



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

February 14, 2020

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 cellular fraud involving the unauthorized use, tampering, or manipulation of a consumer's cellular phone or service. Consumer protection is a key strategic goal of the Commission, and I have made it a priority as Chairman to provide consumers with the information they need to protect themselves against cellular phone-related scams, such as SIM swaps or port-out requests by criminals, and to ensure the Commission's rules protect consumers' personal and sensitive information.

We use a multipronged approach when it comes to educating the public on these topics. We are continuously posting new content to our Consumer Help Center to address these issues, as well as training our Consumer Complaint Center agents to provide tips and relevant information to consumers who call or file electronic inquiries. Regarding SIM swaps and port-out requests, the FCC has had a consumer guide on cellular fraud since 2015 that provides useful information on how consumers can protect themselves, available at <https://www.fcc.gov/consumers/guides/cell-phone-fraud>. Last fall, we released a Consumer Help Center post on port-out scams, available at <https://www.fcc.gov/port-out-fraud-targets-your-private-accounts>. Consistent with these efforts, I recently asked the FCC's Consumer and Governmental Affairs Bureau to review whether there are other steps consumers can take to protect themselves and what consumer education efforts may be beneficial.

Content is also shared through webinars, email messaging, press releases, ongoing engagement with media outlets, and social media channels, through in-person events throughout the country, and through coordination with national, regional, and local partners to reach various constituencies. Specifically, we have launched an online Scam Glossary, which includes descriptions of more than fifty common phone-based scams—including the type of scam referenced in your letter—with links to additional information to educate and protect consumers. We continue to update the other relevant consumer guides with new information and detailed tips.

With respect to your concerns about port-out scams and the Commission's rules, our rules require the exchange of 14 fields to accomplish a simple port. Three of these fields—the ported telephone number, the customer's account number, and customer's zip code—are consumer-focused and are designed to help protect against fraudulent ports. The Commission found that the exchange of these fields strikes the right balance between streamlining the porting process and ensuring accurate ports. To further protect against fraudulent ports, our rules permit

customers to request that user-assigned passcodes be applied to their accounts, which any given consumer must then provide before a port can be accomplished. The Commission concluded that these measures reasonably balance consumer concerns about slamming and port-out fraud with the public interest in ensuring that porting obligations are not used in an anticompetitive manner to inhibit consumer choice.

I believe that current law and regulations already address the concerns raised in your letter. In particular, section 222 imposes a general duty on carriers to protect the confidentiality of their customers' proprietary information and specifically prohibits carriers from using or sharing customer proprietary network information (CPNI) without customer approval for purposes other than providing the telecommunications service. Section 222 and the Commission's implementing rules define CPNI to include information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship. Section 222 also permits carriers, with the approval of the customer, to use, disclose, or permit access to customer proprietary network information to protect telecommunications customers "from fraudulent, abusive, or unlawful use of, or subscription to" telecommunications services.

In 2007, the Commission amended our CPNI rules to adopt additional safeguards to protect customers' CPNI against unauthorized access and disclosure. As a result, these rules restrict the release of call detail information based on customer-initiated telephone contact, impose password requirements for customer account access, and require carriers to appropriately authenticate both new and existing customers seeking access to CPNI online. Our rules implementing section 222 also require carriers to take reasonable measures to both discover and protect against attempts to gain unauthorized access to CPNI. Further, the Commission has made clear that carriers have a fundamental duty to remain vigilant in their protection of CPNI.

We also require carriers to notify customers immediately of certain account changes, including whenever a password, customer response to a carrier-designed back-up means of authentication, online account, or address of record is created or changed. In order to protect customers from malicious account changes, these notifications cannot reveal the changed account information, nor can they be sent to any updated account information associated with the change. The Commission has found this notice requirement appropriate to warn consumers in the event of possible fraudulent activity.

Nothing in our rules prevents carriers from reporting illegal SIM swaps to the authorities. Indeed, our rules require carriers to notify law enforcement of breaches of its customers' CPNI—or, more specifically, "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI."

