MARK R. WARNER
VIRGINIA

United States Senate
WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

October 24, 2024

Mr. Matthew Prince
CEO
Cloudflare
101 Townsend St
San Francisco, CA 94107

Dear Mr. Prince,

I write to express concerns about the extent to which your company has ostensibly facilitated sustained covert influence activity by the Russian Federation and influence networks operating on its behalf. In particular, recent disruption actions by the Department of Justice indicate that your company has provided domain registration services to the Russian covert influence network known as "Doppelganger."[1] The Department of Justice and private sector actors have attributed this network to Russian influence organizations Social Design Agency, Structura National Technology, and ANO Dialog all assessed to be operating under the direction and control of the Russian government, including to influence voters in the U.S. 2024 Presidential Election.

Operating since Russia's invasion of Ukraine in 2022, the hallmark of the Doppelganger network has been the impersonation of Western media institutions online. Through the maintenance of both inauthentic social media accounts and websites, Russian influence operatives have impersonated dozens of legitimate organizations as early as September 2022, when the EU Disinfo Lab first identified the network's campaigns.[2] Disturbingly, the EU Disinfo Lab's original report noted the lapses by the domain name industry – including, explicitly, GoDaddy and NameCheap – in facilitating Russian covert influence activity.

Research by Meta in 2023 put into sharper focus the extent to which the global domain name industry has enabled Russian malign influence activity and Doppelganger campaigns, in particular. Specifically, Meta noted a number of ways in which firms such as yours have prevented efforts to address this activity, including withholding vital domain name registration information from good-faith researchers and digital forensic investigators, ignoring inaccurate registration information submitted by registrants, and failing to identify repeated instances of intentional and malicious domain name squatting used to impersonate legitimate organizations.[3] Concerningly, Meta's research even identified instances of Doppelganger impersonating *government* websites – including inauthentic websites posing as the German police, Polish and

[1] Affidavit in Support of Seizure Warrant, *United States of America v. Certain Domains*, Case No.: 24-mj-1395 (E.D. PA 2024).
[2] Alexandre Alaphilippe et al, "Doppelganger: Media Clones Serving Russian Propaganda," EU Disinfo Lab (September 27, 2022).
[3] Ben Nimmo et al, "Adversarial Threat Report – Second Quarter," (August 2023).

Ukrainian governments, NATO, and the French Foreign Ministry facilitated by your services. In the context of the U.S. 2024 Presidential Election, the prospect of foreign actors impersonating state and local government websites – and seeding narratives related to election outcomes or electoral processes – is especially dire.

Information included in the affidavit supporting recent seizure of a number of these domains provides further indication of your industry's apparent inattention to abuses by foreign actors engaged in covert influence. Specifically, Russian influence actors utilized a number of tactics, techniques, and procedures that – against the backdrop of extensive open source literature on Doppelganger's practices – should have alerted your company to abuse of its services, including the use of cryptocurrency to purchase domains, heavy reliance on anonymizing infrastructure to access your registration services (including the use of IPs widely associated with cybercriminal obfuscation network activity), the use of credit cards issued to a U.S. company "that has significant ties to, and employees based in, Russia," use of fictitious and poorly-backstopped identities for registrants, and in at least one instance the use of a Russian address.[4] While there are legitimate rationales for protecting the privacy of domain registrants, repeated and overlapping indications of malicious and/or fraudulent activity should counsel in favor of greater scrutiny and transparency by your industry. Further, many of the domains seized by the Department of Justice – including those impersonating the *Washington Post* and Fox News – bore close resemblance (or in some cases, such as fox-news[.]top and fox-news[.]in, *were identical*) to impersonation domains mimicking those same news organizations in Meta's August 2023 report. The content of these recently-seized domains also exhibited clear use by the Doppelganger network – including use of media trademarks and content identified previously by researchers, as well as impersonation of the same Washington Post and Fox News journalists publicly identified by Meta and others over a year prior.

While foreign covert influence represents one of the most egregious abuses of the domain name system, the industry's inattention to abuse has been well-documented for years, enabling malicious activity such as phishing campaigns, drive-by malware, and online scams – all possible because of malicious actors using your services.[5] Moreover, Meta's report indicates that your industry has effectively externalized the costs of addressing this abusive behavior to victims and third parties – who must pursue costly and time-consuming litigation or dispute resolution via the World Intellectual Property Office.[6]

Given the continued lapses of your industry to address these abuses, I believe Congress may need to evaluate legislative remedies that promote greater diligence across the global domain name ecosystem. In the interim, your company must take immediate steps to address the

---

[4] Affidavit in Support of Seizure Warrant, *United States of America v. Certain Domains*, Case No.: 24-mj-1395 (E.D. PA 2024).

