UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MATTHEW SMITH, Individually and on Behalf of All Others Similarly Situated, Plaintiff, -v- F5, INC., FRANCOIS LOCOH-DONOU, EDWARD COOPER WERNER, KUNAL ANAND, and THOMAS DEAN FOUNTAIN, Defendants.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Matthew Smith ("Plaintiff"), individually and on behalf of all other persons similarly situated, by his undersigned attorneys, alleges in this Complaint for violations of the federal securities laws (the "Complaint") the following based upon knowledge with respect to his own acts, and upon facts obtained through an investigation conducted by his counsel, which included, *inter alia*: (a) review and analysis of relevant filings made by F5, Inc. ("F5" or the "Company") with the United States Securities and Exchange Commission (the "SEC"); (b) review and analysis of F5's public documents, conference calls, press releases, and stock chart; (c) review

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

and analysis of securities analysts' reports and advisories concerning the Company; and (d) information readily obtainable on the internet.

Plaintiff believes that further substantial evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery. Most of the facts supporting the allegations contained herein are known only to the defendants or are exclusively within their control.

NATURE OF THE ACTION

1. This is a federal securities class action on behalf of all investors who purchased or otherwise acquired F5 securities between October 28, 2024, and October 27, 2025, inclusive (the "Class Period"), seeking to recover damages caused by Defendants' violations of the federal securities laws (the "Class").

2. Defendants provided investors with material information concerning F5's cybersecurity capabilities and effectiveness. Defendants' statements included, among other things, confidence in the Company's security coverage; Defendants routinely emphasized the importance of effective security measures to its clientele. Defendants' statements included, among other things, confidence in the Company's ability to uniquely address newly developing security concerns, provide best-in-class security offerings, and overall protect its clients' data while capitalizing on the market potential for enhanced security offerings.

3. Defendants provided these overwhelmingly positive statements to investors while, at the same time, disseminating materially false and misleading statements and/or concealing material adverse facts concerning the true state of F5's security capabilities; notably, that it was not truly equipped to safely secure data for its clients as F5 itself was, for all relevant times, experiencing a significant security breach (the "Security Breach") of some of its key offerings and, further, that the revelation of this breach would significantly impact F5's potential to capitalize on the security market. Such statements absent these material facts caused Plaintiff and other shareholders to purchase F5's securities at artificially inflated prices.

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

4. Investors began to question the veracity of Defendants' public statements on October 15, 2025, following a press release and associated 8-K. In pertinent part, Defendants announced a "long-term, persistent" breach to its systems, during which the Company's BIG-IP product development and engineering knowledge management platforms were compromised, including the BIG-IP source code.

5. Investors and analysts reacted immediately to F5's revelation. The price of F5's common stock declined dramatically. From a closing market price of $343.17 per share on October 14, 2025, F5's stock price fell to $295.35 per share on October 16, 2025, a decline of about 13.9% in the span of just two days.

6. Notwithstanding the October 15 disclosures, F5 and the Individual Defendants continued to mislead investors. Defendants did not present information related to the Company's updated financial projections, a potential scope of client exposure, or the cost or significance of the remedial measures underway, planned, or otherwise contemplated. At the time of the disclosure Defendants claimed they were still evaluating the impact of the incident on its financial conditions and operations.

7. The full truth finally emerged on October 27, 2025 when F5 announced their fourth quarter fiscal year 2025 results after the market closed, providing significantly below-market growth expectations for fiscal 2026 due in significant part to the Security Breach as the Company announced expected reductions to sales and renewals, elongated sales cycles, terminated projections, and increased expenses attributed to ongoing remediation efforts. Pertinently, Defendants also disclosed that BIG-IP, the product that was the subject of the Security Breach, is the company's highest revenue product, elevating the scope of the impact from the original disclosure as F5 does not otherwise provide revenue contributions by product line.

8. Investors and analysts again reacted promptly to F5's revelations. The price of F5's common stock declined dramatically. From a closing market price of $290.41 per share on October 27, 2025, F5's stock price fell to $258.76 per share on October 28, 2025, a decline of an additional 10.9% in the span of two days.

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

JURISDICTION AND VENUE

9. Plaintiff brings this action, on behalf of himself and other similarly situated investors, to recover losses sustained in connection with Defendants' fraud.

10. The claims asserted herein arise under and pursuant to §§10(b) and 20(a) of the Exchange Act (15 U.S.C. §§ 78j(b) and 78t(a)) and Rule 10b-5 promulgated thereunder by the SEC (17 C.F.R. §240.10b-5).

11. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. §§1331 and 1337, and Section 27 of the Exchange Act, 15 U.S.C. §78aa.

12. Venue is proper in this District pursuant to §27 of the Exchange Act and 28 U.S.C. §1391(b), as Defendant F5 is headquartered in this District and a significant portion of its business, actions, and the subsequent damages to Plaintiff and the Class, took place within this District.

13. In connection with the acts, conduct and other wrongs alleged in this Complaint, Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce, including but not limited to, the United States mail, interstate telephone communications and the facilities of the national securities exchange.

THE PARTIES

14. Plaintiff purchased F5 common stock at artificially inflated prices during the Class Period and was damaged upon the revelation of the Defendants' fraud. Plaintiff's certification evidencing his transaction(s) in F5 is attached hereto.

15. F5, Inc. is a Washington corporation with its principal executive offices located at 801 5th Avenue, Seattle, Washington 98104. During the Class Period, the Company's common stock traded on the NASDAQ Stock Market (the "NASDAQ") under the symbol "FFIV."

16. Defendant Francois Locoh-Donou ("Locoh-Donou") was, at all relevant times, the President, Chief Executive Officer, and Director of F5.

17. Defendant Edward Cooper Werner ("Werner") was, at all relevant times, the Chief Financial Officer of F5.

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

18. Defendant Kunal Anand ("Anand") was, at all relevant times, the Executive Vice President and Chief Innovation Officer of F5.

19. Defendant Thomas Dean Fountain ("Fountain") was, at all relevant times, the Executive Vice President and Chief Operating Officer of F5.

20. Defendants Locoh-Donou, Werner, Anand, and Fountain are sometimes referred to herein as the "Individual Defendants." F5 together with the Individual Defendants are referred to herein as the "Defendants."

21. The Individual Defendants, because of their positions with the Company, possessed the power and authority to control the contents of F5's reports to the SEC, press releases, and presentations to securities analysts, money and portfolio managers, and institutional investors, *i.e.*, the market. Each Individual Defendant was provided with copies of the Company's reports and press releases alleged herein to be misleading prior to, or shortly after, their issuance and had the ability and opportunity to prevent their issuance or cause them to be corrected. Because of their positions and access to material non-public information available to them, each of these Individual Defendants knew that the adverse facts specified herein had not been disclosed to, and were being concealed from, the public, and that the positive representations which were being made were then materially false and/or misleading. The Individual Defendants are liable for the false statements pleaded herein, as those statements were each "group-published" information, the result of the collective actions of the Individual Defendants.

22. F5 is liable for the acts of the Individual Defendants, and its employees under the doctrine of respondeat superior and common law principles of agency as all the wrongful acts complained of herein were carried out within the scope of their employment with authorization.

23. The scienter of the Individual Defendants, and other employees and agents of the Company are similarly imputed to F5 under respondeat superior and agency principles.

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

SUBSTANTIVE ALLEGATIONS

Company Background

24. F5 is a global multicloud application security and delivery company which enables customers to deploy, secure, and operate applications on-premises or via public cloud. The Company operates through three major product portfolios: F5 Distributed Cloud Services, F5 NGINX, and F5 BIG-IP.

25. In particular, the BIG-IP family of products primarily serves traditional/legacy solutions, providing application security and delivery solutions through packaged software products, including BIG-IP Security, BIG-IP Application Delivery, BIG-IP Automation Tool Chain, BIG-IP Centralized Management, and BIG-IP Next.

The Defendants Materially Misled Investors Concerning F5's Security Capabilities

October 28, 2024

26. On October 28, 2024, Defendants published their fourth quarter fiscal 2024 results. During the corresponding earnings call, Defendant Locoh-Donou praised F5's shift to a "security and software leader" and touted the Company's ability to handle its customer's security, stating, in pertinent part:

> ***In a relatively short period of time, we have substantially reshaped F5 from a hardware-centric, single-product company into a security and software leader in today's hybrid multicloud world.*** Our transformation has redefined F5's role beyond the data center, increasing our value to customers, diversifying our revenue and expanding our total addressable market.
>
> . . .
>
> I will speak first to the industry trends. First, hybrid multicloud environments are now the norm and will remain so. According to our latest State of Application Strategy Report, nearly 90% of customers are operating across multiple environments with the benefits of choice clearly outweighing the challenges of managing apps across different deployment models.
>
> Second, applications and the APIs that connect them are becoming increasingly distributed, which means traditional single-environment solutions are not capable of managing and securing them. Third, the number of application instances

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

continues to grow. In fact, it is projected to grow from roughly 2 billion today to 6 billion by 2029.

Fourth, APIs are rapidly proliferating, creating new challenges and risks for application owners. A recent F5 survey found that nearly 1/3 of customer-facing APIs lack fundamental protection. Fifth, applications and APIs require more security and delivery services today than they used to. In 2016, organizations deployed a minimum of 2 app services to ensure an app remain performant and secure. Today, that number has grown to 13 on average and 27 in total. And finally, the emergence and eventual widespread adoption of AI and AI-powered applications will accelerate and further complicate all of these trends while also leading to new demands related to data ingestion and optimization of GPU environment.

Individually, these dynamics are driving new complexity, cost and security risks for customers. The fact that they are all happening simultaneously is creating significant challenges for the IT teams managing them. ***You have heard us describe the confluence of these dynamics as the ball of fire, and we continue to believe that F5 is uniquely positioned to address it.***

. . .