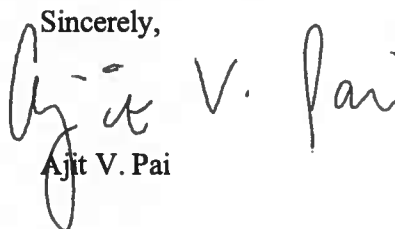
Over the past year, the Commission's Enforcement Bureau staff has not received any reports of violations of CPNI that involve the hacking of wireless carriers as described in your letter but would review and investigate any reports alleging such violations.

Finally, the agency's Consumer and Governmental Affairs Bureau has provided me with the following numbers regarding consumer complaints discussing SIM swapping or port out fraud received by our Consumer Complaint Center. Based on the specific nature of the complaint, Bureau staff either served the complaint on the individual provider through the Bureau's informal complaint process or processed it in other ways such as pointing a consumer to the relevant Consumer Guide or referring the matter to the Federal Trade Commission.

Informal Complaints Discussing Port Out Fraud or SIM Swapping			
	2017	2018	2019
January	10	21	2
February	14	17	31
March	19	15	22
April	17	23	13
May	19	25	10
June	16	14	10
July	20	15	8
August	22	17	21
September	22	11	21
October	21	19	10
November	21	19	14
December	17	15	21
Totals	218	211	183

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

Sincerely,

A handwritten signature in black ink, appearing to read "Ajit V. Pai". The signature is fluid and cursive, with the first name "Ajit" being the most prominent part.

Ajit V. Pai



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

February 14, 2020

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

Dear Senator Wyden:

Thank you for your letter regarding cellular fraud involving the unauthorized use, tampering, or manipulation of a consumer's cellular phone or service. Consumer protection is a key strategic goal of the Commission, and I have made it a priority as Chairman to provide consumers with the information they need to protect themselves against cellular phone-related scams, such as SIM swaps or port-out requests by criminals, and to ensure the Commission's rules protect consumers' personal and sensitive information.

We use a multipronged approach when it comes to educating the public on these topics. We are continuously posting new content to our Consumer Help Center to address these issues, as well as training our Consumer Complaint Center agents to provide tips and relevant information to consumers who call or file electronic inquiries. Regarding SIM swaps and port-out requests, the FCC has had a consumer guide on cellular fraud since 2015 that provides useful information on how consumers can protect themselves, available at <https://www.fcc.gov/consumers/guides/cell-phone-fraud>. Last fall, we released a Consumer Help Center post on port-out scams, available at <https://www.fcc.gov/port-out-fraud-targets-your-private-accounts>. Consistent with these efforts, I recently asked the FCC's Consumer and Governmental Affairs Bureau to review whether there are other steps consumers can take to protect themselves and what consumer education efforts may be beneficial.

Content is also shared through webinars, email messaging, press releases, ongoing engagement with media outlets, and social media channels, through in-person events throughout the country, and through coordination with national, regional, and local partners to reach various constituencies. Specifically, we have launched an online Scam Glossary, which includes descriptions of more than fifty common phone-based scams—including the type of scam referenced in your letter—with links to additional information to educate and protect consumers. We continue to update the other relevant consumer guides with new information and detailed tips.

With respect to your concerns about port-out scams and the Commission's rules, our rules require the exchange of 14 fields to accomplish a simple port. Three of these fields—the ported telephone number, the customer's account number, and customer's zip code—are consumer-focused and are designed to help protect against fraudulent ports. The Commission found that the exchange of these fields strikes the right balance between streamlining the porting process and ensuring accurate ports. To further protect against fraudulent ports, our rules permit

customers to request that user-assigned passcodes be applied to their accounts, which any given consumer must then provide before a port can be accomplished. The Commission concluded that these measures reasonably balance consumer concerns about slamming and port-out fraud with the public interest in ensuring that porting obligations are not used in an anticompetitive manner to inhibit consumer choice.