[5] *See, e.g.,* Brian Krebs, "Why is .US Being Used to Phish So Many of Us?," KrebsOnSecurity (November 1, 2023); Zhanhao Chen and Janos Szurdi, "Cybersquatting: Attackers Mimicking Domains of Major Brands Including Facebook, Apple, Amazon and Netflix to Scam Consumers," Palo Alto Networks (September 1, 2020); Ihab Shraim, "New Research Says Domain Registration Fraud Surging in Post-Pandemic Era," Security Infowatch (Feb. 21, 2022).

[6] Ben Nimmo et al, "Adversarial Threat Report – Second Quarter," (August 2023).

continued abuse of your services for foreign covert influence – particularly in the days preceding, and weeks immediately following, Election Day. With the prospect of a close election – and declassified intelligence demonstrating the past practice of foreign adversaries in spreading narratives that undermine confidence in election processes[7] – Americans will be particularly reliant on media organizations and state and local government websites to provide authoritative and accurate election information. It is imperative that your company work to diminish the risk that foreign adversaries use impersonated domains to promote false narratives in this context.

Sincerely,

Mark R. Warner
United States Senator

Cc: Fox News Corporation
Cc: The Washington Post
Cc: The Forward

[7] National Intelligence Council, "Foreign Threats to the 2020 US Federal Elections," Intelligence Community Assessment (March 10, 2021) (describing efforts by Iran, Russia, and foreign hacktivists to denigrate election processes and sow narratives to undermine public confidence in 2020 elections).

MARK R. WARNER
VIRGINIA

United States Senate
WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

October 24, 2024

Mr. Aman Bhutani
CEO
GoDaddy
2155 E. GoDaddy Way
Tempe, AZ 85284

Dear Mr. Bhutani,

I write to express concerns about the extent to which your company has ostensibly facilitated sustained covert influence activity by the Russian Federation and influence networks operating on its behalf. In particular, recent disruption actions by the Department of Justice indicate that your company has provided domain registration services to the Russian covert influence network known as "Doppelganger."[1] The Department of Justice and private sector actors have attributed this network to Russian influence organizations Social Design Agency, Structura National Technology, and ANO Dialog all assessed to be operating under the direction and control of the Russian government, including to influence voters in the U.S. 2024 Presidential Election.

Operating since Russia's invasion of Ukraine in 2022, the hallmark of the Doppelganger network has been the impersonation of Western media institutions online. Through the maintenance of both inauthentic social media accounts and websites, Russian influence operatives have impersonated dozens of legitimate organizations as early as September 2022, when the EU Disinfo Lab first identified the network's campaigns.[2] Disturbingly, the EU Disinfo Lab's original report noted the lapses by the domain name industry – including, explicitly, GoDaddy and NameCheap – in facilitating Russian covert influence activity.

Research by Meta in 2023 put into sharper focus the extent to which the global domain name industry has enabled Russian malign influence activity and Doppelganger campaigns, in particular. Specifically, Meta noted a number of ways in which firms such as yours have prevented efforts to address this activity, including withholding vital domain name registration information from good-faith researchers and digital forensic investigators, ignoring inaccurate registration information submitted by registrants, and failing to identify repeated instances of intentional and malicious domain name squatting used to impersonate legitimate organizations.[3] Concerningly, Meta's research even identified instances of Doppelganger impersonating *government* websites – including inauthentic websites posing as the German police, Polish and

[1] Affidavit in Support of Seizure Warrant, *United States of America v. Certain Domains*, Case No.: 24-mj-1395 (E.D. PA 2024).
[2] Alexandre Alaphilippe et al, "Doppelganger: Media Clones Serving Russian Propaganda," EU Disinfo Lab (September 27, 2022).
[3] Ben Nimmo et al, "Adversarial Threat Report – Second Quarter," (August 2023).

Ukrainian governments, NATO, and the French Foreign Ministry facilitated by your services. In the context of the U.S. 2024 Presidential Election, the prospect of foreign actors impersonating state and local government websites – and seeding narratives related to election outcomes or electoral processes – is especially dire.