F5 delivers the most effective and comprehensive app and API security platform in the industry. We enable our customers to consolidate point products, targeting specific threats onto a single integrated platform with a suite of best-in-class capabilities

. . .

The second AI use case we are focused on is AI factory load balancing where we are optimizing the performance and scalability of AI factories with advanced traffic management. Just last week, we announced our exciting collaboration with NVIDIA to enable high-performance software ADC on AI infrastructure.

There are 2 important pieces of this news. ***First, we have enabled BIG-IP Next to run in Kubernetes***. Enterprises and service providers building AI factories are driving strong demand for advanced semiconductors such as GPUs. AI workloads that run within this infrastructure are running on Kubernetes. ***F5 BIG-IP next for Kubernetes brings our market-leading networking, traffic management and security capabilities to these modern environments.***

Second, we partnered with NVIDIA to ensure that BIG-IP Next for Kubernetes works seamlessly with NVIDIA BlueField-3 DPUs. When combined with BIG-IP Next for Kubernetes, these DPUs effectively become AI accelerators, increasing the performance and security of training and inference workloads, delivering superior AI-driven customer experiences.

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

(Emphasis added).

27. Defendant Locoh-Donou also praised F5's new Chief Innovation Officer, Defendant Anand, who was touted as having significant security experience, stating:

> I am pleased to announce that Kunal Anand will lead our product organization as Chief Innovation Officer. After a thorough search that included interviews with leaders from across our industry, it was clear that Kunal had both the experience and perspective required for the role. Through his prior experience leading the technical and security teams at Imperva, Kunal brings deep domain expertise and technical knowledge across cloud, security, networking, SaaS and AI.

28. During the question-and-answer segment of the call that followed management's prepared remarks, Defendant Locoh-Donou detailed the Company's collaboration with Nvidia, suggesting F5's security capabilities are unmatched during the following exchange, in pertinent part:

> <Q: Sebastien Cyrus Naji – William Blair & Company LLC – Associate> And then my second question, just so it's out there, is around the new BlueField NVIDIA announcement. What are you serving as an alternative to here? Are you replacing a native NVIDIA load balancer? And if so, what is the risk for them to build a more competitive offering and drive that higher utilization internally with their own solution?
>
> <A: Francois Locoh-Donou> As it relates to the second question on the BlueField-3 with NVIDIA, look, there will be -- our view of this is we provide a very compelling way of addressing the issue of GPU utilization in GPU cluster. It's an issue for the whole industry. GPUs are expensive and scarce resources, and ***the expertise in Layer 4 through 7, traffic management and security that F5 has, and that is factored for Kubernetes environment, is unique. Nobody else in the industry has that expertise. Nobody else in our industry has those capabilities***. And NVIDIA, of course, recognizes that, which is why we have spent a lot of time with them building this technical solution together.
>
> That being said, of course, I'm sure that others in the industry will look to address this issue over time. And I'm sure that it will be -- there will be competition. It will be a solution that is contested over time. But we think we are early in the market. We think we have a solution that is compelling. ***And we know that the 2 decades of expertise that we have amassed in high-performance traffic management and security directly applies to these AI workloads and that no one brings that expertise to the table today or, frankly, in the foreseeable future***. So we are pretty

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

> confident about the differentiation in the technical solution. The work that is ahead of us is figuring out what are the go-to-market and commercial models that will work for customers in the field.

(Emphasis added).

November 20, 2024

29. On November 20, 2024, Defendants Werner and Anand presented on behalf of F5 at the 2024 RBC Capital Markets Global Technology, Internet, Media and Telecommunications Conference. During the interview, Defendant Anand highlighted the significance of cybersecurity to the Company's customers during the following exchange:

> <Q: Matthew Goerge Hedberg – RBC Capital Markets – Analyst> And then maybe from a technology perspective, I'm always curious, you guys are on the front line of innovation and you're talking to customers. And do you have any like interesting predictions from a technology perspective on -- obviously, everybody wants to talk about Gen AI and all that kind of stuff, but do you have any sort of like crystal ball predictions on, like from a tech perspective, what we should be thinking about?
>
> <A: Kunal Anand> I think cybersecurity is one of the most important
>
> . . .
>
> ***I think the nation state attacks that are happening are in the same when you kind of take a step back, some of the campaigns that are run against critical infrastructure as well as some of the biggest companies in the world***. It's so . . .
>
> <Q: Matthew Goerge Hedberg> Mind-boggling when you see it on the ground.
>
> <A: Kunal Anand> It is and then also the software supply chain, can be underestimated as well and the attacks in the overall supply chain. Most people don't realize how many software component, open source components are in one of these deployments. And all of them are going to be targeted by all these things out there. So I just think that's still issue #1 for a lot of CIOs and CISOs right now is dealing with risk, risk discovery, and risk buy down top of mind

(Emphasis added).

30. Defendant Werner similarly emphasized the significance of cybersecurity to the federal government as well during the following exchange:

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

> <Q: Matthew George Hedberg> What about from a federal exposure? I tend to think software could be an enabler for more government efficiency, because it just feels like the user experience from a federal perspective would certainly improve. What is your -- do you think like F5's role in federal could improve with maybe whether it's us talking about AI or just government is becoming more efficient?
>
> <A: Cooper Werner> Yes. I mean absolutely, ***that's one of the big draws for our technologies.*** We can help customers, whether they're enterprise service provider or the federal government get more efficient in how they deploy their infrastructure, ***security remains of paramount concern, especially in the federal government***. And so we don't think that that's an area that would be where the demand would be negatively impacted overall from any efficiency initiatives. So I think, potentially, there's a little bit of a tailwind on driving broad efficiency into those environments. And then ***security will continue to be a big driver of demand.***

(Emphasis added).

January 28, 2025

31. On January 28, 2025, F5 reported their first quarter fiscal 2025 results. During the corresponding earnings call, Defendant Locoh-Donou touted F5's purported best-in-industry security offering, stating, in pertinent part:

> Over the last several years, we have substantially reshaped F5 for the hybrid and multi-cloud architectures of the AI era. With all its advantages, hybrid multi-cloud also brings with it new challenges. IT teams are being overwhelmed by high cost, crushing complexity and escalating cyber risk, a set of challenges we call the ball of fire.
>
> ***As AI becomes ubiquitous, it will add fuel to the ball of fire, requiring more capacity to handle massive amounts of data, more sophisticated traffic management to deal with complex traffic patterns and enhanced security capabilities to stay ahead of new security threats***. Unlike competitors who invested solely in cloud or SaaS, or significantly reduced investment limiting their applicability in a multi-cloud world, over the last several years, F5 innovated across hybrid SaaS and next-generation software and hardware.
>
> As a result, we stand alone with the only complete hybrid multi-cloud portfolio for application security and delivery. We are the only player that can partner with a CIO or CISO to secure and deliver all of their applications and APIs across hybrid, multi-cloud environments.
>
> . . .

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

> ***F5 has the most effective and comprehensive application and API security platform in the industry***

(Emphasis added).

32. Defendant Locoh-Donou then confidently outlined F5's AI opportunities, which leverage the Company's purported security capabilities and expertise in pertinent part, as follows:

> While AI promises to bring massive productivity benefits, it is also creating new compliance, infrastructure, networking and security challenges for customers. AI is already exacerbating the ball of fire and accelerating the pressure to simplify hybrid multi-cloud deployments.
>
> Our early AI opportunities are concentrated on 3 areas of high-performance data delivery and security. ***The dominant AI opportunity for F5 thus far is delivering and securing data for both AI model training and inference***. AI model training requires higher performance traffic management to ensure the efficiency, speed and reliability of lengthy and expensive training processes. ***Customers are using F5 BIG-IP to move incredible amounts of data at high speed to and from their data stores, providing greater efficiency for the training process.***
>
> . . .
>
> ***The second AI opportunity we see today leverages our market-leading WAP solution for secure AI inferencing***. APIs connect the AI ecosystem and AI APIs are subject to the same security challenges and vulnerabilities as traditional APIs. F5's WAP solutions protect hybrid and multi-cloud applications with functionality that spans from API discovery to API security, which is essential for AI workloads. ***Customers are leveraging F5's complete security portfolio to protect their AI workloads, including BIG-IP, NGINX and F5 distributed cloud services. We expect secure AI inferencing will become a bigger opportunity for F5 as organizations move from experimenting to leveraging AI inferencing at scale.***

(Emphasis added).

April 28, 2025

33. On April 28, 2025, Defendants unveiled their second quarter results. During the associated earnings call, Defendant Locoh-Donou again praised F5's security, claiming the Company "has the most effective and comprehensive application and API security platform in the industry."

