies.

It had been sixteen years since the Commission last updated its policies to protect consumers from data breaches. In the intervening time a lot has changed about when, where, and how consumers use their phones, and what data providers collect about them when we do. That is why the updates we made are vital. They help protect consumers from digital age data breaches and reinforce the obligation carriers have to protect the privacy and security of consumer data under the Communications Act.

First, we modernized our data breach rules to make clear they include all personally identifiable information. In the past, these rules have only prohibited the disclosure of information about who we call and when. But we know now that data breaches often involve the leak of other sensitive information like our social security numbers and financial data—so we made sure our rules prohibit their disclosure, too.

Second, we made clear that our rules cover intentional and inadvertent disclosure of customer information. Our past policies only accounted for intentional leaks. But every consumer deserves protection regardless of whether the release of their personal information was on purpose or accidental.

Third, we updated our standards for notification to ensure that a carrier must inform the Commission, in addition to law enforcement, and customers of a breach and what personal information may be at risk in a timely manner. The agency's previous rules required carriers to wait seven business days before telling consumers what breaches had taken place. This approach was clearly dated. If there is a leak of your personal and financial information, you want to know as soon as possible.

Finally, we also made clear that these policies apply to telecommunications relay service providers, so that those with disabilities get the same protections as everyone else.

In taking this action, the Commission acted in a manner consistent with the Congressional Review Act. The Congressional Review Act states that an agency rule "may not be reissued in substantially the same form, and a new rule that is substantially the same as such a rule may not be issued, unless the reissued or new rule is specifically authorized by a law enacted after the date of the joint resolution disapproving the original rule." 5 U.S.C. § 801(b)(2).

In the order updating the Commission's data breach policies that was adopted on December 13, 2023, the agency addressed why the decision does not take any action or issue any rules that are prohibited by the Congressional Review Act.

To understand why, it is important to recognize that in this decision the Commission revised its rules governing when telecommunications carriers, providers of interconnected Voice over Internet Protocol services, and providers of telecommunications relay service must report breaches of customer information to governmental entities and affected consumers. On the other hand, the decision in 2016 that was the subject of Congressional Review Act action was focused on adopting privacy rules for broadband internet access service. These are different services. That means when the decision from 2016 is viewed as a whole, there is little point-to-point comparison between it and the order adopted in 2023.

The 2023 order also explains that, even if the "substantially the same" analysis were conducted on a more granular basis, these more recent breach notification requirements would not be barred because they are not substantially the same as the breach notification requirements adopted in the 2016 order. For example, the customer notification requirement adopted in 2023 is materially less prescriptive regarding the content and manner of customer notice than what the Commission adopted in 2016. Further, the 2016 rules for customer notifications and government agency notifications did not incorporate the good-faith exception from the definition of covered breaches adopted in 2023. With respect to the federal agency notification requirements, as compared to the 2016 rules, the 2023 rules provide for the Commission and other law enforcement agencies to gain a much more complete picture of data breaches, including trends and emerging activities, consistent with the demonstrated need for such oversight.

Finally, the legislative history of the Congressional Review Act makes clear that an agency is not foreclosed from further action in the same substantive area as a disapproved rule. Instead, when taking action in that area, the agency should look to "the debate on any resolution of disapproval" to understand "the congressional intent regarding the agency's options or lack thereof after enactment of a joint resolution of disapproval."[1] As the 2023 order observed, members of Congress speaking in support of the 2017 resolution of disapproval highlighted aspects of the 2016 order that imposed privacy obligations on internet service providers. Breach reporting obligations for voice providers—the subject of the 2023 order—were not the focus of these statements.

[1] Statement for the Record by Senators Nickles, Reid, and Stevens, 142 Cong. Rec. S3686 (Apr. 18, 1996) (post-enactment).

I appreciate your interest in this matter. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

April 23, 2024

The Honorable Neal Patrick Dunn
U.S. House of Representatives
466 Cannon House Office Building
Washington, DC 20515

Dear Representative Dunn:

Thank you for your letter regarding the *Data Breach Reporting Requirements* proceeding at the Federal Communications Commission. On December 13, 2023, the agency adopted an order updating its data breach policies.

It had been sixteen years since the Commission last updated its policies to protect consumers from data breaches. In the intervening time a lot has changed about when, where, and how consumers use their phones, and what data providers collect about them when we do. That is why the updates we made are vital. They help protect consumers from digital age data breaches and reinforce the obligation carriers have to protect the privacy and security of consumer data under the Communications Act.

First, we modernized our data breach rules to make clear they include all personally identifiable information. In the past, these rules have only prohibited the disclosure of information about who we call and when. But we know now that data breaches often involve the leak of other sensitive information like our social security numbers and financial data—so we made sure our rules prohibit their disclosure, too.

Second, we made clear that our rules cover intentional and inadvertent disclosure of customer information. Our past policies only accounted for intentional leaks. But every consumer deserves protection regardless of whether the release of their personal information was on purpose or accidental.

Third, we updated our standards for notification to ensure that a carrier must inform the Commission, in addition to law enforcement, and customers of a breach and what personal information may be at risk in a timely manner. The agency's previous rules required carriers to wait seven business days before telling consumers what breaches had taken place. This approach was clearly dated. If there is a leak of your personal and financial information, you want to know as soon as possible.