Information included in the affidavit supporting recent seizure of a number of these domains provides further indication of your industry's apparent inattention to abuses by foreign actors engaged in covert influence. Specifically, Russian influence actors utilized a number of tactics, techniques, and procedures that – against the backdrop of extensive open source literature on Doppelganger's practices – should have alerted your company to abuse of its services, including the use of cryptocurrency to purchase domains, heavy reliance on anonymizing infrastructure to access your registration services (including the use of IPs widely associated with cybercriminal obfuscation network activity), the use of credit cards issued to a U.S. company "that has significant ties to, and employees based in, Russia," use of fictitious and poorly-backstopped identities for registrants, and in at least one instance the use of a Russian address.[4] While there are legitimate rationales for protecting the privacy of domain registrants, repeated and overlapping indications of malicious and/or fraudulent activity should counsel in favor of greater scrutiny and transparency by your industry. Further, many of the domains seized by the Department of Justice – including those impersonating the *Washington Post* and Fox News – bore close resemblance (or in some cases, such as fox-news[.]top and fox-news[.]in, *were identical*) to impersonation domains mimicking those same news organizations in Meta's August 2023 report. The content of these recently-seized domains also exhibited clear use by the Doppelganger network – including use of media trademarks and content identified previously by researchers, as well as impersonation of the same Washington Post and Fox News journalists publicly identified by Meta and others over a year prior.

While foreign covert influence represents one of the most egregious abuses of the domain name system, the industry's inattention to abuse has been well-documented for years, enabling malicious activity such as phishing campaigns, drive-by malware, and online scams – all possible because of malicious actors using your services.[5] Moreover, Meta's report indicates that your industry has effectively externalized the costs of addressing this abusive behavior to victims and third parties – who must pursue costly and time-consuming litigation or dispute resolution via the World Intellectual Property Office.[6]

Given the continued lapses of your industry to address these abuses, I believe Congress may need to evaluate legislative remedies that promote greater diligence across the global domain name ecosystem. In the interim, your company must take immediate steps to address the

---

[4] Affidavit in Support of Seizure Warrant, *United States of America v. Certain Domains*, Case No.: 24-mj-1395 (E.D. PA 2024).

[5] *See, e.g.,* Brian Krebs, "Why is .US Being Used to Phish So Many of Us?," KrebsOnSecurity (November 1, 2023); Zhanhao Chen and Janos Szurdi, "Cybersquatting: Attackers Mimicking Domains of Major Brands Including Facebook, Apple, Amazon and Netflix to Scam Consumers," Palo Alto Networks (September 1, 2020); Ihab Shraim, "New Research Says Domain Registration Fraud Surging in Post-Pandemic Era," Security Infowatch (Feb. 21, 2022).

[6] Ben Nimmo et al, "Adversarial Threat Report – Second Quarter," (August 2023).

continued abuse of your services for foreign covert influence – particularly in the days preceding, and weeks immediately following, Election Day. With the prospect of a close election – and declassified intelligence demonstrating the past practice of foreign adversaries in spreading narratives that undermine confidence in election processes[7] – Americans will be particularly reliant on media organizations and state and local government websites to provide authoritative and accurate election information. It is imperative that your company work to diminish the risk that foreign adversaries use impersonated domains to promote false narratives in this context.

Sincerely,

Mark R. Warner
United States Senator

Cc: Fox News Corporation
Cc: The Washington Post
Cc: The Forward

[7] National Intelligence Council, "Foreign Threats to the 2020 US Federal Elections," Intelligence Community Assessment (March 10, 2021) (describing efforts by Iran, Russia, and foreign hacktivists to denigrate election processes and sow narratives to undermine public confidence in 2020 elections).

MARK R. WARNER
VIRGINIA

United States Senate
WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

October 24, 2024

Mr. Richard Kirkendall
CEO
NameCheap
4600 East Washington St, Suite 300
Phoenix, AZ 85034

Dear Mr. Kirkendall,

I write to express concerns about the extent to which your company has ostensibly facilitated sustained covert influence activity by the Russian Federation and influence networks operating on its behalf. In particular, recent disruption actions by the Department of Justice indicate that your company has provided domain registration services to the Russian covert influence network known as "Doppelganger."[1] The Department of Justice and private sector actors have attributed this network to Russian influence organizations Social Design Agency, Structura National Technology, and ANO Dialog all assessed to be operating under the direction and control of the Russian government, including to influence voters in the U.S. 2024 Presidential Election.

Operating since Russia's invasion of Ukraine in 2022, the hallmark of the Doppelganger network has been the impersonation of Western media institutions online. Through the maintenance of both inauthentic social media accounts and websites, Russian influence operatives have impersonated dozens of legitimate organizations as early as September 2022, when the EU Disinfo Lab first identified the network's campaigns.[2] Disturbingly, the EU Disinfo Lab's original report noted the lapses by the domain name industry – including, explicitly, GoDaddy and NameCheap – in facilitating Russian covert influence activity.