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

34. During the question-and-answer segment of the call, Defendant Locoh-Donou highlighted the company's strongest AI use case rests in the BIG-IP platform and its security offering:

> <Q: Amit Jawaharlaz Daryanani – Evercore ISI Institutional Equities – Senior Managing Direct and Fundamental Research Analyst> . . . you talked about sort of 3 use cases on AI that are starting to ramp up from what you folks see. Can you just talk about, at least qualitatively, which of these 3 use cases you think is the largest opportunity from a dollar basis for the company? And then where are you seeing better traction right now versus not?
>
> <A: Francois Locoh-Donou> Yes. That's a really important topic. We are -- the largest use case for us today in terms of where most -- we're seeing most of the dollars is in data delivery for AI models. So this is where we are -- ***BIG-IP is -- typically actually in hardware is being inserted in front of data stores to enable the rapid movement and secure movement of massive amounts of data between data stores and AI applications in training or in inferencing, frankly***. So that is, I would say, the lion's share of the opportunity today. Then when we go to the next 2, we think they are largely ahead of us.
>
> ***We are starting with security and securing web app -- securing AI-powered applications, both with our WAF solution and with the AI Gateway that we just recently announced, which is a new solution that's purpose-built for AI that went GA this quarter, and we're starting to see early traction with that.*** But again, that opportunity is very early. And the third opportunity is also early, which is AI factory load balancing. Again, ***BIG-IP will play an important role in that load balancing traffic in front of AI factories or within AI factories.***
>
> . . .
>
> <Q: Tal Lani – BofA Securities – MD, Head of Technology Supersector and Senior Analyst> . . . we talk a lot about AI, and you have a great position in AI. And this is enterprise AI, right? So the question is about timing. When do you think AI starts to be a meaningful driver or a notable driver to growth?
>
> . . .
>
> <A: Francois Locoh-Donou> And Tal, on your question on AI. Look, we are already driving revenue from AI today. And I mentioned earlier that there are 3 areas where we're driving and seeing growing momentum in AI. And those are specific use cases that our customers identify as AI use cases. There are certain -- we also believe that some of the strength we're seeing in AI -- sorry, in hardware, even in hardware refresh from customers, is actually driven by some of our customers getting ready for AI and increasing capacity and driving expansion in

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

> their data centers for AI, even though they don't necessarily target to that at the time of a transaction with us. And those things are happening today, and we think it's early days, but it is going to grow over time.
>
> We're also very excited, Tal, by the innovation that we are starting to bring to market in AI. So I mentioned earlier that we just launched an AI Gateway, which we think is going to gain traction in the market with the need to secure AI applications to secure large language models. And we're also driving innovation with AI inside of our own portfolio that will further our differentiation and competitiveness in the market. We just launched our Application Delivery and Security Platform. We're leveraging AI in that platform to bring analytics, to bring insights to customers, to make it way easier for them to deliver and secure their applications. And that is a catalyst for growth over time as we consolidate more functionality onto F5 and expand into existing customers.
>
> So the AI opportunity, when you look at it in aggregate, we're really happy with where we are. ***It so happened that the big challenges in AI are moving data and moving data securely. And we happen to have the best technology in the industry to move data security and at real speed for customers. So the opportunity is in front of us and I think will be durable over time.***

(Emphasis added).

May 14, 2025

35. On May 14, 2025, Defendant Anand and Werner presented on behalf of F5 at the 53rd Annual JPMorgan Global Technology, Media and Communications Conference. During the interview, Defendant Anand discussed the significance of security to its customers and how the Company differentiates itself from its competitors with respect to security, in pertinent part, as follows:

> <Q: Samik Chatterjee – JPMorgan Chase & Co – Head of IT Hardware, Telecom and Networking Equipment> Since we are on the topic of AI. Maybe just outline how do you think about how F5 is associated with the enterprise adoption of AI or sort of AI adoption by the enterprises and how F5 can help on that?
>
> <A: Kunal Anand> So I think enterprises are still in more of a foundational phase when it comes to AI today. We roughly see about 3 different use cases related to AI. One is sitting in front of data stores that organizations have. For those that don't quite know in order to get the most utility out of these large language models that are out there, enterprises have found success infusing it with their own enterprise data. And what customers have begun to do is put F5 technology in front of those

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

data stores to help with scaling and to help with the information retrieval that eventually going into these large language models.

The second area is securing access and securing the information that's going to and from those large language models, whether they're locally hosted or in the cloud. And for that, that's where we introduced the F5 AI gateway effectively sit between these applications and APIs as well as these large language models, whether they're deployed somewhere else or locally. And then last but not least, is around load balancing specifically load balancing these AI clusters. How does information get to these clusters and then intra-load balancing as well. So we recently announced the GA of what we're calling BIG-IP next for Kubernetes that runs on NVIDIA's BlueField-3 DPUs, ***which now gives organizations the ability to do delivery and security within an AI factory or inside of an AI super pod***. ***So we really think that those 3 opportunities are very meaningful***.

<Q: Samik Chatterjee> Okay. And do you mind just giving us maybe one more layer down when you think of these 3 use cases where you're seeing sort of the most appetite from customers today and which would be sort of more, I would, I guess, more sort of staggered in terms of ramping up maybe a bit later with the enterprises?

<A: Kunal Anand> . . . Then the second use case around securing access is speaking more to a CISO, and they're truly worried about governance. ***They're truly worried about information security***. And that is something that we see cutting across all enterprises. We announced the AI gateway, and we're seeing early wins right now, which is very promising, but at the same time, ***I think it's very telling of the moment that we're in, which is a lot of companies are experimenting with these large language models, but they don't have the security and the governance that they need to properly lock that down***.

. . .

<Q: Samik Chatterjee> Maybe talk about the competitive landscape, the way you see it today, particularly related to traditional competitors that you've had in the space, Citrix and Radware, and then we can go into sort of the more sort of public cloud competition, but maybe let's talk about the traditional competitors that you've had in this space?

<A: Kunal Anand> Yes. I mean what we've been focusing on is obviously a bunch of innovation around, I would say, modernizing what would be a traditional ADC. When we look at our competitors, Citrix, Radware, et cetera, they spent a lot of time in ADC, but relatively one-dimensional in their capabilities. What we've been focusing on is bridging both delivery and security together. I think for the longest time, ADC has been synonymous with things like load balancing, traffic management.

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

> ***What we've been able to do with a lot of investment and obviously, a lot of work is bridging a lot of the security use cases along with the load balancing and traffic management and that includes application security, API security, bot protection. We really believe that the infusion of security and delivery is fundamentally important. So for us, we think that, that investment in building out that platform play is a core differentiator as it relates to our traditional competitors.***

(Emphasis added).

June 4, 2025

36. On June 4, 2025, Defendants Werner and Fountain presented on behalf of F5 at the Bank of America Global Technology Conference 2025. During the interview, Defendants detailed the significance of cybersecurity to the competitive landscape during the following pertinent exchanges:

> <Q: Tal Liani – BofA Securities – MD, Head of Technology Supersector & Senior Analyst> How is the competitive landscape changing? You are completely dominating the market through technology and systems. In software, when it's in NGINX, do you have different types of competitors are cloud companies, cloud titans, do they offer solutions that compete with you? And how do you see kind of the market evolving?
>
> <A: Thomas Dean Fountain> Yes. So maybe I'll start on kind of our ADC market. We talked a little bit about the competitive dynamics there and that there are far fewer competitors than we've had historically, and I think we're very, very well positioned there. ***Across a number of our security segments, I would describe it as competing with point solutions***. So there are security vendors that have very strong offerings in individual security features***. I think we feel very good about the security efficacy of the products that we have in each of those segments***. ***So we go toe-to-toe with them, but there are a number of competitors there.*** And then certainly, there are some, I'll call them platform type players like the public clouds who offer some basic functionality in a number of these areas that are really optimized for their environment. What I think really stands out is there's nobody who is able to operate across all these different deployment models. And ***so I think we're quite unique in the range of both functions that we're able to provide and environments in which we are able to operate. And for the large organizations that we serve, large enterprise, service providers, governments, that's an absolute necessity. And so I think we stand out in a pretty unique way.***
>
> . . .

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

> <Q: Tal Liani> What happens upon renewal, meaning you spoke about expansion of scope of contracts. Can you elaborate a little bit and tell us what kind of things are driving up the expansion?
>
> <A: Edward Cooper Werner> And then there's what else might serve our needs in the next period, the next 3-year period. And that's where we really have the opportunity to engage with the customer and understand their environment and introduce other components of our portfolio. And we've seen that time and time again where customers have outsized expansion because they've got growth with their existing set of use cases, but they build in new F5 solutions into their expansion. And the third more minor component of the growth is really around price realization. So we've had modest price increases over the last few years. And so that increase in pricing gets built into that next contract.
>
> <Q: Tal Liani> And security gets into the second component you mentioned? [indiscernible] security
>
> <A: Edward Cooper Werner> Yes. ***Typically, that's the way it works. I mean, in some cases, it could be the other way where you have a security solution and they add traffic management***. But typically, when you see expansion, it might be either adding NGINX you referenced earlier, you may have been using BIG-IP and then you say, I've got modern workloads that could be well served. Let's scope NGINX into that next agreement. It could be new security use cases. ***The strength in Q1 was really about expansion into security use cases at the time of renewal. But effectively, it's a lot of new business that's coming forward in the renewal motion.***

(Emphasis added).

July 30, 2025

37. On July 30, 2025, Defendants published their third quarter results for fiscal year 2025. During the same-day earnings call, Defendant Locoh-Donou highlighted F5's "significant competitive advantage" due to its security prowess, stating, in pertinent part:

> Our Q3 results demonstrate F5's position at the forefront of these transformative shifts. We delivered 12% total revenue growth, including 26% growth in product revenue, our strongest in 14 years. This performance is a testament to our team's execution, our continued innovation and the enormous trust the largest enterprises and service providers across the globe place in F5. F5's unique ability to deliver and secure every app, every API anywhere, on premises, in the cloud, at the edge and across hybrid multi-cloud environments is a significant competitive advantage.
>
> . . .

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

> F5 delivers and secures every app and API anywhere, on-prem, cloud, edge or hybrid environments, we lead in solving today's toughest business challenges. Our F5 application delivery and security platform is the first in the industry, offering consistent policies, full visibility and AI-driven insights. We are enabling customers to modernize data centers, embrace hybrid multi-cloud and scale for rising performance and security demands in an AI-driven world.

(Emphasis added).