Finally, we also made clear that these policies apply to telecommunications relay service providers, so that those with disabilities get the same protections as everyone else.

In taking this action, the Commission acted in a manner consistent with the Congressional Review Act. The Congressional Review Act states that an agency rule "may not be reissued in substantially the same form, and a new rule that is substantially the same as such a rule may not be issued, unless the reissued or new rule is specifically authorized by a law enacted after the date of the joint resolution disapproving the original rule." 5 U.S.C. § 801(b)(2).

In the order updating the Commission's data breach policies that was adopted on December 13, 2023, the agency addressed why the decision does not take any action or issue any rules that are prohibited by the Congressional Review Act.

To understand why, it is important to recognize that in this decision the Commission revised its rules governing when telecommunications carriers, providers of interconnected Voice over Internet Protocol services, and providers of telecommunications relay service must report breaches of customer information to governmental entities and affected consumers. On the other hand, the decision in 2016 that was the subject of Congressional Review Act action was focused on adopting privacy rules for broadband internet access service. These are different services. That means when the decision from 2016 is viewed as a whole, there is little point-to-point comparison between it and the order adopted in 2023.

The 2023 order also explains that, even if the "substantially the same" analysis were conducted on a more granular basis, these more recent breach notification requirements would not be barred because they are not substantially the same as the breach notification requirements adopted in the 2016 order. For example, the customer notification requirement adopted in 2023 is materially less prescriptive regarding the content and manner of customer notice than what the Commission adopted in 2016. Further, the 2016 rules for customer notifications and government agency notifications did not incorporate the good-faith exception from the definition of covered breaches adopted in 2023. With respect to the federal agency notification requirements, as compared to the 2016 rules, the 2023 rules provide for the Commission and other law enforcement agencies to gain a much more complete picture of data breaches, including trends and emerging activities, consistent with the demonstrated need for such oversight.

Finally, the legislative history of the Congressional Review Act makes clear that an agency is not foreclosed from further action in the same substantive area as a disapproved rule. Instead, when taking action in that area, the agency should look to "the debate on any resolution of disapproval" to understand "the congressional intent regarding the agency's options or lack thereof after enactment of a joint resolution of disapproval."[1] As the 2023 order observed, members of Congress speaking in support of the 2017 resolution of disapproval highlighted aspects of the 2016 order that imposed privacy obligations on internet service providers. Breach reporting obligations for voice providers—the subject of the 2023 order—were not the focus of these statements.

[1] Statement for the Record by Senators Nickles, Reid, and Stevens, 142 Cong. Rec. S3686 (Apr. 18, 1996) (post-enactment).

I appreciate your interest in this matter. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

April 23, 2024

The Honorable Gus Bilirakis
U.S. House of Representatives
2306 Rayburn House Office Building
Washington, DC 20515

Dear Representative Bilirakis:

Thank you for your letter regarding the *Data Breach Reporting Requirements* proceeding at the Federal Communications Commission. On December 13, 2023, the agency adopted an order updating its data breach policies.

It had been sixteen years since the Commission last updated its policies to protect consumers from data breaches. In the intervening time a lot has changed about when, where, and how consumers use their phones, and what data providers collect about them when we do. That is why the updates we made are vital. They help protect consumers from digital age data breaches and reinforce the obligation carriers have to protect the privacy and security of consumer data under the Communications Act.

First, we modernized our data breach rules to make clear they include all personally identifiable information. In the past, these rules have only prohibited the disclosure of information about who we call and when. But we know now that data breaches often involve the leak of other sensitive information like our social security numbers and financial data—so we made sure our rules prohibit their disclosure, too.

Second, we made clear that our rules cover intentional and inadvertent disclosure of customer information. Our past policies only accounted for intentional leaks. But every consumer deserves protection regardless of whether the release of their personal information was on purpose or accidental.

Third, we updated our standards for notification to ensure that a carrier must inform the Commission, in addition to law enforcement, and customers of a breach and what personal information may be at risk in a timely manner. The agency's previous rules required carriers to wait seven business days before telling consumers what breaches had taken place. This approach was clearly dated. If there is a leak of your personal and financial information, you want to know as soon as possible.

Finally, we also made clear that these policies apply to telecommunications relay service providers, so that those with disabilities get the same protections as everyone else.

In taking this action, the Commission acted in a manner consistent with the Congressional Review Act. The Congressional Review Act states that an agency rule "may not be reissued in substantially the same form, and a new rule that is substantially the same as such a rule may not be issued, unless the reissued or new rule is specifically authorized by a law enacted after the date of the joint resolution disapproving the original rule." 5 U.S.C. § 801(b)(2).

In the order updating the Commission's data breach policies that was adopted on December 13, 2023, the agency addressed why the decision does not take any action or issue any rules that are prohibited by the Congressional Review Act.