Research by Meta in 2023 put into sharper focus the extent to which the global domain name industry has enabled Russian malign influence activity and Doppelganger campaigns, in particular. Specifically, Meta noted a number of ways in which firms such as yours have prevented efforts to address this activity, including withholding vital domain name registration information from good-faith researchers and digital forensic investigators, ignoring inaccurate registration information submitted by registrants, and failing to identify repeated instances of intentional and malicious domain name squatting used to impersonate legitimate organizations.[3] Concerningly, Meta's research even identified instances of Doppelganger impersonating *government* websites – including inauthentic websites posing as the German police, Polish and

[1] Affidavit in Support of Seizure Warrant, *United States of America v. Certain Domains*, Case No.: 24-mj-1395 (E.D. PA 2024).
[2] Alexandre Alaphilippe et al, "Doppelganger: Media Clones Serving Russian Propaganda," EU Disinfo Lab (September 27, 2022).
[3] Ben Nimmo et al, "Adversarial Threat Report – Second Quarter," (August 2023).

Ukrainian governments, NATO, and the French Foreign Ministry facilitated by your services. In the context of the U.S. 2024 Presidential Election, the prospect of foreign actors impersonating state and local government websites – and seeding narratives related to election outcomes or electoral processes – is especially dire.

Information included in the affidavit supporting recent seizure of a number of these domains provides further indication of your industry's apparent inattention to abuses by foreign actors engaged in covert influence. Specifically, Russian influence actors utilized a number of tactics, techniques, and procedures that – against the backdrop of extensive open source literature on Doppelganger's practices – should have alerted your company to abuse of its services, including the use of cryptocurrency to purchase domains, heavy reliance on anonymizing infrastructure to access your registration services (including the use of IPs widely associated with cybercriminal obfuscation network activity), the use of credit cards issued to a U.S. company "that has significant ties to, and employees based in, Russia," use of fictitious and poorly-backstopped identities for registrants, and in at least one instance the use of a Russian address.[4] While there are legitimate rationales for protecting the privacy of domain registrants, repeated and overlapping indications of malicious and/or fraudulent activity should counsel in favor of greater scrutiny and transparency by your industry. Further, many of the domains seized by the Department of Justice – including those impersonating the *Washington Post* and Fox News – bore close resemblance (or in some cases, such as fox-news[.]top and fox-news[.]in, *were identical*) to impersonation domains mimicking those same news organizations in Meta's August 2023 report. The content of these recently-seized domains also exhibited clear use by the Doppelganger network – including use of media trademarks and content identified previously by researchers, as well as impersonation of the same Washington Post and Fox News journalists publicly identified by Meta and others over a year prior.

While foreign covert influence represents one of the most egregious abuses of the domain name system, the industry's inattention to abuse has been well-documented for years, enabling malicious activity such as phishing campaigns, drive-by malware, and online scams – all possible because of malicious actors using your services.[5] Moreover, Meta's report indicates that your industry has effectively externalized the costs of addressing this abusive behavior to victims and third parties – who must pursue costly and time-consuming litigation or dispute resolution via the World Intellectual Property Office.[6]

Given the continued lapses of your industry to address these abuses, I believe Congress may need to evaluate legislative remedies that promote greater diligence across the global domain name ecosystem. In the interim, your company must take immediate steps to address the

---

[4] Affidavit in Support of Seizure Warrant, *United States of America v. Certain Domains*, Case No.: 24-mj-1395 (E.D. PA 2024).

[5] *See, e.g.,* Brian Krebs, "Why is .US Being Used to Phish So Many of Us?," KrebsOnSecurity (November 1, 2023); Zhanhao Chen and Janos Szurdi, "Cybersquatting: Attackers Mimicking Domains of Major Brands Including Facebook, Apple, Amazon and Netflix to Scam Consumers," Palo Alto Networks (September 1, 2020); Ihab Shraim, "New Research Says Domain Registration Fraud Surging in Post-Pandemic Era," Security Infowatch (Feb. 21, 2022).

[6] Ben Nimmo et al, "Adversarial Threat Report – Second Quarter," (August 2023).

continued abuse of your services for foreign covert influence – particularly in the days preceding, and weeks immediately following, Election Day. With the prospect of a close election – and declassified intelligence demonstrating the past practice of foreign adversaries in spreading narratives that undermine confidence in election processes[7] – Americans will be particularly reliant on media organizations and state and local government websites to provide authoritative and accurate election information. It is imperative that your company work to diminish the risk that foreign adversaries use impersonated domains to promote false narratives in this context.

Sincerely,

Mark R. Warner
United States Senator

Cc: Fox News Corporation
Cc: The Washington Post
Cc: The Forward

[7] National Intelligence Council, "Foreign Threats to the 2020 US Federal Elections," Intelligence Community Assessment (March 10, 2021) (describing efforts by Iran, Russia, and foreign hacktivists to denigrate election processes and sow narratives to undermine public confidence in 2020 elections).