I believe that current law and regulations already address the concerns raised in your letter. In particular, section 222 imposes a general duty on carriers to protect the confidentiality of their customers' proprietary information and specifically prohibits carriers from using or sharing customer proprietary network information (CPNI) without customer approval for purposes other than providing the telecommunications service. Section 222 and the Commission's implementing rules define CPNI to include information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship. Section 222 also permits carriers, with the approval of the customer, to use, disclose, or permit access to customer proprietary network information to protect telecommunications customers "from fraudulent, abusive, or unlawful use of, or subscription to" telecommunications services.

In 2007, the Commission amended our CPNI rules to adopt additional safeguards to protect customers' CPNI against unauthorized access and disclosure. As a result, these rules restrict the release of call detail information based on customer-initiated telephone contact, impose password requirements for customer account access, and require carriers to appropriately authenticate both new and existing customers seeking access to CPNI online. Our rules implementing section 222 also require carriers to take reasonable measures to both discover and protect against attempts to gain unauthorized access to CPNI. Further, the Commission has made clear that carriers have a fundamental duty to remain vigilant in their protection of CPNI.

We also require carriers to notify customers immediately of certain account changes, including whenever a password, customer response to a carrier-designed back-up means of authentication, online account, or address of record is created or changed. In order to protect customers from malicious account changes, these notifications cannot reveal the changed account information, nor can they be sent to any updated account information associated with the change. The Commission has found this notice requirement appropriate to warn consumers in the event of possible fraudulent activity.

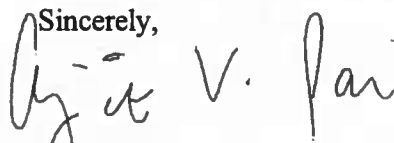
Nothing in our rules prevents carriers from reporting illegal SIM swaps to the authorities. Indeed, our rules require carriers to notify law enforcement of breaches of its customers' CPNI—or, more specifically, "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI."

Over the past year, the Commission's Enforcement Bureau staff has not received any reports of violations of CPNI that involve the hacking of wireless carriers as described in your letter but would review and investigate any reports alleging such violations.

Finally, the agency's Consumer and Governmental Affairs Bureau has provided me with the following numbers regarding consumer complaints discussing SIM swapping or port out fraud received by our Consumer Complaint Center. Based on the specific nature of the complaint, Bureau staff either served the complaint on the individual provider through the Bureau's informal complaint process or processed it in other ways such as pointing a consumer to the relevant Consumer Guide or referring the matter to the Federal Trade Commission.

Informal Complaints Discussing Port Out Fraud or SIM Swapping			
	2017	2018	2019
January	10	21	2
February	14	17	31
March	19	15	22
April	17	23	13
May	19	25	10
June	16	14	10
July	20	15	8
August	22	17	21
September	22	11	21
October	21	19	10
November	21	19	14
December	17	15	21
Totals	218	211	183

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

Sincerely,

Ajit V. Pai



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

February 14, 2020

The Honorable Yvette D. Clarke
U.S. House of Representatives
2058 Rayburn House Office Building
Washington, DC 20515

Dear Congresswoman Clarke:

Thank you for your letter regarding cellular fraud involving the unauthorized use, tampering, or manipulation of a consumer's cellular phone or service. Consumer protection is a key strategic goal of the Commission, and I have made it a priority as Chairman to provide consumers with the information they need to protect themselves against cellular phone-related scams, such as SIM swaps or port-out requests by criminals, and to ensure the Commission's rules protect consumers' personal and sensitive information.

We use a multipronged approach when it comes to educating the public on these topics. We are continuously posting new content to our Consumer Help Center to address these issues, as well as training our Consumer Complaint Center agents to provide tips and relevant information to consumers who call or file electronic inquiries. Regarding SIM swaps and port-out requests, the FCC has had a consumer guide on cellular fraud since 2015 that provides useful information on how consumers can protect themselves, available at <https://www.fcc.gov/consumers/guides/cell-phone-fraud>. Last fall, we released a Consumer Help Center post on port-out scams, available at <https://www.fcc.gov/port-out-fraud-targets-your-private-accounts>. Consistent with these efforts, I recently asked the FCC's Consumer and Governmental Affairs Bureau to review whether there are other steps consumers can take to protect themselves and what consumer education efforts may be beneficial.