To understand why, it is important to recognize that in this decision the Commission revised its rules governing when telecommunications carriers, providers of interconnected Voice over Internet Protocol services, and providers of telecommunications relay service must report breaches of customer information to governmental entities and affected consumers. On the other hand, the decision in 2016 that was the subject of Congressional Review Act action was focused on adopting privacy rules for broadband internet access service. These are different services. That means when the decision from 2016 is viewed as a whole, there is little point-to-point comparison between it and the order adopted in 2023.

The 2023 order also explains that, even if the "substantially the same" analysis were conducted on a more granular basis, these more recent breach notification requirements would not be barred because they are not substantially the same as the breach notification requirements adopted in the 2016 order. For example, the customer notification requirement adopted in 2023 is materially less prescriptive regarding the content and manner of customer notice than what the Commission adopted in 2016. Further, the 2016 rules for customer notifications and government agency notifications did not incorporate the good-faith exception from the definition of covered breaches adopted in 2023. With respect to the federal agency notification requirements, as compared to the 2016 rules, the 2023 rules provide for the Commission and other law enforcement agencies to gain a much more complete picture of data breaches, including trends and emerging activities, consistent with the demonstrated need for such oversight.

Finally, the legislative history of the Congressional Review Act makes clear that an agency is not foreclosed from further action in the same substantive area as a disapproved rule. Instead, when taking action in that area, the agency should look to "the debate on any resolution of disapproval" to understand "the congressional intent regarding the agency's options or lack thereof after enactment of a joint resolution of disapproval."[1] As the 2023 order observed, members of Congress speaking in support of the 2017 resolution of disapproval highlighted aspects of the 2016 order that imposed privacy obligations on internet service providers. Breach reporting obligations for voice providers—the subject of the 2023 order—were not the focus of these statements.

[1] Statement for the Record by Senators Nickles, Reid, and Stevens, 142 Cong. Rec. S3686 (Apr. 18, 1996) (post-enactment).

I appreciate your interest in this matter. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

April 23, 2024

The Honorable Morgan Griffith
U.S. House of Representatives
2202 Rayburn House Office Building
Washington, DC 20515

Dear Representative Griffith:

Thank you for your letter regarding the *Data Breach Reporting Requirements* proceeding at the Federal Communications Commission. On December 13, 2023, the agency adopted an order updating its data breach policies.

It had been sixteen years since the Commission last updated its policies to protect consumers from data breaches. In the intervening time a lot has changed about when, where, and how consumers use their phones, and what data providers collect about them when we do. That is why the updates we made are vital. They help protect consumers from digital age data breaches and reinforce the obligation carriers have to protect the privacy and security of consumer data under the Communications Act.

First, we modernized our data breach rules to make clear they include all personally identifiable information. In the past, these rules have only prohibited the disclosure of information about who we call and when. But we know now that data breaches often involve the leak of other sensitive information like our social security numbers and financial data—so we made sure our rules prohibit their disclosure, too.

Second, we made clear that our rules cover intentional and inadvertent disclosure of customer information. Our past policies only accounted for intentional leaks. But every consumer deserves protection regardless of whether the release of their personal information was on purpose or accidental.

Third, we updated our standards for notification to ensure that a carrier must inform the Commission, in addition to law enforcement, and customers of a breach and what personal information may be at risk in a timely manner. The agency's previous rules required carriers to wait seven business days before telling consumers what breaches had taken place. This approach was clearly dated. If there is a leak of your personal and financial information, you want to know as soon as possible.

Finally, we also made clear that these policies apply to telecommunications relay service providers, so that those with disabilities get the same protections as everyone else.

In taking this action, the Commission acted in a manner consistent with the Congressional Review Act. The Congressional Review Act states that an agency rule "may not be reissued in substantially the same form, and a new rule that is substantially the same as such a rule may not be issued, unless the reissued or new rule is specifically authorized by a law enacted after the date of the joint resolution disapproving the original rule." 5 U.S.C. § 801(b)(2).

In the order updating the Commission's data breach policies that was adopted on December 13, 2023, the agency addressed why the decision does not take any action or issue any rules that are prohibited by the Congressional Review Act.

To understand why, it is important to recognize that in this decision the Commission revised its rules governing when telecommunications carriers, providers of interconnected Voice over Internet Protocol services, and providers of telecommunications relay service must report breaches of customer information to governmental entities and affected consumers. On the other hand, the decision in 2016 that was the subject of Congressional Review Act action was focused on adopting privacy rules for broadband internet access service. These are different services. That means when the decision from 2016 is viewed as a whole, there is little point-to-point comparison between it and the order adopted in 2023.

The 2023 order also explains that, even if the "substantially the same" analysis were conducted on a more granular basis, these more recent breach notification requirements would not be barred because they are not substantially the same as the breach notification requirements adopted in the 2016 order. For example, the customer notification requirement adopted in 2023 is materially less prescriptive regarding the content and manner of customer notice than what the Commission adopted in 2016. Further, the 2016 rules for customer notifications and government agency notifications did not incorporate the good-faith exception from the definition of covered breaches adopted in 2023. With respect to the federal agency notification requirements, as compared to the 2016 rules, the 2023 rules provide for the Commission and other law enforcement agencies to gain a much more complete picture of data breaches, including trends and emerging activities, consistent with the demonstrated need for such oversight.