MARK R. WARNER
VIRGINIA

United States Senate
WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

October 24, 2024

Mr. Kristaps Ronka
CEO
NameSilo
390 NE 191st St Suite 8437
Miami, FL 33179

Dear Mr. Ronka,

I write to express concerns about the extent to which your company has ostensibly facilitated sustained covert influence activity by the Russian Federation and influence networks operating on its behalf. In particular, recent disruption actions by the Department of Justice indicate that your company has provided domain registration services to the Russian covert influence network known as "Doppelganger."[1] The Department of Justice and private sector actors have attributed this network to Russian influence organizations Social Design Agency, Structura National Technology, and ANO Dialog all assessed to be operating under the direction and control of the Russian government, including to influence voters in the U.S. 2024 Presidential Election.

Operating since Russia's invasion of Ukraine in 2022, the hallmark of the Doppelganger network has been the impersonation of Western media institutions online. Through the maintenance of both inauthentic social media accounts and websites, Russian influence operatives have impersonated dozens of legitimate organizations as early as September 2022, when the EU Disinfo Lab first identified the network's campaigns.[2] Disturbingly, the EU Disinfo Lab's original report noted the lapses by the domain name industry – including, explicitly, GoDaddy and NameCheap – in facilitating Russian covert influence activity.

Research by Meta in 2023 put into sharper focus the extent to which the global domain name industry has enabled Russian malign influence activity and Doppelganger campaigns, in particular. Specifically, Meta noted a number of ways in which firms such as yours have prevented efforts to address this activity, including withholding vital domain name registration information from good-faith researchers and digital forensic investigators, ignoring inaccurate registration information submitted by registrants, and failing to identify repeated instances of intentional and malicious domain name squatting used to impersonate legitimate organizations.[3] Concerningly, Meta's research even identified instances of Doppelganger impersonating *government* websites – including inauthentic websites posing as the German police, Polish and

[1] Affidavit in Support of Seizure Warrant, *United States of America v. Certain Domains*, Case No.: 24-mj-1395 (E.D. PA 2024).
[2] Alexandre Alaphilippe et al, "Doppelganger: Media Clones Serving Russian Propaganda," EU Disinfo Lab (September 27, 2022).
[3] Ben Nimmo et al, "Adversarial Threat Report – Second Quarter," (August 2023).

Ukrainian governments, NATO, and the French Foreign Ministry facilitated by your services. In the context of the U.S. 2024 Presidential Election, the prospect of foreign actors impersonating state and local government websites – and seeding narratives related to election outcomes or electoral processes – is especially dire.

Information included in the affidavit supporting recent seizure of a number of these domains provides further indication of your industry's apparent inattention to abuses by foreign actors engaged in covert influence. Specifically, Russian influence actors utilized a number of tactics, techniques, and procedures that – against the backdrop of extensive open source literature on Doppelganger's practices – should have alerted your company to abuse of its services, including the use of cryptocurrency to purchase domains, heavy reliance on anonymizing infrastructure to access your registration services (including the use of IPs widely associated with cybercriminal obfuscation network activity), the use of credit cards issued to a U.S. company "that has significant ties to, and employees based in, Russia," use of fictitious and poorly-backstopped identities for registrants, and in at least one instance the use of a Russian address.[4] While there are legitimate rationales for protecting the privacy of domain registrants, repeated and overlapping indications of malicious and/or fraudulent activity should counsel in favor of greater scrutiny and transparency by your industry. Further, many of the domains seized by the Department of Justice – including those impersonating the *Washington Post* and Fox News – bore close resemblance (or in some cases, such as fox-news[.]top and fox-news[.]in, *were identical*) to impersonation domains mimicking those same news organizations in Meta's August 2023 report. The content of these recently-seized domains also exhibited clear use by the Doppelganger network – including use of media trademarks and content identified previously by researchers, as well as impersonation of the same Washington Post and Fox News journalists publicly identified by Meta and others over a year prior.

While foreign covert influence represents one of the most egregious abuses of the domain name system, the industry's inattention to abuse has been well-documented for years, enabling malicious activity such as phishing campaigns, drive-by malware, and online scams – all possible because of malicious actors using your services.[5] Moreover, Meta's report indicates that your industry has effectively externalized the costs of addressing this abusive behavior to victims and third parties – who must pursue costly and time-consuming litigation or dispute resolution via the World Intellectual Property Office.[6]

Given the continued lapses of your industry to address these abuses, I believe Congress may need to evaluate legislative remedies that promote greater diligence across the global domain name ecosystem. In the interim, your company must take immediate steps to address the

---

[4] Affidavit in Support of Seizure Warrant, *United States of America v. Certain Domains*, Case No.: 24-mj-1395 (E.D. PA 2024).