Content is also shared through webinars, email messaging, press releases, ongoing engagement with media outlets, and social media channels, through in-person events throughout the country, and through coordination with national, regional, and local partners to reach various constituencies. Specifically, we have launched an online Scam Glossary, which includes descriptions of more than fifty common phone-based scams—including the type of scam referenced in your letter—with links to additional information to educate and protect consumers. We continue to update the other relevant consumer guides with new information and detailed tips.

With respect to your concerns about port-out scams and the Commission's rules, our rules require the exchange of 14 fields to accomplish a simple port. Three of these fields—the ported telephone number, the customer's account number, and customer's zip code—are consumer-focused and are designed to help protect against fraudulent ports. The Commission found that the exchange of these fields strikes the right balance between streamlining the porting process and ensuring accurate ports. To further protect against fraudulent ports, our rules permit

customers to request that user-assigned passcodes be applied to their accounts, which any given consumer must then provide before a port can be accomplished. The Commission concluded that these measures reasonably balance consumer concerns about slamming and port-out fraud with the public interest in ensuring that porting obligations are not used in an anticompetitive manner to inhibit consumer choice.

I believe that current law and regulations already address the concerns raised in your letter. In particular, section 222 imposes a general duty on carriers to protect the confidentiality of their customers' proprietary information and specifically prohibits carriers from using or sharing customer proprietary network information (CPNI) without customer approval for purposes other than providing the telecommunications service. Section 222 and the Commission's implementing rules define CPNI to include information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship. Section 222 also permits carriers, with the approval of the customer, to use, disclose, or permit access to customer proprietary network information to protect telecommunications customers "from fraudulent, abusive, or unlawful use of, or subscription to" telecommunications services.

In 2007, the Commission amended our CPNI rules to adopt additional safeguards to protect customers' CPNI against unauthorized access and disclosure. As a result, these rules restrict the release of call detail information based on customer-initiated telephone contact, impose password requirements for customer account access, and require carriers to appropriately authenticate both new and existing customers seeking access to CPNI online. Our rules implementing section 222 also require carriers to take reasonable measures to both discover and protect against attempts to gain unauthorized access to CPNI. Further, the Commission has made clear that carriers have a fundamental duty to remain vigilant in their protection of CPNI.

We also require carriers to notify customers immediately of certain account changes, including whenever a password, customer response to a carrier-designed back-up means of authentication, online account, or address of record is created or changed. In order to protect customers from malicious account changes, these notifications cannot reveal the changed account information, nor can they be sent to any updated account information associated with the change. The Commission has found this notice requirement appropriate to warn consumers in the event of possible fraudulent activity.

Nothing in our rules prevents carriers from reporting illegal SIM swaps to the authorities. Indeed, our rules require carriers to notify law enforcement of breaches of its customers' CPNI—or, more specifically, "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI."

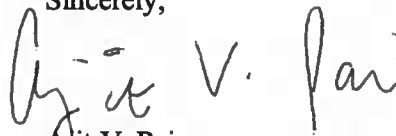
Over the past year, the Commission's Enforcement Bureau staff has not received any reports of violations of CPNI that involve the hacking of wireless carriers as described in your letter but would review and investigate any reports alleging such violations.

Finally, the agency's Consumer and Governmental Affairs Bureau has provided me with the following numbers regarding consumer complaints discussing SIM swapping or port out fraud received by our Consumer Complaint Center. Based on the specific nature of the complaint, Bureau staff either served the complaint on the individual provider through the Bureau's informal complaint process or processed it in other ways such as pointing a consumer to the relevant Consumer Guide or referring the matter to the Federal Trade Commission.