38. During the question-and-answer segment, Defendants outlined early expectations for fiscal 2026, touting "continued strength" in the Company's renewal process during the following pertinent exchanges:

> <Q: Michael Ng – Goldman Sachs Group, Inc. – Research Analyst> I just have 2. First, on the hardware piece. It's encouraging to hear that you expect systems revenue to be up next year. In the past, you've talked a little bit about how much of the installed base was on the legacy iSeries and VIPRION.
>
> I was just wondering if you could talk about where you are today and how much of that systems refresh we should expect over the next couple of years? And then second, just on software, kind of relatedly, could you see software revenue growth in fiscal '26, just given the very strong term renewals that we've seen this year?
>
> <A: Francois Locoh-Donou> Michael, thank you for the question. We'll do the same thing. I'll start with hardware and ask Cooper to take the second part. On hardware, Michael, we have indeed some end-of-software-support dates that are coming up in '26 and early '27.
>
> ***We expect the refresh to continue to be strong, certainly throughout 2026 and beyond because customers continue to refresh even after these end-of-software-support dates.*** Well after that, they continue to refresh. So not the entire installed base is not refreshed at those dates.
>
> ***So we continue to expect to see that to be strong over the next 18 months.*** Now that said, Michael, there is -- we're seeing a part of our hardware business that is driven not by tech refresh motions, by other trends that I've just articulated around hybrid multi-cloud architectures, data center modernization and increasingly customers investing in AI readiness and AI use cases.
>
> ***We think these trends are less cyclical and more durable***. And so we're excited to see these developments, and we'll see how this play out over time. ***But for the time being, we're really encouraged by what we're seeing outside of the tech refresh motion in our hardware.***

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

<A: Edward Cooper Werner> And then on the software side, it's a little bit early. We wouldn't guide software for next year, ***but I'll kind of give you just a few dynamics for consideration is kind of what's a reasonable estimate from where we sit today. So I'll start with just a way to think about FY '26 in terms of growth rates and then I'll get into some of the dynamics that we're looking at***.

I think it's reasonable to assume software would grow in the mid-single digits for next year and then reaccelerate in the following year. And just to kind of walk through some of the things to consider. So first, we're still seeing really strong consumption in that renewal motion. So as I said earlier, that's increased performance and consumption along with new use cases that are part of that renewal motion.

And just as a point of emphasis, the growth comes from -- over time is coming from new use cases and that increased consumption that's embedded in the renew and expand motion. So it's not simply repeat business.

Then a second dynamic, and we talked about this a little bit on the last call in April, is that the subscription base that comes up for renewal in FY '26, that base largely comes from our software revenue from FY '23 because of that 3-year renewal cycle. And so our FY '23 software sales were roughly flat over FY '22. So that represents a bit of a math headwind on that subscription base where we do that renew and expand motion. And then that same dynamic becomes a tailwind into FY '27, and it's why we would expect the growth rate to reinflect from there.

And then the last dynamic, we touched on it a little bit is just some of the evolving customer preferences around deployment models. And this is really one of the big strengths around our ADSP platform is that we do give customers a choice in how they want to deploy. And so when we talk about hardware and software, something to keep in mind is that those are not products, they're delivery models. BIG-IP is a product.

And some customers are choosing to deploy BIG-IP in that hardware form factor just because of the evolving needs for more performance. And so those are all just things that we consider as we look ahead to next year, and then we'll see how that plays out.

. . .

<Q: Priyanka Thapa – JPMorgan – Analyst> . . . you anticipate hardware to grow strongly in 2026. How much of that strength is this newfound shift where people are using systems instead of software that you would otherwise expect for them to use software like you saw in this particular quarter? Was there -- was this unexpected? And is this a trend that you think might continue?

<A: Edward Cooper Werner> ***Yes. So we would expect hardware to grow, albeit it will be at a more modest growth rate than what we're seeing this current year***

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

> ***because clearly, we're well into the 20% growth rate year-to-date for the current year, but we expect continued growth next year.*** I would say that there is a portion of it that is coming from customer preferences to moving into a hardware model.
>
> I don't think that's the main driver. It's really both tech refresh and some of the dynamics where customers really need more performance and they're trying to scale out their data center capacity to support those performance needs. And then at the margin, there are cases where customers may choose a hardware deployment model in lieu of what previously they may have been thinking software for the deployment model.

(Emphasis added).

September 9, 2025

39. On September 9, 2025, Defendants presented at Goldman Sachs Communacopia and Technology Conference 2025. During the interview, Defendant Locoh-Donou touted the strength of F5's security offerings and capabilities during the following pertinent exchanges:

> <Q: Michael Ng – Goldman Sachs Group, Inc. – Research Analyst> F5 is a leader in the ADC and security market. The company's talks about this intensifying complexity that customers face in a hybrid multi-cloud environment. Could you elaborate on some of the challenges here and why F5 is uniquely situated to address some of the complexities that customers face?
>
> <A: Francois Locoh-Donou> So the complexity that customers face today comes from a couple of what we consider to be secular trends. The first one is that most large enterprises now have embraced hybrid and multi-cloud architectures. They need the flexibility of being in multiple infrastructure environments to deploy their apps in the most efficient way and different apps need different kinds of environment. ***But of course, with that flexibility of being in multiplying cloud environments comes a complexity of securing and delivering apps across these environments***. So that's first source of complexity.
>
> . . .
>
> ***The reason we're very well positioned to address that is because we made a strategic choice several years ago to remain entirely focused on application and API delivery and security***. But within that category, to invest across hardware, software and Software as a Service, such that we could secure and deliver all these apps and APIs across all these infrastructure environments.
>
> And increasingly, we have been bringing all products, all of these form factors in our portfolio into a single platform to make it even easier for customers to operate across multi-cloud environments.

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

. . .

<Q: Michael Ng> Could we just talk a little bit about security. I mean the company has, I think, increasingly been incorporating and investing in security capabilities across its entire portfolio. And I think, last year, security represented about 41% of revenue. Why is F5 well positioned to address application security when you think about security as an umbrella, like which facets of security does F5 compete in most aggressively?

<A: Francois Locoh-Donou> So the -- I'm going to go back to what I said earlier, that we -- ADCs control 100% of the traffic going into mission-critical applications. Originally, our customers use that -- the ADC capability, this very granular inspection of application traffic. They use it primarily to keep the applications performing and to keep them available. But ***over time, customers have realized that, that place of inspection was an ideal place to also secure applications, protect them before attacks reach the applications or the database behind the application. And so F5 has been in security now for over a decade, primarily from this place of inspecting traffic very granularly and securing applications.***

Today, application delivery and security have converged. You cannot really separate performance of an application from the application being secure. And that makes F5 absolutely critical to all application security. Now where we do that today is in three places.

First is, we secure the front end of all applications in APIs with our -- what we call our WAAP portfolio, which is web application API protection. So we secure the front end of applications with those solutions in also in hardware, software or SaaS. Two is, we also secure users in the workforce by securing their access with our Zero Trust Access solution, securing their access to applications.

And increasingly, we're bringing our capabilities to securing the new AI stack. And so we -- these -- if you should think about it in AI, securing AI basically requires securing every token. And that is more of a Layer 7 capability, and that's where F5 shines. So we are bringing this capability. We've built -- introduced a product called an AI Gateway that secures the connections between AI applications and AI models, provide delivery and security for these connections. That's very specific to AI traffic and AI protocols. And we're going to augment the capabilities of this solution going forward because we think AI security as a market is one where F5 has an important role to play.

(Emphasis added).

40. Defendant Locoh-Donou further emphasized the significance of the continued security opportunity for F5 and highlighted the Company's focus on a joint application and

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

security platform that necessarily relies on F5's security capabilities during the following exchange:

> <Q: Michael Ng> Francois, in closing, I was just wondering if you could tie it all together for us and talk about the next 12 to 24 months key priorities, things you're most excited about. It seems like between ADC refresh, nonrefreshed demand wins, AI, the term renewal seeing good expansion rates, it seems like there's a lot of things going in your favor right now, but perhaps you can pull it all together for us.
>
> <A: Francois Locoh-Donou> Yes. ***Our focus over the next 12, 24 months, #1 is our application delivery and security platform***. So bringing our product families together under a single platform that really makes things way easier for -- ***it has a benefit of making things way easier for our customers in terms of securing and delivering all their apps across all their environments***, but doing that with essentially a single way of provisioning policies, orchestrating their environment, visualizing their environment.
>
> ***And so that application delivery and security platform and making that real for our customers is kind of the #1 priority***. And then second is AI. And in AI, we see opportunity in AI data delivery that I mentioned, which we think is largely an opportunity in hardware for BIG-IP. And we see opportunities in AI security that are nascent and also inside of AI factories.
>
> So really, these are very early opportunities. It's a space that is nascent that we understand less well because there's less of a history and a track record. And it's very difficult to extrapolate numbers from this because it's very early days. But we see the opportunity. And so we are focused on the work to bring these opportunities to life.

(Emphasis added).

41. The above statements in Paragraphs 26 to 40 were false and/or materially misleading. Defendants created the false impression that they possessed reliable information pertaining to the Company's projected revenue outlook and anticipated growth while also minimizing risk from seasonality and macroeconomic fluctuations. In truth, F5's optimistic claims, touting its purported best-in-industry security and overall emphasis and confidence in the Company's ability to meet and capitalize on the growing security needs for its clientele fell short of reality; F5 was, at the time, the subject of a significant security incident, placing its clientele's security and the Company's future prospects at significant risk. Defendants misled investors by

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

providing the public with materially flawed statements of confidence and growth projections which did not account or otherwise disclose the existence or potential of a security incident.