Finally, the legislative history of the Congressional Review Act makes clear that an agency is not foreclosed from further action in the same substantive area as a disapproved rule. Instead, when taking action in that area, the agency should look to "the debate on any resolution of disapproval" to understand "the congressional intent regarding the agency's options or lack thereof after enactment of a joint resolution of disapproval."[1] As the 2023 order observed, members of Congress speaking in support of the 2017 resolution of disapproval highlighted aspects of the 2016 order that imposed privacy obligations on internet service providers. Breach reporting obligations for voice providers—the subject of the 2023 order—were not the focus of these statements.

[1] Statement for the Record by Senators Nickles, Reid, and Stevens, 142 Cong. Rec. S3686 (Apr. 18, 1996) (post-enactment).

I appreciate your interest in this matter. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

April 23, 2024

The Honorable Randy Weber
U.S. House of Representatives
107 Cannon House Office Building
Washington, DC 20515

Dear Representative Weber:

Thank you for your letter regarding the *Data Breach Reporting Requirements* proceeding at the Federal Communications Commission. On December 13, 2023, the agency adopted an order updating its data breach policies.

It had been sixteen years since the Commission last updated its policies to protect consumers from data breaches. In the intervening time a lot has changed about when, where, and how consumers use their phones, and what data providers collect about them when we do. That is why the updates we made are vital. They help protect consumers from digital age data breaches and reinforce the obligation carriers have to protect the privacy and security of consumer data under the Communications Act.

First, we modernized our data breach rules to make clear they include all personally identifiable information. In the past, these rules have only prohibited the disclosure of information about who we call and when. But we know now that data breaches often involve the leak of other sensitive information like our social security numbers and financial data—so we made sure our rules prohibit their disclosure, too.

Second, we made clear that our rules cover intentional and inadvertent disclosure of customer information. Our past policies only accounted for intentional leaks. But every consumer deserves protection regardless of whether the release of their personal information was on purpose or accidental.

Third, we updated our standards for notification to ensure that a carrier must inform the Commission, in addition to law enforcement, and customers of a breach and what personal information may be at risk in a timely manner. The agency's previous rules required carriers to wait seven business days before telling consumers what breaches had taken place. This approach was clearly dated. If there is a leak of your personal and financial information, you want to know as soon as possible.

Finally, we also made clear that these policies apply to telecommunications relay service providers, so that those with disabilities get the same protections as everyone else.

In taking this action, the Commission acted in a manner consistent with the Congressional Review Act. The Congressional Review Act states that an agency rule "may not be reissued in substantially the same form, and a new rule that is substantially the same as such a rule may not be issued, unless the reissued or new rule is specifically authorized by a law enacted after the date of the joint resolution disapproving the original rule." 5 U.S.C. § 801(b)(2).

In the order updating the Commission's data breach policies that was adopted on December 13, 2023, the agency addressed why the decision does not take any action or issue any rules that are prohibited by the Congressional Review Act.

To understand why, it is important to recognize that in this decision the Commission revised its rules governing when telecommunications carriers, providers of interconnected Voice over Internet Protocol services, and providers of telecommunications relay service must report breaches of customer information to governmental entities and affected consumers. On the other hand, the decision in 2016 that was the subject of Congressional Review Act action was focused on adopting privacy rules for broadband internet access service. These are different services. That means when the decision from 2016 is viewed as a whole, there is little point-to-point comparison between it and the order adopted in 2023.

The 2023 order also explains that, even if the "substantially the same" analysis were conducted on a more granular basis, these more recent breach notification requirements would not be barred because they are not substantially the same as the breach notification requirements adopted in the 2016 order. For example, the customer notification requirement adopted in 2023 is materially less prescriptive regarding the content and manner of customer notice than what the Commission adopted in 2016. Further, the 2016 rules for customer notifications and government agency notifications did not incorporate the good-faith exception from the definition of covered breaches adopted in 2023. With respect to the federal agency notification requirements, as compared to the 2016 rules, the 2023 rules provide for the Commission and other law enforcement agencies to gain a much more complete picture of data breaches, including trends and emerging activities, consistent with the demonstrated need for such oversight.

Finally, the legislative history of the Congressional Review Act makes clear that an agency is not foreclosed from further action in the same substantive area as a disapproved rule. Instead, when taking action in that area, the agency should look to "the debate on any resolution of disapproval" to understand "the congressional intent regarding the agency's options or lack thereof after enactment of a joint resolution of disapproval."[1] As the 2023 order observed, members of Congress speaking in support of the 2017 resolution of disapproval highlighted aspects of the 2016 order that imposed privacy obligations on internet service providers. Breach reporting obligations for voice providers—the subject of the 2023 order—were not the focus of these statements.

[1] Statement for the Record by Senators Nickles, Reid, and Stevens, 142 Cong. Rec. S3686 (Apr. 18, 1996) (post-enactment).

I appreciate your interest in this matter. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

April 23, 2024

The Honorable Larry Bucshon
U.S. House of Representatives
2313 Rayburn House Office Building
Washington, DC 20515

Dear Representative Bucshon:

Thank you for your letter regarding the *Data Breach Reporting Requirements* proceeding at the Federal Communications Commission. On December 13, 2023, the agency adopted an order updating its data breach policies.