Informal Complaints Discussing Port Out Fraud or SIM Swapping			
	2017	2018	2019
January	10	21	2
February	14	17	31
March	19	15	22
April	17	23	13
May	19	25	10
June	16	14	10
July	20	15	8
August	22	17	21
September	22	11	21
October	21	19	10
November	21	19	14
December	17	15	21
Totals	218	211	183

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

Sincerely,


Ajit V. Pai



OFFICE OF
THE CHAIRMAN

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

February 14, 2020

The Honorable Anna G. Eshoo
U.S. House of Representatives
202 Cannon House Office Building
Washington, DC 20515

Dear Congresswoman Eshoo:

Thank you for your letter regarding cellular fraud involving the unauthorized use, tampering, or manipulation of a consumer's cellular phone or service. Consumer protection is a key strategic goal of the Commission, and I have made it a priority as Chairman to provide consumers with the information they need to protect themselves against cellular phone-related scams, such as SIM swaps or port-out requests by criminals, and to ensure the Commission's rules protect consumers' personal and sensitive information.

We use a multipronged approach when it comes to educating the public on these topics. We are continuously posting new content to our Consumer Help Center to address these issues, as well as training our Consumer Complaint Center agents to provide tips and relevant information to consumers who call or file electronic inquiries. Regarding SIM swaps and port-out requests, the FCC has had a consumer guide on cellular fraud since 2015 that provides useful information on how consumers can protect themselves, available at <https://www.fcc.gov/consumers/guides/cell-phone-fraud>. Last fall, we released a Consumer Help Center post on port-out scams, available at <https://www.fcc.gov/port-out-fraud-targets-your-private-accounts>. Consistent with these efforts, I recently asked the FCC's Consumer and Governmental Affairs Bureau to review whether there are other steps consumers can take to protect themselves and what consumer education efforts may be beneficial.

Content is also shared through webinars, email messaging, press releases, ongoing engagement with media outlets, and social media channels, through in-person events throughout the country, and through coordination with national, regional, and local partners to reach various constituencies. Specifically, we have launched an online Scam Glossary, which includes descriptions of more than fifty common phone-based scams—including the type of scam referenced in your letter—with links to additional information to educate and protect consumers. We continue to update the other relevant consumer guides with new information and detailed tips.

With respect to your concerns about port-out scams and the Commission's rules, our rules require the exchange of 14 fields to accomplish a simple port. Three of these fields—the ported telephone number, the customer's account number, and customer's zip code—are consumer-focused and are designed to help protect against fraudulent ports. The Commission found that the exchange of these fields strikes the right balance between streamlining the porting process and ensuring accurate ports. To further protect against fraudulent ports, our rules permit

customers to request that user-assigned passcodes be applied to their accounts, which any given consumer must then provide before a port can be accomplished. The Commission concluded that these measures reasonably balance consumer concerns about slamming and port-out fraud with the public interest in ensuring that porting obligations are not used in an anticompetitive manner to inhibit consumer choice.

I believe that current law and regulations already address the concerns raised in your letter. In particular, section 222 imposes a general duty on carriers to protect the confidentiality of their customers' proprietary information and specifically prohibits carriers from using or sharing customer proprietary network information (CPNI) without customer approval for purposes other than providing the telecommunications service. Section 222 and the Commission's implementing rules define CPNI to include information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship. Section 222 also permits carriers, with the approval of the customer, to use, disclose, or permit access to customer proprietary network information to protect telecommunications customers "from fraudulent, abusive, or unlawful use of, or subscription to" telecommunications services.

In 2007, the Commission amended our CPNI rules to adopt additional safeguards to protect customers' CPNI against unauthorized access and disclosure. As a result, these rules restrict the release of call detail information based on customer-initiated telephone contact, impose password requirements for customer account access, and require carriers to appropriately authenticate both new and existing customers seeking access to CPNI online. Our rules implementing section 222 also require carriers to take reasonable measures to both discover and protect against attempts to gain unauthorized access to CPNI. Further, the Commission has made clear that carriers have a fundamental duty to remain vigilant in their protection of CPNI.

We also require carriers to notify customers immediately of certain account changes, including whenever a password, customer response to a carrier-designed back-up means of authentication, online account, or address of record is created or changed. In order to protect customers from malicious account changes, these notifications cannot reveal the changed account information, nor can they be sent to any updated account information associated with the change. The Commission has found this notice requirement appropriate to warn consumers in the event of possible fraudulent activity.