F5 Discloses a Persistent Security Breach of its BIG-IP Product Development Environment

October 15, 2025

42. On October 15, 2025, Defendants published a press release announcing a significant security breach that they had purportedly uncovered more than two months prior to the disclosure. In pertinent part, Defendants detailed the Security Breach and its exposure as follows:

> ***In August 2025, we learned a highly sophisticated nation-state threat actor maintained long-term, persistent access to, and downloaded files from, certain F5 systems. These systems included our BIG-IP product development environment and engineering knowledge management platforms***. We have taken extensive actions to contain the threat actor. Since beginning these activities, we have not seen any new unauthorized activity, and we believe our containment efforts have been successful.
>
> In response to this incident, we are taking proactive measures to protect our customers and strengthen the security posture of our enterprise and product environments. We have engaged CrowdStrike, Mandiant, and other leading cybersecurity experts to support this work, and we are actively engaged with law enforcement and our government partners.
>
> We have released updates for BIG-IP, F5OS, BIG-IP Next for Kubernetes, BIG-IQ, and APM clients. More information can be found in our October 2025 Quarterly Security Notification. We strongly advise updating to these new releases as soon as possible.
>
> What we know
> At this time, based on our investigation of available logs:
>
> - ***We have confirmed that the threat actor exfiltrated files from our BIG-IP product development environment and engineering knowledge management platforms. These files contained some of our BIG-IP source code and information about undisclosed vulnerabilities we were working on in BIG-IP***. We have no knowledge of undisclosed critical or remote code vulnerabilities, and we are not aware of active exploitation of any undisclosed F5 vulnerabilities.

(Emphasis added).

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

43. The corresponding 8-K filing provided some additional details concerning both the company's purported discovery of the Security Breach and the timing of the disclosure itself, stating, in pertinent part:

> ***On August 9, 2025***, F5, Inc. . . . learned that a highly sophisticated nation-state threat actor had gained unauthorized access to certain Company systems.
>
> . . .
>
> On September 12, 2025, the U.S. Department of Justice determined that a delay in public disclosure was warranted pursuant to Item 1.05(c) of Form 8-K. F5 is now filing this report in a timely manner.
>
> As of the date of this disclosure, this incident has not had a material impact on the Company's operations, and the Company is evaluating the impact this incident may reasonably have on its financial condition or results of operations.

(Emphasis added).

44. The aforementioned press releases and statements made by the Individual Defendants are in direct contrast to statements they made during the October 28, 2024, November 20, 2024, January 28, 2025, April 28, 2025, May 14, 2025, June 4, 2025, July 30, 2025, and September 9, 2025 earnings calls and investor presentations. On those calls and presentations, Defendants continually praised F5's security potential, offerings, and overall experience and expertise, while continually minimizing the risks associated with the ongoing breach of its systems and/or F5's capability to properly secure itself.

45. Investors and analysts reacted immediately to F5's revelation. The price of F5's common stock declined dramatically. From a closing market price of $343.17 per share on October 14, 2025, F5's stock price fell to $295.35 per share on October 16, 2025, a decline of about 13.9% in the span of just two days.

46. A number of well-known analysts who had been following F5 highlighted the initial disclosure, but also emphasized that little was disclosed as to the potential impacts to F5's business. For example, Raymond James, while reiterating their market perform rating but highlighting a

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

"negative" sentiment, summarized that "F5 disclosed a material security incident via an 8K that stated the company learned on August 9 that a nation-state threat actor gained long-term persistent access (Bloomberg reports at least 12 months) to some company systems." The analyst went on to highlight that "it's early to tell what impacts may come to results, customer behavior or legal scrutiny the company may come under. That said, our worry is the unknown impacts given the long-term access by the threat actor to undisclosed vulnerabilities along with the BIG-IP development environment."

47. Similarly, CFRA, while maintaining their 'hold' opinion noted that "Beyond high-level details, not much is known about who is behind the attack or what the fallout from the attack will be. We hope to get more of an update during its earnings call on October 27 but doubt we will receive much given the nature of the attack."

48. The fact that these analysts, and others, discussed F5's surprise Security Breach announcement suggests the public placed significant weight on F5's prior statements detailing a focus on and confidence in the Company's security offerings. The frequent, in-depth discussion of the Security Breach and corresponding breach of F5's systems confirms that Defendants' statements during the Class Period were material.

49. Notwithstanding Defendants' disclosures during the call, they continued to mislead investors by omitting key details from their disclosure related to any updated financial projections, a potential scope of client exposure, or the cost and scope of planned and current remedial operations. In doing so, Defendants minimized the significance and scope of the breach to the company's continued prospects and ability to capitalize on the growing security market.

50. The above statements in Paragraphs 31 to 35 were false and/or materially misleading. Defendants omitted key information related to the scope of exposure, ongoing costs, and future losses or otherwise potential missed opportunities caused by the Security Breach. Defendants misled investors by providing the public with only partial information despite the significant two-month gap between purported detection and public disclosure of the Security

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

Breach. This prevented investors from properly valuing F5 after the Security Breach was revealed until Defendants eventually articulated the impacts during the fourth quarter earnings call.

The Truth Emerges during F5's Fourth Quarter Earnings Report

October 27, 2025

51. In the evening of October 27, 2025, F5 published its fourth quarter fiscal year 2025 results; notably highlighting a significant impact to the company's business going forward. In pertinent part Defendant Locoh-Donou provided full-year results and highlighted the steps taken following the discovery of the Security Breach, stating, in pertinent part:

> In FY '25, we maintained our strong profitability, delivering gross margins of 83.6%, up 80 basis points over FY '24, an operating margin of 35.2%, up 160 basis points over FY '24. This performance resulted in record free cash flow of $906 million, up 19% compared to FY '24 underscoring the strength of our financial model and execution.
>
> Our FY '25 results demonstrate the power of our platform and our strategic role in the marketplace. They also strengthen our confidence in our vision and road map for the future. Our immediate focus, however, has been on our incident response and I will speak to our priorities and offer an update on where we are now.
>
> Upon identifying the threat on August 9, our team immediately activated our incident response process. Our priorities were clear. First, contain the threat actor, initiate a thorough investigation and take immediate and urgent action to strengthen F5's security posture. While the investigation will continue and the work of bolstering our security posture will expand, our initial steps have been successful.
>
> Second, we prioritized delivering reliable software releases to address all undisclosed high vulnerabilities in BIG-IP code as quickly as possible. Through the exceptional efforts of our engineering and support teams, we achieved this, enabling thousands of customers to promptly deploy critical updates upon disclosure.
>
> Our customers are moving quickly to update their BIG-IP environment, and a significant number of our largest customers have completed their updates with minimal disruption. As an example, a North American technology provider completed updates to 814 devices in a 6-hour window in the first weekend. Customers have expressed appreciation for our transparency, the thoroughness of the information we provided and the clarity in the steps they need to take to improve the security of their environment.
>
> . . .

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

> Our third priority is raising the bar on security across all aspects of our business. We are acutely aware of the increasing sophistication of attackers and the fact that the threat surface is expanding rapidly. Each year, over the last several years, we have aggressively increased our investment in security, and we are making further significant investment this year and beyond.
>
> To further this work, Michael Montoya, a recognized cybersecurity expert and former member of our Board, has joined F5 as Chief Technology Operations Officer. Michael brings deep operational expertise and will drive the execution of a robust road map to further enhance security across our internal processes, environments and products. Our goal across all these actions is to better protect our customers and we believe F5 will be a stronger partner to customers because of it.
>
> ***We know customers will judge us by how we respond to this incident***. Throughout this process, we have been committed to transparent customer communication at every step, reflecting lessons learned from how others have navigated similar challenges***. We acknowledge that we may see some near-term impact to our business.*** We are fully focused on mitigating that impact while doubling down on the value we deliver to our customers.

(Emphasis added).

52. Defendant Werner provided the Company's underwhelming first quarter and full fiscal year 2026 outlook, detailing previously undisclosed impacts due to the Security Breach, in pertinent part:

> As we enter FY '26, we see several persistent demand drivers, including hybrid multicloud adoption driving expansion across our platform, the continuing strong systems refresh opportunity with more than half of our installed base on legacy systems nearing end of software support, growing systems demand beyond tech refresh for data sovereignty and AI readiness use cases and a return to growth in revenue from our SaaS and managed services with the transition of legacy offerings largely completed in FY '25.
>
> These drivers in our current pipeline support mid-single-digit revenue growth in FY '26 against our exceptional 10% growth in FY '25. ***However, we also anticipate some near-term disruption to sales cycles as customers focus on assessing and remediating their environments. Taking this into account, we are guiding FY '26 revenue growth in the range of 0% to 4% with any demand impacts expected to be more pronounced in the first half, before normalizing in the second half.***
>
> Moving to our operating model. We ***recognize the revenue guide may lead to a modest impact to our operating margin near term.*** We are committed to driving

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

> continued operating margin leverage and believe any demand impact is likely to be short term and therefore any effect on our operating model would also be temporary.
>
> With that context, we estimate FY '26 gross margin in a range of 83% to 83.5%. We estimate FY '26 non-GAAP operating margin to be in the range of 33.5% to 34.5% with operating margins lowest in our fiscal Q2 due to payroll tax resets in January and costs associated with our large customer event in March. We expect our FY '26 non-GAAP effective tax rate will be in a range of 21% to 22%. And we expect FY '26 EPS in a range of $14.50 to $15.50. Finally, we intend to continue to use at least 50% of our free cash flow towards share repurchases in FY '26.
>
> Turning to our Q1 outlook. We expect Q1 revenue in a range of $730 million to $780 million. ***This is the wider range than we would typically guide, reflecting the potential for some near-term disruption to sales cycles***. While we are not guiding revenue mix, we expect Q1 software to be down year-over-year given the strong growth in the year-ago period. We expect non-GAAP gross margin in a range of 82.5% to 83.5%. We estimate Q1 non-GAAP operating expenses of $360 million to $376 million. We expect Q1 share-based compensation expense of approximately $61 million to $63 million. We anticipate Q1 non-GAAP EPS in a range of $3.35 to $3.85 per share.