[5] *See, e.g.,* Brian Krebs, "Why is .US Being Used to Phish So Many of Us?," KrebsOnSecurity (November 1, 2023); Zhanhao Chen and Janos Szurdi, "Cybersquatting: Attackers Mimicking Domains of Major Brands Including Facebook, Apple, Amazon and Netflix to Scam Consumers," Palo Alto Networks (September 1, 2020); Ihab Shraim, "New Research Says Domain Registration Fraud Surging in Post-Pandemic Era," Security Infowatch (Feb. 21, 2022).

[6] Ben Nimmo et al, "Adversarial Threat Report – Second Quarter," (August 2023).

continued abuse of your services for foreign covert influence – particularly in the days preceding, and weeks immediately following, Election Day. With the prospect of a close election – and declassified intelligence demonstrating the past practice of foreign adversaries in spreading narratives that undermine confidence in election processes[7] – Americans will be particularly reliant on media organizations and state and local government websites to provide authoritative and accurate election information. It is imperative that your company work to diminish the risk that foreign adversaries use impersonated domains to promote false narratives in this context.

Sincerely,

Mark R. Warner
United States Senator

Cc: Fox News Corporation
Cc: The Washington Post
Cc: The Forward

[7] National Intelligence Council, "Foreign Threats to the 2020 US Federal Elections," Intelligence Community Assessment (March 10, 2021) (describing efforts by Iran, Russia, and foreign hacktivists to denigrate election processes and sow narratives to undermine public confidence in 2020 elections).

MARK R. WARNER
VIRGINIA

United States Senate
WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

October 24, 2024

Ms. Sharon Rowlands
CEO
Newfold Digital
5335 Gate Pkwy
Jacksonville, FL 32256

Dear Ms. Rowlands,

I write to express concerns about the extent to which your company has ostensibly facilitated sustained covert influence activity by the Russian Federation and influence networks operating on its behalf. In particular, recent disruption actions by the Department of Justice indicate that your company has provided domain registration services to the Russian covert influence network known as "Doppelganger."[1] The Department of Justice and private sector actors have attributed this network to Russian influence organizations Social Design Agency, Structura National Technology, and ANO Dialog all assessed to be operating under the direction and control of the Russian government, including to influence voters in the U.S. 2024 Presidential Election.

Operating since Russia's invasion of Ukraine in 2022, the hallmark of the Doppelganger network has been the impersonation of Western media institutions online. Through the maintenance of both inauthentic social media accounts and websites, Russian influence operatives have impersonated dozens of legitimate organizations as early as September 2022, when the EU Disinfo Lab first identified the network's campaigns.[2] Disturbingly, the EU Disinfo Lab's original report noted the lapses by the domain name industry – including, explicitly, GoDaddy and NameCheap – in facilitating Russian covert influence activity.

Research by Meta in 2023 put into sharper focus the extent to which the global domain name industry has enabled Russian malign influence activity and Doppelganger campaigns, in particular. Specifically, Meta noted a number of ways in which firms such as yours have prevented efforts to address this activity, including withholding vital domain name registration information from good-faith researchers and digital forensic investigators, ignoring inaccurate registration information submitted by registrants, and failing to identify repeated instances of intentional and malicious domain name squatting used to impersonate legitimate organizations.[3] Concerningly, Meta's research even identified instances of Doppelganger impersonating *government* websites – including inauthentic websites posing as the German police, Polish and

[1] Affidavit in Support of Seizure Warrant, *United States of America v. Certain Domains*, Case No.: 24-mj-1395 (E.D. PA 2024).
[2] Alexandre Alaphilippe et al, "Doppelganger: Media Clones Serving Russian Propaganda," EU Disinfo Lab (September 27, 2022).
[3] Ben Nimmo et al, "Adversarial Threat Report – Second Quarter," (August 2023).

Ukrainian governments, NATO, and the French Foreign Ministry facilitated by your services. In the context of the U.S. 2024 Presidential Election, the prospect of foreign actors impersonating state and local government websites – and seeding narratives related to election outcomes or electoral processes – is especially dire.