Nothing in our rules prevents carriers from reporting illegal SIM swaps to the authorities. Indeed, our rules require carriers to notify law enforcement of breaches of its customers' CPNI—or, more specifically, "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI."

Over the past year, the Commission's Enforcement Bureau staff has not received any reports of violations of CPNI that involve the hacking of wireless carriers as described in your letter but would review and investigate any reports alleging such violations.

Finally, the agency's Consumer and Governmental Affairs Bureau has provided me with the following numbers regarding consumer complaints discussing SIM swapping or port out fraud received by our Consumer Complaint Center. Based on the specific nature of the complaint, Bureau staff either served the complaint on the individual provider through the Bureau's informal complaint process or processed it in other ways such as pointing a consumer to the relevant Consumer Guide or referring the matter to the Federal Trade Commission.

Informal Complaints Discussing Port Out Fraud or SIM Swapping			
	2017	2018	2019
January	10	21	2
February	14	17	31
March	19	15	22
April	17	23	13
May	19	25	10
June	16	14	10
July	20	15	8
August	22	17	21
September	22	11	21
October	21	19	10
November	21	19	14
December	17	15	21
Totals	218	211	183

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

Sincerely,

Ajit V. Pai



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

February 14, 2020

The Honorable Sherrod Brown
United States Senate
713 Hart Senate Office Building
Washington, DC 20510

Dear Senator Brown:

Thank you for your letter regarding cellular fraud involving the unauthorized use, tampering, or manipulation of a consumer's cellular phone or service. Consumer protection is a key strategic goal of the Commission, and I have made it a priority as Chairman to provide consumers with the information they need to protect themselves against cellular phone-related scams, such as SIM swaps or port-out requests by criminals, and to ensure the Commission's rules protect consumers' personal and sensitive information.

We use a multipronged approach when it comes to educating the public on these topics. We are continuously posting new content to our Consumer Help Center to address these issues, as well as training our Consumer Complaint Center agents to provide tips and relevant information to consumers who call or file electronic inquiries. Regarding SIM swaps and port-out requests, the FCC has had a consumer guide on cellular fraud since 2015 that provides useful information on how consumers can protect themselves, available at <https://www.fcc.gov/consumers/guides/cell-phone-fraud>. Last fall, we released a Consumer Help Center post on port-out scams, available at <https://www.fcc.gov/port-out-fraud-targets-your-private-accounts>. Consistent with these efforts, I recently asked the FCC's Consumer and Governmental Affairs Bureau to review whether there are other steps consumers can take to protect themselves and what consumer education efforts may be beneficial.

Content is also shared through webinars, email messaging, press releases, ongoing engagement with media outlets, and social media channels, through in-person events throughout the country, and through coordination with national, regional, and local partners to reach various constituencies. Specifically, we have launched an online Scam Glossary, which includes descriptions of more than fifty common phone-based scams—including the type of scam referenced in your letter—with links to additional information to educate and protect consumers. We continue to update the other relevant consumer guides with new information and detailed tips.

With respect to your concerns about port-out scams and the Commission's rules, our rules require the exchange of 14 fields to accomplish a simple port. Three of these fields—the ported telephone number, the customer's account number, and customer's zip code—are consumer-focused and are designed to help protect against fraudulent ports. The Commission found that the exchange of these fields strikes the right balance between streamlining the porting process and ensuring accurate ports. To further protect against fraudulent ports, our rules permit

customers to request that user-assigned passcodes be applied to their accounts, which any given consumer must then provide before a port can be accomplished. The Commission concluded that these measures reasonably balance consumer concerns about slamming and port-out fraud with the public interest in ensuring that porting obligations are not used in an anticompetitive manner to inhibit consumer choice.