(Emphasis added).

53. Defendants elaborated further on the continuing impact of the Security Breach during the following pertinent exchanges in the question-and-answer segment of the call:

> <Q: Meta A. Marshall – Morgan Stanley – Vice President> Just a question in terms of what form of kind of conservatism have you put into the estimates? I guess I'm just trying to get a sense of are you accommodating customers through discounting? Is this you're pushing off -- maybe people are pushing off purchasing decisions while they're handling kind of servicing or upgrading incidents? Or are you having to give other incentives to kind of upgrade boxes? Just trying to get a sense of kind of what form that kind of customer conservatism is taking?
>
> . . .
>
> <A: Francois Locoh-Donou> Let me just start from -- you saw that we delivered a very strong quarter and, in fact, a very strong fiscal 2025. And the momentum in the business has been very, very strong. And that is driven increasingly by the secular trends that we've talked about, specifically hybrid multicloud and AI, and I can come back to that a little bit later.
>
> ***Based on these trends, we felt the trajectory of the business going into 2026 was more in the mid-single-digit growth. But we said we are guiding to 0% to 4%***

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

growth for 2026 based on what we see as potential near-term impact related to the security incident. And when I say near-term impact, we think we would see probably the majority of the impact in the first half of the year with trends kind of normalizing in the second half of the year. So let's double click on this near-term impact for your question.

What we have in there, Meta, is really ***3 categories of things that could create near-term disruption. The first is that we have our own resources, our field resources and sales resources over the last few couple of weeks, and I think that will go on for a few more weeks***, have really been focused on attending customers, helping them upgrade their environments, remediate issues, answer any questions, et cetera. ***And inevitably that takes time away from normal sales cycles. And the same is true for customers who are putting a lot of resources on upgrading their BIG-IPs, ensuring their environment is in the right place and that takes time away from considering the next project***. So that is a short-term disruption around allocation of resources both at F5 and with our customers.

There's a second potential disruption that we have considered in our guidance which is that given the visibility that this security incident has had, it would be natural that in some of our customers at an executive level, we may see some delays of approvals or delays of deals or additional approval as customers across a complex organization make sure that they want to be reassured that their project should move forward and they have no further interrogation around that. That's the second consideration.

And then the ***third one is that potentially for some of our customers there may be some projects that they were going to move forward with, and they end up deciding not to do that***. And we have considered that as a third potential impact. Now, I want to be clear, the -- everything I've just talked about, as you know, Meta, more than 70% of our revenues are recurring. Everything I've just talked about with the impact that would be mostly with new projects or new footprint acquisition. And so far, it is very early days because this was disclosed only 2 weeks ago. We haven't seen any of the impacts that I'm talking about, but we are very prudent about this because we are very, very early after the disclosure and the interaction with customers. Cooper?

. . .

<Q: George Charles Notter – Wolfe Research, LLC – MD & Senior Analyst> Just continuing on that line of discussion, I guess I'm curious about how you actually size the potential impact from the security breach. I would imagine it's probably a complex exercise, but I'm curious if you could just kind of walk us through like the logic here. And then maybe related to that, can you give us a sense for how many customers were affected where there was configuration information taken or are there specific customer issues that you can point to?

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

<A: Edward Cooper Werner> Yes. Sure, George. This is Cooper. I'll take the first part, and then François can address the second question. So François kind of touched at it a little bit at a high level when he kind of referenced the percentage of our business that is recurring in nature. But ***as we went through this process, we really took a fairly granular approach at kind of profiling our revenue base across all the different revenue streams and kind of taking a look at which of these revenue streams could be more impacted and which ones would be more resilient in the near term.***

So if you think about our revenue base, a lot of the revenue that we recognize comes straight off the balance sheet. So our service revenue -- that maintenance revenue is mostly coming off of deferred revenue. We've got our -- this is, for example, our SaaS revenue is coming out of beginning ARR and then we've got a lot of our software businesses coming through in the form of subscription renewals. So those are revenue streams that are highly resilient, and we wouldn't expect to have much of a near-term impact.

And ***then if you look at kind of newer use cases, whether that's competitive takeout or new software projects, that's where there potentially could be more of a near-term impact.*** And so we kind of looked at these different cohorts of our revenue base and just kind of made a judgment as to what the potential impact could be in the near term as customers are kind of going through some of their operational activities around the incident.

And then we also kind of balance that just looking at other peers historically that have gone through similar incidents and what revenue impacts they saw. And then, of course, we've spent a lot of time with our sales teams, just kind of assessing at the outset what their view was as to what impact, if any, they might see and then continuing those conversations as they've engaged with their customers in the field. And I think we're very encouraged by some of the early feedback we've gotten from those conversations. They've been very healthy discussions with customers in helping them kind of address some of these early concerns. And I think we're feeling pretty good about our relationship and how those interactions are going with our customers.

<A: Francois Locoh-Donou> And I'll take the second part of your question, George, on customer impact. First of all, I do want to take this opportunity to say that, of course, we are disappointed that this happened and very aware as a team and as a company of the burden that this has placed in our customers who have had to work long hours to upgrade their BIG-IPs and secure their environment. And we're continuing to work with all of our customers in ensuring that they are in the place they want to be.

With that said, the customers who were impacted, so we shared that there was no evidence of access to F5 Distributed Cloud Services environment or NGINX environmental. ***So it was essentially BIG-IP customers that were impacted. There***

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

were really 2 categories of impact. All of our BIG-IP customers, we recommended strongly to all of them that they upgrade their BIG-IP to the latest releases that we worked very hard to make available on the day of disclosure.

And we were very impressed frankly, with the speed with which our customers have mobilized resources to be able to make these upgrades and put them in production fairly rapidly. So the impact really on them was having to mobilize resources to do that work shortly after our disclosure. And we are actually pleased that a lot of customers are through that work. It will continue, but we're very pleased to see the speed with which customers have upgraded their BIG-IP.

The second category of impact was related to data exfiltration. That impacted a small percentage of our customers for -- and we will continue to go through the sort of e-discovery process around what specific data with the customer -- but from the first body of work that we have done on that, we have already identified the customers that were impacted and we have sent them their information, their data package for the data that might have been exfiltrated. And the most common feedback from customers so far has been that, that data is not sensitive, and they're not concerned about it. There was no impact to our CRM or our support system.

. . .

<Q: Michael Ng – Goldman Sachs Group, Inc. – Research Analyst> I just have two. First, just on OpEx, it seems like the implied OpEx growth for fiscal '26 is about 4% at the midpoint. Just wondering if you're seeing any additional costs as a result of the data breach, other investments in systems internally or costs related to offering free Falcon EDR subscription to affected customers. And then second, certainly encouraging to hear that it was just BIG-IP that was impacted, not NGINX or DCS. Could you just tell us what percentage of the revenue comes from BIG-IP?

<A: Edward Cooper Werner> We don't break out our product by revenue line. We're a single-segment company, but it's -- ***BIG-IP is the highest revenue product, of course, but we don't actually break out what the contribution is.***

And then in terms of investment security and the OpEx, so yes, ***we actually have been investing aggressively in secured -- cybersecurity over the last several years. We've more than doubled our investment in cybersecurity just in the last 3 years alone. And we had already accounted for continued investment in our planning for this year even before we learned of this incident***. And of course, we've learned a lot in the last several weeks, and so ***there's some additional investments incorporated into our planning,*** but that was among the highest priority areas of investment in our plan going into the...

<Q: Michael NG> And any costs related to the Falcon EDR subscription?

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

> <A: Edward Cooper Werner> ***Yes. So there are a number of costs related to the incident remediation and in the offering that you're referencing as part of that, those are either going to be accounted for in our -- with our cyber insurance or they would be remediation costs that are accounted for separately as a onetime expense***.

(Emphasis added).

54. Defendant Locoh-Donou went on to detail additional remedial efforts F5 would now have to undergo in an attempt to restore investor confidence in the Company's security offerings during the following exchange:

> <Q: Amit Jawaharlaz Daryanani – Evercore ISI Institutional Equities – Senior Managing Director & Fundamental Research Analyst> And then François, just on the breach side and the challenges you're having, can you just -- maybe just help us understand if the source code is compromised, how do you give customers the confidence that there's no zero-day threat that's kind of hiding in there over time? Just maybe walk through that. And then does this also dampen your ability to implement price increases when it comes to the hardware side, really to reflect what Citrix has been doing to some extent in that space. So I'd love to just understand kind of the zero-day risk and the potential for price increases maybe being a bit more muted there as you go forward.
>
> <A: Francois Locoh-Donou> Thank you. Well, let me start with the code and then let's come back to price increase as a separate topic. Look, I said earlier that I think customers will continue to choose F5 because we provide best-in-class app delivery and security capabilities for our customer. ***Now when you look at the code, I shared earlier some of the things that we are doing to ensure that we remain vigilant about potential vulnerabilities in our code***. And so we have engaged partners that are scanning our code and will continue to do so to ensure that if there are any vulnerabilities that we remediate them immediately.
>
> ***I shared with you that we are setting up a trust center that will be there to allow our customers to come and do penetration testing with our code. We are going to leverage AI for hunting for penetration as well in our code. We are enhancing our bug bounty program. So there are a number of things that we are putting in place, all designed to ensure we remain hypervigilant about this, and we give customers maximum comfort around the security of our code going forward.***
>
> And I think in our industry we really intend to be best-in-class in doing this. And I think as we have these conversations and frankly, as we have shared these plans and these road maps around the things we're going to do with our customers, they have been very pleased with our response and I think are getting a lot of comfort

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

> that we are doing all the right things to ensure that their -- the product they get from F5 continue to be safe and free of potential vulnerabilities or zero days.
>
> I would also say that we have taken this further, and you may have seen in our disclosure that ***we are working with CrowdStrike to implement EDR capabilities on BIG-IP***. And that's an extra layer of protection that we are offering customers to have way more observability, monitoring into their BIG-IPs which is something that hasn't been done in the industry. You haven't seen perimeter devices really enabled with EDR. And so it's just one example of where we are innovating with other industry partners to raise the game on security for our customers.