It had been sixteen years since the Commission last updated its policies to protect consumers from data breaches. In the intervening time a lot has changed about when, where, and how consumers use their phones, and what data providers collect about them when we do. That is why the updates we made are vital. They help protect consumers from digital age data breaches and reinforce the obligation carriers have to protect the privacy and security of consumer data under the Communications Act.

First, we modernized our data breach rules to make clear they include all personally identifiable information. In the past, these rules have only prohibited the disclosure of information about who we call and when. But we know now that data breaches often involve the leak of other sensitive information like our social security numbers and financial data—so we made sure our rules prohibit their disclosure, too.

Second, we made clear that our rules cover intentional and inadvertent disclosure of customer information. Our past policies only accounted for intentional leaks. But every consumer deserves protection regardless of whether the release of their personal information was on purpose or accidental.

Third, we updated our standards for notification to ensure that a carrier must inform the Commission, in addition to law enforcement, and customers of a breach and what personal information may be at risk in a timely manner. The agency's previous rules required carriers to wait seven business days before telling consumers what breaches had taken place. This approach was clearly dated. If there is a leak of your personal and financial information, you want to know as soon as possible.

Finally, we also made clear that these policies apply to telecommunications relay service providers, so that those with disabilities get the same protections as everyone else.

In taking this action, the Commission acted in a manner consistent with the Congressional Review Act. The Congressional Review Act states that an agency rule "may not be reissued in substantially the same form, and a new rule that is substantially the same as such a rule may not be issued, unless the reissued or new rule is specifically authorized by a law enacted after the date of the joint resolution disapproving the original rule." 5 U.S.C. § 801(b)(2).

In the order updating the Commission's data breach policies that was adopted on December 13, 2023, the agency addressed why the decision does not take any action or issue any rules that are prohibited by the Congressional Review Act.

To understand why, it is important to recognize that in this decision the Commission revised its rules governing when telecommunications carriers, providers of interconnected Voice over Internet Protocol services, and providers of telecommunications relay service must report breaches of customer information to governmental entities and affected consumers. On the other hand, the decision in 2016 that was the subject of Congressional Review Act action was focused on adopting privacy rules for broadband internet access service. These are different services. That means when the decision from 2016 is viewed as a whole, there is little point-to-point comparison between it and the order adopted in 2023.

The 2023 order also explains that, even if the "substantially the same" analysis were conducted on a more granular basis, these more recent breach notification requirements would not be barred because they are not substantially the same as the breach notification requirements adopted in the 2016 order. For example, the customer notification requirement adopted in 2023 is materially less prescriptive regarding the content and manner of customer notice than what the Commission adopted in 2016. Further, the 2016 rules for customer notifications and government agency notifications did not incorporate the good-faith exception from the definition of covered breaches adopted in 2023. With respect to the federal agency notification requirements, as compared to the 2016 rules, the 2023 rules provide for the Commission and other law enforcement agencies to gain a much more complete picture of data breaches, including trends and emerging activities, consistent with the demonstrated need for such oversight.

Finally, the legislative history of the Congressional Review Act makes clear that an agency is not foreclosed from further action in the same substantive area as a disapproved rule. Instead, when taking action in that area, the agency should look to "the debate on any resolution of disapproval" to understand "the congressional intent regarding the agency's options or lack thereof after enactment of a joint resolution of disapproval."[1] As the 2023 order observed, members of Congress speaking in support of the 2017 resolution of disapproval highlighted aspects of the 2016 order that imposed privacy obligations on internet service providers. Breach reporting obligations for voice providers—the subject of the 2023 order—were not the focus of these statements.

[1] Statement for the Record by Senators Nickles, Reid, and Stevens, 142 Cong. Rec. S3686 (Apr. 18, 1996) (post-enactment).

I appreciate your interest in this matter. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

April 23, 2024

The Honorable Richard Hudson
U.S. House of Representatives
2112 Rayburn House Office Building
Washington, DC 20515

Dear Representative Hudson:

Thank you for your letter regarding the *Data Breach Reporting Requirements* proceeding at the Federal Communications Commission. On December 13, 2023, the agency adopted an order updating its data breach policies.

It had been sixteen years since the Commission last updated its policies to protect consumers from data breaches. In the intervening time a lot has changed about when, where, and how consumers use their phones, and what data providers collect about them when we do. That is why the updates we made are vital. They help protect consumers from digital age data breaches and reinforce the obligation carriers have to protect the privacy and security of consumer data under the Communications Act.

First, we modernized our data breach rules to make clear they include all personally identifiable information. In the past, these rules have only prohibited the disclosure of information about who we call and when. But we know now that data breaches often involve the leak of other sensitive information like our social security numbers and financial data—so we made sure our rules prohibit their disclosure, too.

Second, we made clear that our rules cover intentional and inadvertent disclosure of customer information. Our past policies only accounted for intentional leaks. But every consumer deserves protection regardless of whether the release of their personal information was on purpose or accidental.