I believe that current law and regulations already address the concerns raised in your letter. In particular, section 222 imposes a general duty on carriers to protect the confidentiality of their customers' proprietary information and specifically prohibits carriers from using or sharing customer proprietary network information (CPNI) without customer approval for purposes other than providing the telecommunications service. Section 222 and the Commission's implementing rules define CPNI to include information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship. Section 222 also permits carriers, with the approval of the customer, to use, disclose, or permit access to customer proprietary network information to protect telecommunications customers "from fraudulent, abusive, or unlawful use of, or subscription to" telecommunications services.

In 2007, the Commission amended our CPNI rules to adopt additional safeguards to protect customers' CPNI against unauthorized access and disclosure. As a result, these rules restrict the release of call detail information based on customer-initiated telephone contact, impose password requirements for customer account access, and require carriers to appropriately authenticate both new and existing customers seeking access to CPNI online. Our rules implementing section 222 also require carriers to take reasonable measures to both discover and protect against attempts to gain unauthorized access to CPNI. Further, the Commission has made clear that carriers have a fundamental duty to remain vigilant in their protection of CPNI.

We also require carriers to notify customers immediately of certain account changes, including whenever a password, customer response to a carrier-designed back-up means of authentication, online account, or address of record is created or changed. In order to protect customers from malicious account changes, these notifications cannot reveal the changed account information, nor can they be sent to any updated account information associated with the change. The Commission has found this notice requirement appropriate to warn consumers in the event of possible fraudulent activity.

Nothing in our rules prevents carriers from reporting illegal SIM swaps to the authorities. Indeed, our rules require carriers to notify law enforcement of breaches of its customers' CPNI—or, more specifically, "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI."

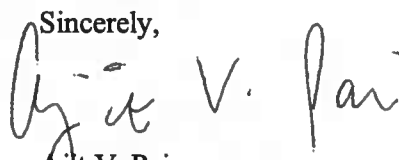
Over the past year, the Commission's Enforcement Bureau staff has not received any reports of violations of CPNI that involve the hacking of wireless carriers as described in your letter but would review and investigate any reports alleging such violations.

Finally, the agency's Consumer and Governmental Affairs Bureau has provided me with the following numbers regarding consumer complaints discussing SIM swapping or port out fraud received by our Consumer Complaint Center. Based on the specific nature of the complaint, Bureau staff either served the complaint on the individual provider through the Bureau's informal complaint process or processed it in other ways such as pointing a consumer to the relevant Consumer Guide or referring the matter to the Federal Trade Commission.

Informal Complaints Discussing Port Out Fraud or SIM Swapping			
	2017	2018	2019
January	10	21	2
February	14	17	31
March	19	15	22
April	17	23	13
May	19	25	10
June	16	14	10
July	20	15	8
August	22	17	21
September	22	11	21
October	21	19	10
November	21	19	14
December	17	15	21
Totals	218	211	183

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

Sincerely,



Ajit V. Pai



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

February 14, 2020

The Honorable Ted Lieu
U.S. House of Representatives
403 Cannon House Office Building
Washington, DC 20515

Dear Congressman Lieu:

Thank you for your letter regarding cellular fraud involving the unauthorized use, tampering, or manipulation of a consumer's cellular phone or service. Consumer protection is a key strategic goal of the Commission, and I have made it a priority as Chairman to provide consumers with the information they need to protect themselves against cellular phone-related scams, such as SIM swaps or port-out requests by criminals, and to ensure the Commission's rules protect consumers' personal and sensitive information.

We use a multipronged approach when it comes to educating the public on these topics. We are continuously posting new content to our Consumer Help Center to address these issues, as well as training our Consumer Complaint Center agents to provide tips and relevant information to consumers who call or file electronic inquiries. Regarding SIM swaps and port-out requests, the FCC has had a consumer guide on cellular fraud since 2015 that provides useful information on how consumers can protect themselves, available at <https://www.fcc.gov/consumers/guides/cell-phone-fraud>. Last fall, we released a Consumer Help Center post on port-out scams, available at <https://www.fcc.gov/port-out-fraud-targets-your-private-accounts>. Consistent with these efforts, I recently asked the FCC's Consumer and Governmental Affairs Bureau to review whether there are other steps consumers can take to protect themselves and what consumer education efforts may be beneficial.