Information included in the affidavit supporting recent seizure of a number of these domains provides further indication of your industry's apparent inattention to abuses by foreign actors engaged in covert influence. Specifically, Russian influence actors utilized a number of tactics, techniques, and procedures that – against the backdrop of extensive open source literature on Doppelganger's practices – should have alerted your company to abuse of its services, including the use of cryptocurrency to purchase domains, heavy reliance on anonymizing infrastructure to access your registration services (including the use of IPs widely associated with cybercriminal obfuscation network activity), the use of credit cards issued to a U.S. company "that has significant ties to, and employees based in, Russia," use of fictitious and poorly-backstopped identities for registrants, and in at least one instance the use of a Russian address.[4] While there are legitimate rationales for protecting the privacy of domain registrants, repeated and overlapping indications of malicious and/or fraudulent activity should counsel in favor of greater scrutiny and transparency by your industry. Further, many of the domains seized by the Department of Justice – including those impersonating the *Washington Post* and Fox News – bore close resemblance (or in some cases, such as fox-news[.]top and fox-news[.]in, *were identical*) to impersonation domains mimicking those same news organizations in Meta's August 2023 report. The content of these recently-seized domains also exhibited clear use by the Doppelganger network – including use of media trademarks and content identified previously by researchers, as well as impersonation of the same Washington Post and Fox News journalists publicly identified by Meta and others over a year prior.

While foreign covert influence represents one of the most egregious abuses of the domain name system, the industry's inattention to abuse has been well-documented for years, enabling malicious activity such as phishing campaigns, drive-by malware, and online scams – all possible because of malicious actors using your services.[5] Moreover, Meta's report indicates that your industry has effectively externalized the costs of addressing this abusive behavior to victims and third parties – who must pursue costly and time-consuming litigation or dispute resolution via the World Intellectual Property Office.[6]

Given the continued lapses of your industry to address these abuses, I believe Congress may need to evaluate legislative remedies that promote greater diligence across the global domain name ecosystem. In the interim, your company must take immediate steps to address the

---

[4] Affidavit in Support of Seizure Warrant, *United States of America v. Certain Domains*, Case No.: 24-mj-1395 (E.D. PA 2024).

[5] *See, e.g.,* Brian Krebs, "Why is .US Being Used to Phish So Many of Us?," KrebsOnSecurity (November 1, 2023); Zhanhao Chen and Janos Szurdi, "Cybersquatting: Attackers Mimicking Domains of Major Brands Including Facebook, Apple, Amazon and Netflix to Scam Consumers," Palo Alto Networks (September 1, 2020); Ihab Shraim, "New Research Says Domain Registration Fraud Surging in Post-Pandemic Era," Security Infowatch (Feb. 21, 2022).

[6] Ben Nimmo et al, "Adversarial Threat Report – Second Quarter," (August 2023).

continued abuse of your services for foreign covert influence – particularly in the days preceding, and weeks immediately following, Election Day. With the prospect of a close election – and declassified intelligence demonstrating the past practice of foreign adversaries in spreading narratives that undermine confidence in election processes[7] – Americans will be particularly reliant on media organizations and state and local government websites to provide authoritative and accurate election information. It is imperative that your company work to diminish the risk that foreign adversaries use impersonated domains to promote false narratives in this context.

Sincerely,

Mark R. Warner
United States Senator

Cc: Fox News Corporation
Cc: The Washington Post
Cc: The Forward

[7] National Intelligence Council, "Foreign Threats to the 2020 US Federal Elections," Intelligence Community Assessment (March 10, 2021) (describing efforts by Iran, Russia, and foreign hacktivists to denigrate election processes and sow narratives to undermine public confidence in 2020 elections).

MARK R. WARNER
VIRGINIA

United States Senate
WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

October 24, 2024

Mr. D. James Bidzos
CEO
Verisign
12061 Bluemont Way
Reston, VA 20190

Dear Mr. Bidzos,

I write to express concerns about the extent to which your company has ostensibly facilitated sustained covert influence activity by the Russian Federation and influence networks operating on its behalf. In particular, recent disruption actions by the Department of Justice indicate that your company has provided domain registration services to the Russian covert influence network known as "Doppelganger."[1] The Department of Justice and private sector actors have attributed this network to Russian influence organizations Social Design Agency, Structura National Technology, and ANO Dialog all assessed to be operating under the direction and control of the Russian government, including to influence voters in the U.S. 2024 Presidential Election.

Operating since Russia's invasion of Ukraine in 2022, the hallmark of the Doppelganger network has been the impersonation of Western media institutions online. Through the maintenance of both inauthentic social media accounts and websites, Russian influence operatives have impersonated dozens of legitimate organizations as early as September 2022, when the EU Disinfo Lab first identified the network's campaigns.[2] Disturbingly, the EU Disinfo Lab's original report noted the lapses by the domain name industry – including, explicitly, GoDaddy and NameCheap – in facilitating Russian covert influence activity.