Third, we updated our standards for notification to ensure that a carrier must inform the Commission, in addition to law enforcement, and customers of a breach and what personal information may be at risk in a timely manner. The agency's previous rules required carriers to wait seven business days before telling consumers what breaches had taken place. This approach was clearly dated. If there is a leak of your personal and financial information, you want to know as soon as possible.

Finally, we also made clear that these policies apply to telecommunications relay service providers, so that those with disabilities get the same protections as everyone else.

In taking this action, the Commission acted in a manner consistent with the Congressional Review Act. The Congressional Review Act states that an agency rule "may not be reissued in substantially the same form, and a new rule that is substantially the same as such a rule may not be issued, unless the reissued or new rule is specifically authorized by a law enacted after the date of the joint resolution disapproving the original rule." 5 U.S.C. § 801(b)(2).

In the order updating the Commission's data breach policies that was adopted on December 13, 2023, the agency addressed why the decision does not take any action or issue any rules that are prohibited by the Congressional Review Act.

To understand why, it is important to recognize that in this decision the Commission revised its rules governing when telecommunications carriers, providers of interconnected Voice over Internet Protocol services, and providers of telecommunications relay service must report breaches of customer information to governmental entities and affected consumers. On the other hand, the decision in 2016 that was the subject of Congressional Review Act action was focused on adopting privacy rules for broadband internet access service. These are different services. That means when the decision from 2016 is viewed as a whole, there is little point-to-point comparison between it and the order adopted in 2023.

The 2023 order also explains that, even if the "substantially the same" analysis were conducted on a more granular basis, these more recent breach notification requirements would not be barred because they are not substantially the same as the breach notification requirements adopted in the 2016 order. For example, the customer notification requirement adopted in 2023 is materially less prescriptive regarding the content and manner of customer notice than what the Commission adopted in 2016. Further, the 2016 rules for customer notifications and government agency notifications did not incorporate the good-faith exception from the definition of covered breaches adopted in 2023. With respect to the federal agency notification requirements, as compared to the 2016 rules, the 2023 rules provide for the Commission and other law enforcement agencies to gain a much more complete picture of data breaches, including trends and emerging activities, consistent with the demonstrated need for such oversight.

Finally, the legislative history of the Congressional Review Act makes clear that an agency is not foreclosed from further action in the same substantive area as a disapproved rule. Instead, when taking action in that area, the agency should look to "the debate on any resolution of disapproval" to understand "the congressional intent regarding the agency's options or lack thereof after enactment of a joint resolution of disapproval."[1] As the 2023 order observed, members of Congress speaking in support of the 2017 resolution of disapproval highlighted aspects of the 2016 order that imposed privacy obligations on internet service providers. Breach reporting obligations for voice providers—the subject of the 2023 order—were not the focus of these statements.

[1] Statement for the Record by Senators Nickles, Reid, and Stevens, 142 Cong. Rec. S3686 (Apr. 18, 1996) (post-enactment).

I appreciate your interest in this matter. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

April 23, 2024

The Honorable Jeff Duncan
U.S. House of Representatives
2229 Rayburn House Office Building
Washington, DC 20515

Dear Representative Duncan:

Thank you for your letter regarding the *Data Breach Reporting Requirements* proceeding at the Federal Communications Commission. On December 13, 2023, the agency adopted an order updating its data breach policies.

It had been sixteen years since the Commission last updated its policies to protect consumers from data breaches. In the intervening time a lot has changed about when, where, and how consumers use their phones, and what data providers collect about them when we do. That is why the updates we made are vital. They help protect consumers from digital age data breaches and reinforce the obligation carriers have to protect the privacy and security of consumer data under the Communications Act.

First, we modernized our data breach rules to make clear they include all personally identifiable information. In the past, these rules have only prohibited the disclosure of information about who we call and when. But we know now that data breaches often involve the leak of other sensitive information like our social security numbers and financial data—so we made sure our rules prohibit their disclosure, too.

Second, we made clear that our rules cover intentional and inadvertent disclosure of customer information. Our past policies only accounted for intentional leaks. But every consumer deserves protection regardless of whether the release of their personal information was on purpose or accidental.

Third, we updated our standards for notification to ensure that a carrier must inform the Commission, in addition to law enforcement, and customers of a breach and what personal information may be at risk in a timely manner. The agency's previous rules required carriers to wait seven business days before telling consumers what breaches had taken place. This approach was clearly dated. If there is a leak of your personal and financial information, you want to know as soon as possible.

Finally, we also made clear that these policies apply to telecommunications relay service providers, so that those with disabilities get the same protections as everyone else.

In taking this action, the Commission acted in a manner consistent with the Congressional Review Act. The Congressional Review Act states that an agency rule "may not be reissued in substantially the same form, and a new rule that is substantially the same as such a rule may not be issued, unless the reissued or new rule is specifically authorized by a law enacted after the date of the joint resolution disapproving the original rule." 5 U.S.C. § 801(b)(2).

In the order updating the Commission's data breach policies that was adopted on December 13, 2023, the agency addressed why the decision does not take any action or issue any rules that are prohibited by the Congressional Review Act.