Content is also shared through webinars, email messaging, press releases, ongoing engagement with media outlets, and social media channels, through in-person events throughout the country, and through coordination with national, regional, and local partners to reach various constituencies. Specifically, we have launched an online Scam Glossary, which includes descriptions of more than fifty common phone-based scams—including the type of scam referenced in your letter—with links to additional information to educate and protect consumers. We continue to update the other relevant consumer guides with new information and detailed tips.

With respect to your concerns about port-out scams and the Commission's rules, our rules require the exchange of 14 fields to accomplish a simple port. Three of these fields—the ported telephone number, the customer's account number, and customer's zip code—are consumer-focused and are designed to help protect against fraudulent ports. The Commission found that the exchange of these fields strikes the right balance between streamlining the porting process and ensuring accurate ports. To further protect against fraudulent ports, our rules permit

customers to request that user-assigned passcodes be applied to their accounts, which any given consumer must then provide before a port can be accomplished. The Commission concluded that these measures reasonably balance consumer concerns about slamming and port-out fraud with the public interest in ensuring that porting obligations are not used in an anticompetitive manner to inhibit consumer choice.

I believe that current law and regulations already address the concerns raised in your letter. In particular, section 222 imposes a general duty on carriers to protect the confidentiality of their customers' proprietary information and specifically prohibits carriers from using or sharing customer proprietary network information (CPNI) without customer approval for purposes other than providing the telecommunications service. Section 222 and the Commission's implementing rules define CPNI to include information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship. Section 222 also permits carriers, with the approval of the customer, to use, disclose, or permit access to customer proprietary network information to protect telecommunications customers "from fraudulent, abusive, or unlawful use of, or subscription to" telecommunications services.

In 2007, the Commission amended our CPNI rules to adopt additional safeguards to protect customers' CPNI against unauthorized access and disclosure. As a result, these rules restrict the release of call detail information based on customer-initiated telephone contact, impose password requirements for customer account access, and require carriers to appropriately authenticate both new and existing customers seeking access to CPNI online. Our rules implementing section 222 also require carriers to take reasonable measures to both discover and protect against attempts to gain unauthorized access to CPNI. Further, the Commission has made clear that carriers have a fundamental duty to remain vigilant in their protection of CPNI.

We also require carriers to notify customers immediately of certain account changes, including whenever a password, customer response to a carrier-designed back-up means of authentication, online account, or address of record is created or changed. In order to protect customers from malicious account changes, these notifications cannot reveal the changed account information, nor can they be sent to any updated account information associated with the change. The Commission has found this notice requirement appropriate to warn consumers in the event of possible fraudulent activity.

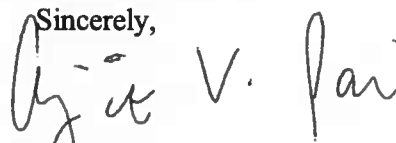
Nothing in our rules prevents carriers from reporting illegal SIM swaps to the authorities. Indeed, our rules require carriers to notify law enforcement of breaches of its customers' CPNI—or, more specifically, "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI."

Over the past year, the Commission's Enforcement Bureau staff has not received any reports of violations of CPNI that involve the hacking of wireless carriers as described in your letter but would review and investigate any reports alleging such violations.

Finally, the agency's Consumer and Governmental Affairs Bureau has provided me with the following numbers regarding consumer complaints discussing SIM swapping or port out fraud received by our Consumer Complaint Center. Based on the specific nature of the complaint, Bureau staff either served the complaint on the individual provider through the Bureau's informal complaint process or processed it in other ways such as pointing a consumer to the relevant Consumer Guide or referring the matter to the Federal Trade Commission.

Informal Complaints Discussing Port Out Fraud or SIM Swapping			
	2017	2018	2019
January	10	21	2
February	14	17	31
March	19	15	22
April	17	23	13
May	19	25	10
June	16	14	10
July	20	15	8
August	22	17	21
September	22	11	21
October	21	19	10
November	21	19	14
December	17	15	21
Totals	218	211	183

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

Sincerely,

Ajit V. Pai