Research by Meta in 2023 put into sharper focus the extent to which the global domain name industry has enabled Russian malign influence activity and Doppelganger campaigns, in particular. Specifically, Meta noted a number of ways in which firms such as yours have prevented efforts to address this activity, including withholding vital domain name registration information from good-faith researchers and digital forensic investigators, ignoring inaccurate registration information submitted by registrants, and failing to identify repeated instances of intentional and malicious domain name squatting used to impersonate legitimate organizations.[3] Concerningly, Meta's research even identified instances of Doppelganger impersonating *government* websites – including inauthentic websites posing as the German police, Polish and

[1] Affidavit in Support of Seizure Warrant, *United States of America v. Certain Domains*, Case No.: 24-mj-1395 (E.D. PA 2024).
[2] Alexandre Alaphilippe et al, "Doppelganger: Media Clones Serving Russian Propaganda," EU Disinfo Lab (September 27, 2022).
[3] Ben Nimmo et al, "Adversarial Threat Report – Second Quarter," (August 2023).

Ukrainian governments, NATO, and the French Foreign Ministry facilitated by your services. In the context of the U.S. 2024 Presidential Election, the prospect of foreign actors impersonating state and local government websites – and seeding narratives related to election outcomes or electoral processes – is especially dire.

Information included in the affidavit supporting recent seizure of a number of these domains provides further indication of your industry's apparent inattention to abuses by foreign actors engaged in covert influence. Specifically, Russian influence actors utilized a number of tactics, techniques, and procedures that – against the backdrop of extensive open source literature on Doppelganger's practices – should have alerted your company to abuse of its services, including the use of cryptocurrency to purchase domains, heavy reliance on anonymizing infrastructure to access your registration services (including the use of IPs widely associated with cybercriminal obfuscation network activity), the use of credit cards issued to a U.S. company "that has significant ties to, and employees based in, Russia," use of fictitious and poorly-backstopped identities for registrants, and in at least one instance the use of a Russian address.[4] While there are legitimate rationales for protecting the privacy of domain registrants, repeated and overlapping indications of malicious and/or fraudulent activity should counsel in favor of greater scrutiny and transparency by your industry. Further, many of the domains seized by the Department of Justice – including those impersonating the *Washington Post* and Fox News – bore close resemblance (or in some cases, such as fox-news[.]top and fox-news[.]in, *were identical*) to impersonation domains mimicking those same news organizations in Meta's August 2023 report. The content of these recently-seized domains also exhibited clear use by the Doppelganger network – including use of media trademarks and content identified previously by researchers, as well as impersonation of the same Washington Post and Fox News journalists publicly identified by Meta and others over a year prior.

While foreign covert influence represents one of the most egregious abuses of the domain name system, the industry's inattention to abuse has been well-documented for years, enabling malicious activity such as phishing campaigns, drive-by malware, and online scams – all possible because of malicious actors using your services.[5] Moreover, Meta's report indicates that your industry has effectively externalized the costs of addressing this abusive behavior to victims and third parties – who must pursue costly and time-consuming litigation or dispute resolution via the World Intellectual Property Office.[6]

Given the continued lapses of your industry to address these abuses, I believe Congress may need to evaluate legislative remedies that promote greater diligence across the global domain name ecosystem. In the interim, your company must take immediate steps to address the

---

[4] Affidavit in Support of Seizure Warrant, *United States of America v. Certain Domains*, Case No.: 24-mj-1395 (E.D. PA 2024).

[5] *See, e.g.,* Brian Krebs, "Why is .US Being Used to Phish So Many of Us?," KrebsOnSecurity (November 1, 2023); Zhanhao Chen and Janos Szurdi, "Cybersquatting: Attackers Mimicking Domains of Major Brands Including Facebook, Apple, Amazon and Netflix to Scam Consumers," Palo Alto Networks (September 1, 2020); Ihab Shraim, "New Research Says Domain Registration Fraud Surging in Post-Pandemic Era," Security Infowatch (Feb. 21, 2022).

[6] Ben Nimmo et al, "Adversarial Threat Report – Second Quarter," (August 2023).

continued abuse of your services for foreign covert influence – particularly in the days preceding, and weeks immediately following, Election Day. With the prospect of a close election – and declassified intelligence demonstrating the past practice of foreign adversaries in spreading narratives that undermine confidence in election processes[7] – Americans will be particularly reliant on media organizations and state and local government websites to provide authoritative and accurate election information. It is imperative that your company work to diminish the risk that foreign adversaries use impersonated domains to promote false narratives in this context.

Sincerely,

Mark R. Warner
United States Senator

Cc: Fox News Corporation
Cc: The Washington Post
Cc: The Forward

[7] National Intelligence Council, "Foreign Threats to the 2020 US Federal Elections," Intelligence Community Assessment (March 10, 2021) (describing efforts by Iran, Russia, and foreign hacktivists to denigrate election processes and sow narratives to undermine public confidence in 2020 elections).