To understand why, it is important to recognize that in this decision the Commission revised its rules governing when telecommunications carriers, providers of interconnected Voice over Internet Protocol services, and providers of telecommunications relay service must report breaches of customer information to governmental entities and affected consumers. On the other hand, the decision in 2016 that was the subject of Congressional Review Act action was focused on adopting privacy rules for broadband internet access service. These are different services. That means when the decision from 2016 is viewed as a whole, there is little point-to-point comparison between it and the order adopted in 2023.

The 2023 order also explains that, even if the "substantially the same" analysis were conducted on a more granular basis, these more recent breach notification requirements would not be barred because they are not substantially the same as the breach notification requirements adopted in the 2016 order. For example, the customer notification requirement adopted in 2023 is materially less prescriptive regarding the content and manner of customer notice than what the Commission adopted in 2016. Further, the 2016 rules for customer notifications and government agency notifications did not incorporate the good-faith exception from the definition of covered breaches adopted in 2023. With respect to the federal agency notification requirements, as compared to the 2016 rules, the 2023 rules provide for the Commission and other law enforcement agencies to gain a much more complete picture of data breaches, including trends and emerging activities, consistent with the demonstrated need for such oversight.

Finally, the legislative history of the Congressional Review Act makes clear that an agency is not foreclosed from further action in the same substantive area as a disapproved rule. Instead, when taking action in that area, the agency should look to "the debate on any resolution of disapproval" to understand "the congressional intent regarding the agency's options or lack thereof after enactment of a joint resolution of disapproval."[1] As the 2023 order observed, members of Congress speaking in support of the 2017 resolution of disapproval highlighted aspects of the 2016 order that imposed privacy obligations on internet service providers. Breach reporting obligations for voice providers—the subject of the 2023 order—were not the focus of these statements.

[1] Statement for the Record by Senators Nickles, Reid, and Stevens, 142 Cong. Rec. S3686 (Apr. 18, 1996) (post-enactment).

I appreciate your interest in this matter. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

April 23, 2024

The Honorable Rick Allen
U.S. House of Representatives
462 Cannon House Office Building
Washington, DC 20515

Dear Representative Allen:

Thank you for your letter regarding the *Data Breach Reporting Requirements* proceeding at the Federal Communications Commission. On December 13, 2023, the agency adopted an order updating its data breach policies.

It had been sixteen years since the Commission last updated its policies to protect consumers from data breaches. In the intervening time a lot has changed about when, where, and how consumers use their phones, and what data providers collect about them when we do. That is why the updates we made are vital. They help protect consumers from digital age data breaches and reinforce the obligation carriers have to protect the privacy and security of consumer data under the Communications Act.

First, we modernized our data breach rules to make clear they include all personally identifiable information. In the past, these rules have only prohibited the disclosure of information about who we call and when. But we know now that data breaches often involve the leak of other sensitive information like our social security numbers and financial data—so we made sure our rules prohibit their disclosure, too.

Second, we made clear that our rules cover intentional and inadvertent disclosure of customer information. Our past policies only accounted for intentional leaks. But every consumer deserves protection regardless of whether the release of their personal information was on purpose or accidental.

Third, we updated our standards for notification to ensure that a carrier must inform the Commission, in addition to law enforcement, and customers of a breach and what personal information may be at risk in a timely manner. The agency's previous rules required carriers to wait seven business days before telling consumers what breaches had taken place. This approach was clearly dated. If there is a leak of your personal and financial information, you want to know as soon as possible.

Finally, we also made clear that these policies apply to telecommunications relay service providers, so that those with disabilities get the same protections as everyone else.

In taking this action, the Commission acted in a manner consistent with the Congressional Review Act. The Congressional Review Act states that an agency rule "may not be reissued in substantially the same form, and a new rule that is substantially the same as such a rule may not be issued, unless the reissued or new rule is specifically authorized by a law enacted after the date of the joint resolution disapproving the original rule." 5 U.S.C. § 801(b)(2).

In the order updating the Commission's data breach policies that was adopted on December 13, 2023, the agency addressed why the decision does not take any action or issue any rules that are prohibited by the Congressional Review Act.

To understand why, it is important to recognize that in this decision the Commission revised its rules governing when telecommunications carriers, providers of interconnected Voice over Internet Protocol services, and providers of telecommunications relay service must report breaches of customer information to governmental entities and affected consumers. On the other hand, the decision in 2016 that was the subject of Congressional Review Act action was focused on adopting privacy rules for broadband internet access service. These are different services. That means when the decision from 2016 is viewed as a whole, there is little point-to-point comparison between it and the order adopted in 2023.

The 2023 order also explains that, even if the "substantially the same" analysis were conducted on a more granular basis, these more recent breach notification requirements would not be barred because they are not substantially the same as the breach notification requirements adopted in the 2016 order. For example, the customer notification requirement adopted in 2023 is materially less prescriptive regarding the content and manner of customer notice than what the Commission adopted in 2016. Further, the 2016 rules for customer notifications and government agency notifications did not incorporate the good-faith exception from the definition of covered breaches adopted in 2023. With respect to the federal agency notification requirements, as compared to the 2016 rules, the 2023 rules provide for the Commission and other law enforcement agencies to gain a much more complete picture of data breaches, including trends and emerging activities, consistent with the demonstrated need for such oversight.