(Emphasis added).

55. The aforementioned press releases and statements made by the Individual Defendants contradicted their earlier statements and provided significant additional disclosures that were omitted from F5's October 15, 2025 press release and associated publications. When disclosing the existence of the Security Breach, Defendants failed to articulate the significant impact to the Company's projections, planned or ongoing remediation efforts, or the scope of how many BIG-IP customers were impacted.

56. Investors and analysts again reacted promptly to F5's revelations. The price of F5's common stock declined dramatically. From a closing market price of $290.41 per share on October 27, 2025, F5's stock price fell to $258.76 per share on October 28, 2025, a decline of an additional 10.9% in the span of two days.

57. A number of well-known analysts who had been following F5 lowered their price targets in response to F5's disclosures. For example, J.P. Morgan, while dropping its price target nearly 8%, summarized the earnings call, noting "the biggest focus on the earnings call and relative to the outlook shared by management was the recent security breach, which has led F5 to take corrective measures to ensure protection of customer environments." The analyst further highlighted the company's disappointing guidance: "given the resources diverted to addressing customer needs as well as the potential ramifications in terms of customers delaying / pausing projects against the backdrop of this breach, F5 is embedding significant conservatism in its guide for F1H26 with expectations of potential revenue impact across both Hardware and Software."

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

58. Similarly, Evercore ISI, dropping their price target by a more significant 12.5%, pointed out the "much softer Dec-qtr/FY26 guide vs. street expectations reflecting headwinds from the recent security breach involving the Big-IP product." The analyst affirmed the "delta vs. expectations [in the guide] is largely driven by potential weakness in purchasing and/or elongated sales cycle post the recent BIG-IP breach. FFIV noted that excluding the breach impact, revenues would be up mid-single digits from strong secular demand drivers … in line with street models."

59. The fact that these analysts, and others, discussed F5's guidance shortfall and overall continuing impact of the Security Breach suggests the public placed significant weight on F5's statements of prior confidence in their security systems and investments, alongside the lack of any continued or future impact disclosure on October 14, 2025, when the Security Breach was initially disclosed to the public. The frequent, in-depth discussion of F5's guidance confirms that Defendants' statements during the Class Period were material.

Additional Scienter Allegations

60. During the Class Period, Defendants acted with scienter in that they knew, should have known, or otherwise were deliberately reckless in not knowing that the public statements disseminated on behalf of F5 were materially false and misleading at the time they were made. Defendants had actual knowledge of, or access to, non-public information concerning the existence, scope, duration, and severity of the incident Security Breach, including that a sophisticated actor had breached F5's BIG-IP product development environment, accessing sensitive source code and vulnerability information, or otherwise that vulnerabilities existed such that the Company could be breached by such an actor.

61. Notwithstanding such, Defendants repeatedly and affirmatively represented to investors that F5 possessed "best-in-class" security capabilities, that customer environments and F5's own systems were secure, and that Defendants were well-positioned to capitalize on the growing security demand.

62. Defendants' scienter was further evidenced by their statements during the class period. Defendants repeatedly claimed to investors that F5 maintains the best security in the

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

industry, despite that Defendants were aware that F5 had significant security vulnerabilities which were currently being exploited.

63. For example, during the above-referenced class period, Defendant Donou repeatedly made claims as to the efficacy and capability of F5's security offerings in comparison to its competitors, stating, in pertinent part:

> F5 delivers the most effective and comprehensive app and API security platform in the industry
>
> . . .
>
> F5 has the most effective and comprehensive application and API security platform in the industry
>
> . . .
>
> And we happen to have the best technology in the industry to move data security and at real speed for customers

64. Similarly, Defendant Anand pertinently spoke to F5's significant investment in its security capabilities, highlighting that the "investment in building out that [security] platform play is a core differentiator as it relates to our traditional competitors."

65. Additionally, Defendant Werner pertinently noted that the big "draw" and "driver of demand" for F5 was its security offering as it remains a "paramount concern" for its clientele, especially in the federal government."

66. Finally, Defendant Fountain remarked that they "feel very good about the security efficacy of the products that we have … And so I think we're quite unique in the range of both functions that we are able to provide and environments in which we are able to operate."

67. Notably, even after Defendants claim to have first learned of the Security Breach, on August 9, 2025, Defendants made no efforts to warn investors or clients of the potential vulnerabilities and instead continued to tout their security offerings. In pertinent part, on September 9, 2025, Defendant Donou pertinently claimed that "[y]ou cannot really separate performance of an application from the application being secure. And that makes ***F5 absolutely***

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

critical to all application security" (emphasis added).

68. Scienter is further supported by Defendants' selective and misleading disclosure on October 15, 2025. While Defendants finally acknowledged to the public the existence of the "long-term, persistent" Security Breach, they simultaneously asserted the "incident has not had a material impact on the Company's operations, and the Company is evaluating the impact this incident may reasonably have on its financial condition or results of operations."

69. Less than two weeks later, however, Defendants promptly reversed course, disclosing significantly reduced growth expectations attributable to the Security Breach and its subsequent disclosure.

Loss Causation and Economic Loss

70. During the Class Period, as detailed herein, Defendants made materially false and misleading statements and engaged in a scheme to deceive the market and a course of conduct that artificially inflated the price of F5's common stock and operated as a fraud or deceit on Class Period purchasers of F5's common stock by materially misleading the investing public. Later, Defendants' prior misrepresentations and fraudulent conduct became apparent to the market, the price of F5's common stock materially declined, as the prior artificial inflation came out of the price over time. As a result of their purchases of F5's common stock during the Class Period, Plaintiff and other members of the Class suffered economic loss, *i.e.*, damages under federal securities laws.

71. F5's stock price fell in response to the partial corrective event on October 15, 2025, as alleged *supra*. On October 15, 2025, Defendants disclosed information that was directly related to their prior misrepresentations and material omissions concerning F5's security capabilities and expertise in serving its clientele.

72. In particular, on October 15, 2025, F5 announced a "long-term, persistent" breach of the Company's critical BIG-IP development suite.

73. F5's stock price fell again in response to the corrective event on October 27, 2025, as alleged *supra*. On October 27, 2025, Defendants disclosed information that was directly related

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

to their prior misrepresentations and material omissions concerning F5's security capabilities and its forecasting processes and growth guidance.

74. In particular, on October 27, 2025, F5 announced significantly below-market growth expectations, announcing disappointing guidance for both the first quarter and full fiscal year 2026 due to the continued and downstream impacts of the Security Breach event.

Presumption of Reliance; Fraud-On-The-Market

75. At all relevant times, the market for F5's common stock was an efficient market for the following reasons, among others:

F5's common stock met the requirements for listing and was listed and actively traded on the NASDAQ during the Class Period, a highly efficient and automated market;

F5 communicated with public investors via established market communication mechanisms, including disseminations of press releases on the national circuits of major newswire services and other wide-ranging public disclosures, such as communications with the financial press and other similar reporting services;

F5 was followed by several securities analysts employed by major brokerage firms who wrote reports that were distributed to the sales force and certain customers of their respective brokerage firms during the Class Period. Each of these reports was publicly available and entered the public marketplace; and

Unexpected material news about F5 was reflected in and incorporated into the Company's stock price during the Class Period.

76. As a result of the foregoing, the market for F5's common stock promptly digested current information regarding the Company from all publicly available sources and reflected such information in F5's stock price. Under these circumstances, all purchasers of F5's common stock during the Class Period suffered similar injury through their purchase of F5's common stock at artificially inflated prices, and a presumption of reliance applies.

77. Alternatively, reliance need not be proven in this action because the action involves omissions and deficient disclosures. Positive proof of reliance is not a prerequisite to recovery

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

pursuant to ruling of the United States Supreme Court in *Affiliated Ute Citizens of Utah v. United States*, 406 U.S. 128 (1972). All that is necessary is that the facts withheld be material in the sense that a reasonable investor might have considered the omitted information important in deciding whether to buy or sell the subject security.

No Safe Harbor; Inapplicability of Bespeaks Caution Doctrine

78. The statutory safe harbor provided for forward-looking statements under certain circumstances does not apply to any of the material misrepresentations and omissions alleged in this Complaint. As alleged above, Defendants' liability stems from the fact that they provided investors with statements of confidence in its ability to meet the security needs of its clientele and claims of a continued climb in growth potential and opportunities for its security services while at the same time failing to provide the public with key information. Defendants provided the public with repeated claims of best-in-class security that failed to account for the existence or possibility of the Security Breach and/or adequately disclose the fact that the Company at the current time did not have adequate security infrastructure. Moreover, Defendants then, upon disclosure of the Security Breach, failed to articulate actual or potential continued impacts from the incident, including remediation efforts, potential lost clientele, and otherwise delayed revenue from elongated decision cycles as F5 endeavors to regain confidence from its customer base.

79. To the extent certain of the statements alleged to be misleading or inaccurate may be characterized as forward looking, they were not identified as "forward-looking statements" when made and there were no meaningful cautionary statements identifying important factors that could cause actual results to differ materially from those in the purportedly forward-looking statements.