Finally, the legislative history of the Congressional Review Act makes clear that an agency is not foreclosed from further action in the same substantive area as a disapproved rule. Instead, when taking action in that area, the agency should look to "the debate on any resolution of disapproval" to understand "the congressional intent regarding the agency's options or lack thereof after enactment of a joint resolution of disapproval."[1] As the 2023 order observed, members of Congress speaking in support of the 2017 resolution of disapproval highlighted aspects of the 2016 order that imposed privacy obligations on internet service providers. Breach reporting obligations for voice providers—the subject of the 2023 order—were not the focus of these statements.

[1] Statement for the Record by Senators Nickles, Reid, and Stevens, 142 Cong. Rec. S3686 (Apr. 18, 1996) (post-enactment).

I appreciate your interest in this matter. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF THE
CHAIRWOMAN

April 23, 2024

The Honorable Greg Pence
U.S. House of Representatives
404 Cannon House Office Building
Washington, DC 20515

Dear Representative Pence:

Thank you for your letter regarding the *Data Breach Reporting Requirements* proceeding at the Federal Communications Commission. On December 13, 2023, the agency adopted an order updating its data breach policies.

It had been sixteen years since the Commission last updated its policies to protect consumers from data breaches. In the intervening time a lot has changed about when, where, and how consumers use their phones, and what data providers collect about them when we do. That is why the updates we made are vital. They help protect consumers from digital age data breaches and reinforce the obligation carriers have to protect the privacy and security of consumer data under the Communications Act.

First, we modernized our data breach rules to make clear they include all personally identifiable information. In the past, these rules have only prohibited the disclosure of information about who we call and when. But we know now that data breaches often involve the leak of other sensitive information like our social security numbers and financial data—so we made sure our rules prohibit their disclosure, too.

Second, we made clear that our rules cover intentional and inadvertent disclosure of customer information. Our past policies only accounted for intentional leaks. But every consumer deserves protection regardless of whether the release of their personal information was on purpose or accidental.

Third, we updated our standards for notification to ensure that a carrier must inform the Commission, in addition to law enforcement, and customers of a breach and what personal information may be at risk in a timely manner. The agency's previous rules required carriers to wait seven business days before telling consumers what breaches had taken place. This approach was clearly dated. If there is a leak of your personal and financial information, you want to know as soon as possible.

Finally, we also made clear that these policies apply to telecommunications relay service providers, so that those with disabilities get the same protections as everyone else.

In taking this action, the Commission acted in a manner consistent with the Congressional Review Act. The Congressional Review Act states that an agency rule "may not be reissued in substantially the same form, and a new rule that is substantially the same as such a rule may not be issued, unless the reissued or new rule is specifically authorized by a law enacted after the date of the joint resolution disapproving the original rule." 5 U.S.C. § 801(b)(2).

In the order updating the Commission's data breach policies that was adopted on December 13, 2023, the agency addressed why the decision does not take any action or issue any rules that are prohibited by the Congressional Review Act.

To understand why, it is important to recognize that in this decision the Commission revised its rules governing when telecommunications carriers, providers of interconnected Voice over Internet Protocol services, and providers of telecommunications relay service must report breaches of customer information to governmental entities and affected consumers. On the other hand, the decision in 2016 that was the subject of Congressional Review Act action was focused on adopting privacy rules for broadband internet access service. These are different services. That means when the decision from 2016 is viewed as a whole, there is little point-to-point comparison between it and the order adopted in 2023.

The 2023 order also explains that, even if the "substantially the same" analysis were conducted on a more granular basis, these more recent breach notification requirements would not be barred because they are not substantially the same as the breach notification requirements adopted in the 2016 order. For example, the customer notification requirement adopted in 2023 is materially less prescriptive regarding the content and manner of customer notice than what the Commission adopted in 2016. Further, the 2016 rules for customer notifications and government agency notifications did not incorporate the good-faith exception from the definition of covered breaches adopted in 2023. With respect to the federal agency notification requirements, as compared to the 2016 rules, the 2023 rules provide for the Commission and other law enforcement agencies to gain a much more complete picture of data breaches, including trends and emerging activities, consistent with the demonstrated need for such oversight.

Finally, the legislative history of the Congressional Review Act makes clear that an agency is not foreclosed from further action in the same substantive area as a disapproved rule. Instead, when taking action in that area, the agency should look to "the debate on any resolution of disapproval" to understand "the congressional intent regarding the agency's options or lack thereof after enactment of a joint resolution of disapproval."[1] As the 2023 order observed, members of Congress speaking in support of the 2017 resolution of disapproval highlighted aspects of the 2016 order that imposed privacy obligations on internet service providers. Breach reporting obligations for voice providers—the subject of the 2023 order—were not the focus of these statements.

[1] Statement for the Record by Senators Nickles, Reid, and Stevens, 142 Cong. Rec. S3686 (Apr. 18, 1996) (post-enactment).

I appreciate your interest in this matter. Please let me know if I can be of further assistance.

Sincerely,

Jessica Rosenworcel