80. Defendants are also liable for any false or misleading "forward-looking statements" pleaded because, at the time each "forward-looking statement" was made, the speaker knew the "forward-looking statement" was false or misleading and the "forward-looking statement" was authorized and/or approved by an executive officer of F5 who knew that the "forward-looking statement" was false. Alternatively, none of the historic or present-tense statements made by

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

Defendants were assumptions underlying or relating to any plan, projection, or statement of future economic performance, as they were not stated to be such assumptions underlying or relating to any projection or statement of future economic performance when made, nor were any of the projections or forecasts made by the defendants expressly related to or stated to be dependent on those historic or present-tense statements when made.

CLASS ACTION ALLEGATIONS

81. Plaintiff brings this action as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3) on behalf of a Class, consisting of all those who purchased or otherwise acquired F5's securities during the Class Period (the "Class"); and were damaged upon the revelation of the alleged corrective disclosure. Excluded from the Class are defendants herein, the officers and directors of the Company, at all relevant times, members of their immediate families and their legal representatives, heirs, successors or assigns and any entity in which defendants have or had a controlling interest.

82. The members of the Class are so numerous that joinder of all members is impracticable. Throughout the Class Period, F5's common stock were actively traded on the NASDAQ. While the exact number of Class members is unknown to Plaintiff at this time and can be ascertained only through appropriate discovery, Plaintiff believes that there are hundreds or thousands of members in the proposed Class. Record owners and other members of the Class may be identified from records maintained by F5 or its transfer agent and may be notified of the pendency of this action by mail, using the form of notice similar to that customarily used in securities class actions. As of July 30, 2025, there were 57.44 million shares of the Company's common stock outstanding. Upon information and belief, these shares are held by thousands, if not millions, of individuals located throughout the country and possibly the world. Joinder would be highly impracticable.

83. Plaintiff's claims are typical of the claims of the members of the Class as all members of the Class are similarly affected by Defendants' wrongful conduct in violation of federal law that is complained of herein.

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

84. Plaintiff will fairly and adequately protect the interests of the members of the Class and has retained counsel competent and experienced in class and securities litigation. Plaintiff has no interests antagonistic to or in conflict with those of the Class.

85. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual members of the Class. Among the questions of law and fact common to the Class are:

(a) whether the federal securities laws were violated by Defendants' acts as alleged herein;

(b) whether statements made by Defendants to the investing public during the Class Period misrepresented material facts about the business, operations and management of F5;

(c) whether the Individual Defendants caused F5 to issue false and misleading financial statements during the Class Period;

(d) whether Defendants acted knowingly or recklessly in issuing false and misleading financial statements;

(e) whether the prices of F5's common stock during the Class Period were artificially inflated because of the Defendants' conduct complained of herein; and

(f) whether the members of the Class have sustained damages and, if so, what is the proper measure of damages.

86. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in the management of this action as a class action.

COUNT I

Against All Defendants for Violations of

Section 10(b) and Rule 10b-5 Promulgated Thereunder

87. Plaintiff repeats and realleges each and every allegation contained above as if fully

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

set forth herein.

88. This Count is asserted against defendants and is based upon Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), and Rule 10b-5 promulgated thereunder by the SEC.

89. During the Class Period, Defendants engaged in a plan, scheme, conspiracy and course of conduct, pursuant to which they knowingly or recklessly engaged in acts, transactions, practices and courses of business which operated as a fraud and deceit upon Plaintiff and the other members of the Class; made various untrue statements of material facts and omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and employed devices, schemes and artifices to defraud in connection with the purchase and sale of securities. Such scheme was intended to, and, throughout the Class Period, did: (i) deceive the investing public, including Plaintiff and other Class members, as alleged herein; (ii) artificially inflate and maintain the market price of F5 common stock; and (iii) cause Plaintiff and other members of the Class to purchase or otherwise acquire F5's securities at artificially inflated prices. In furtherance of this unlawful scheme, plan and course of conduct, Defendants, and each of them, took the actions set forth herein.

90. Pursuant to the above plan, scheme, conspiracy and course of conduct, each of the defendants participated directly or indirectly in the preparation and/or issuance of the quarterly and annual reports, SEC filings, press releases and other statements and documents described above, including statements made to securities analysts and the media that were designed to influence the market for F5's securities. Such reports, filings, releases and statements were materially false and misleading in that they failed to disclose material adverse information and misrepresented the truth about the Company.

91. By virtue of their positions at the Company, Defendants had actual knowledge of the materially false and misleading statements and material omissions alleged herein and intended thereby to deceive Plaintiff and the other members of the Class, or, in the alternative, Defendants acted with reckless disregard for the truth in that they failed or refused to ascertain and disclose such facts as would reveal the materially false and misleading nature of the statements made,

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

although such facts were readily available to Defendants. Said acts and omissions of defendants were committed willfully or with reckless disregard for the truth. In addition, each defendant knew or recklessly disregarded that material facts were being misrepresented or omitted as described above.

92. Information showing that Defendants acted knowingly or with reckless disregard for the truth is peculiarly within defendants' knowledge and control. As the senior managers and/or directors of the Company, the Individual Defendants had knowledge of the details of F5's internal affairs.

93. The Individual Defendants are liable both directly and indirectly for the wrongs complained of herein. Because of their positions of control and authority, the Individual Defendants were able to and did, directly or indirectly, control the content of the statements of the Company. As officers and/or directors of a publicly-held company, the Individual Defendants had a duty to disseminate timely, accurate, and truthful information with respect to F5's businesses, operations, future financial condition and future prospects. As a result of the dissemination of the aforementioned false and misleading reports, releases and public statements, the market price of F5's common stock was artificially inflated throughout the Class Period. In ignorance of the adverse facts concerning the Company which were concealed by Defendants, Plaintiff and the other members of the Class purchased or otherwise acquired F5's common stock at artificially inflated prices and relied upon the price of the common stock, the integrity of the market for the common stock and/or upon statements disseminated by Defendants, and were damaged thereby.

94. During the Class Period, F5's common stock was traded on an active and efficient market. Plaintiff and the other members of the Class, relying on the materially false and misleading statements described herein, which the defendants made, issued or caused to be disseminated, or relying upon the integrity of the market, purchased or otherwise acquired shares of F5's common stock at prices artificially inflated by defendants' wrongful conduct. Had Plaintiff and the other members of the Class known the truth, they would not have purchased or otherwise acquired said common stock, or would not have purchased or otherwise acquired them at the inflated prices that

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

were paid. At the time of the purchases and/or acquisitions by Plaintiff and the Class, the true value of F5's common stock was substantially lower than the prices paid by Plaintiff and the other members of the Class. The market price of F5's common stock declined sharply upon public disclosure of the facts alleged herein to the injury of Plaintiff and Class members.

95. By reason of the conduct alleged herein, Defendants knowingly or recklessly, directly or indirectly, have violated Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder.

96. As a direct and proximate result of defendants' wrongful conduct, Plaintiff and the other members of the Class suffered damages in connection with their respective purchases, acquisitions and sales of the Company's common stock during the Class Period, upon the disclosure that the Company had been disseminating misrepresented financial statements to the investing public.

COUNT II

Against the Individual Defendants

for Violations of Section 20(a) of the Exchange Act

97. Plaintiff repeats and realleges each and every allegation contained in the foregoing paragraphs as if fully set forth herein.

98. During the Class Period, the Individual Defendants participated in the operation and management of the Company, and conducted and participated, directly and indirectly, in the conduct of the Company's business affairs. Because of their senior positions, they knew the adverse non-public information about F5's misstatements.

99. As officers and/or directors of a publicly owned company, the Individual Defendants had a duty to disseminate accurate and truthful information, and to correct promptly any public statements issued by F5 which had become materially false or misleading.

100. Because of their positions of control and authority as senior officers, the Individual Defendants were able to, and did, control the contents of the various reports, press releases and public filings which F5 disseminated in the marketplace during the Class Period concerning the

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

misrepresentations. Throughout the Class Period, the Individual Defendants exercised their power and authority to cause F5 to engage in the wrongful acts complained of herein. The Individual Defendants therefore, were "controlling persons" of the Company within the meaning of Section 20(a) of the Exchange Act. In this capacity, they participated in the unlawful conduct alleged which artificially inflated the market price of F5's common stock.

101. Each of the Individual Defendants, therefore, acted as a controlling person of the Company. By reason of their senior management positions and/or being directors of the Company, each of the Individual Defendants had the power to direct the actions of, and exercised the same to cause F5 to engage in the unlawful acts and conduct complained of herein. Each of the Individual Defendants exercised control over the general operations of the Company and possessed the power to control the specific activities which comprise the primary violations about which Plaintiff and the other members of the Class complain.

102. By reason of the above conduct, the Individual Defendants and/or F5 are liable pursuant to Section 20(a) of the Exchange Act for the violations committed by the Company.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment against defendants as follows:

A. Determining that the instant action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, and certifying Plaintiff as the Class representatives;

B. Requiring Defendants to pay damages sustained by Plaintiff and the Class by reason of the acts and transactions alleged herein;

C. Awarding Plaintiff and the other members of the Class pre-judgment and post-judgment interest, as well as their reasonable attorneys' fees, expert fees and other costs; and

D. Awarding such other and further relief as this Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff hereby demands a trial by jury.

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480

DATED: December 19, 2025

Respectfully submitted,

TOWNSEND LEGAL, PLLC

/s/ *Roger M. Townsend*
Roger M. Townsend
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110
Tel: 206-761-2480
Roger@townsendlegal.com

-and-

LEVI & KORSINSKY, LLP
Adam M. Apton (pro hac vice forthcoming)
33 Whitehall Street, 27th Floor
New York, New York 10004
Tel.: (212) 363-7500
Fax: (212) 363-7171
Email: aapton@zlk.com

Attorneys for Plaintiff

TOWNSEND LEGAL, PLLC
380 Winslow Way, Suite 200
Bainbridge Island, WA 98110 Tel: 206-761-2480