NASDAQ:ARQQ Q2 2026 Earnings Call Transcript

Generated on 11/25/2026

Jonathan | Conference Operator:

On today's call, we will be referring to the press release issued this morning that details the company's first half of fiscal year 2026 results, which can be downloaded from the company's website at architgroup.com. At the end of the company's prepared remarks, there will be a question and answer period for selected equity research analysts. Please note that those selected Equity research analysts that would like to ask a question in the Q&A section will need to dial into the call rather than joining through the webcast link. Finally, a recording of the call will be available on the investor section of the company's website later today. Please note that this webcast includes forward-looking statements. statements about the company's beliefs and expectations containing words such as will could believe expect anticipate and similar expressions are forward-looking statements and are based on assumptions and beliefs as of today the company encourages you to review the safe harbor statements risk factors, and other disclaimers contained in today's press release, as well as the company's filings with the Securities and Exchange Commission, which identify specific risk factors that may cause actual results or events to differ materially from those described in our forward-looking statements. The company does not undertake to publicly update or revise any forward-looking statements after this webcast. And now I'd like to turn the call over to Andy Lieber, the company's chief executive officer. Andy.

Andy Lieber | Chief Executive Officer:

Thank you. And thank you for joining our first half of fiscal year 2026 earnings call. When we spoke in December, reflecting on fiscal year 2025, I said that 2025 had been a year of momentum in the realization of the need for enhanced cybersecurity to address the coming threat to data security posed by quantum computers at scale. Governments were taking their concerns public, some mandating roadmaps to enhance cryptographic postures for governmental agencies and encouraging enterprises to take action as well. I noted that from Archit's conversations with governments and enterprises, it was no longer a question of if organizations need to upgrade their cryptographic security posture, but when they will upgrade their posture. What has become clear in the first half of our current fiscal year is that when is becoming now. While that is my view based on our deep understanding of the threat, let me cite the view of some leading players in the quantum and security space. Google has been aligned with the U.S. National Institute for Standards and Technology, or NIST, timeline for migration to post quantum cryptography, which calls for the deprecation, meaning the market of removal of unsafe cryptography by 2030 and complete disallowance by 2035. On March 25th, Google advised that cryptographic systems migrate by 2029. Google's accelerated timeline was the result of research which it published that demonstrated quantum computers will be able to break elliptical curve cryptography, the kind of cryptography that protects things like crypto wallets, with 20 times fewer qubits engaged than previously projected. That moves the timescale from 2035 to by 2029. That is a serious migration timeline compression. Also, CloudFlare, on April 7th, It pulled forward its advice to migrate by 2029 as well. Cloudflare's revision was based on Google's published research, but also research published by Oratomic on March 30th. Oratomic concluded that by leveraging advances in high-rate quantum error-correcting codes, efficient logical instruction sets, and circuit design, Shor's algorithm can be executed at cryptographically relevant scales with as few as 10,000 reconfigurable atomic qubits. That is a shockingly low estimate of the computational resources needed to crack RSA. And finally, IonQ, on its May the 6th earnings call, CEO Nicola De Masi stated, based on our public roadmap, we expect to achieve the logical cubic count required to challenge RSA 2048 encryption and the 2028 to 2029 window. If IonQ is correct, migration to a post-quantum security posture by 2029 may be too late. The urgency to migrate to post-quantum cryptography is heightened by two factors. Firstly, protecting your existing data against

harvest-now, decrypt-later attacks. Any data that is stolen today, even if protected with current encryption technology, is vulnerable to exposure when a quantum computer sets to work on it at a later date. Any data that is sensitive or has a shelf life should be secured with post-quantum encryption now. Secondly, migrating to post-quantum cryptography involves analysis, planning, and execution across the entire data and communication architecture of an organization, which requires time. If Google, Cloudflare, and IMQ are correct, and we think they are, then time is of the essence. ArcX product set is well positioned to enable an end-to-end migration to a post-quantum cryptographic security posture. from assessing the current risk inherent in an organization's network architecture to implementing software-based post-quantum cryptographic solutions, which are compliant with NIST and NSA standards. Our encryption intelligence risk analysis tool gives organizations complete visibility into all encryption technologies and use across the network, automatically identifying weak points and vulnerabilities, including those susceptible to quantum attacks. This is a critical step in developing a migration strategy. Understanding what encryption is in use, where and what it is protecting allows CISOs and CTOs to scope their risk and develop a game plan to upgrade to post-quantum cryptography. Our software-based post-quantum encryption solutions allow organizations to upgrade now, protecting against harvest now, decrypt later attacks, and when quantum computers arrive at scale. Our solutions are cryptographically agile, which gives CTOs and CTOs flexibility to mix and match PQAs, that's post-quantum algorithms, and symmetric key cryptography. Being software-based and lightweight, our encryption solutions can be flexibly deployed at any level of a network architecture, from servers down to small edge devices. No new hardware devices are required, and it can be implemented quickly. We've completed deployments in as few as a couple of days. So leading industry players are now saying the time for post-quantum cryptography is here, arguably saying we have the products to meet that need. Where do we stand in capturing growing market demand for post-quantum migration? We acquired our encryption intelligence product in 2025 and announced commercial rollouts in January of this year. We are actively directly marketing the solution to end customers. A marketing campaign targeting approximately 450 organizations is in process, and engagement to date has been strong. On May 18th, ArcGIS executed its first encryption intelligence contract supporting PQC migration planning. On May 19th, ArcGIS signed its first partnership agreement with a European specialist cybersecurity provider for ArcGIS encryption intelligence solution. Feedback about encryption intelligence products has been favorable and the breadth of prospective customer engagement has been highly encouraging. The product delivers high utility for organizations, giving deep network encryption visibility and risk assessment a critical first step for CISOs and CTOs on their PQC migration journey. Based on the pipeline of sales opportunities, we expect additional contract wins during the balance of the fiscal year. Our software-based encryption solutions, led by a network-secure product, is gaining traction. Sparkle, a tier one Italian network operator, licensed our product to create a quantum secure network as a service. It is seen take up of its offering, most notably with a financial institution. This is important for several reasons. One, it demonstrates the efficacy of our encryption in a real world use case, securing critical data and communication in transit. Two, it demonstrates the applicability of our cryptographic solutions for the financial service industry, which we believe is a significant market opportunity. And three, and finally take up of Sparkle's network as a service offering means consumption of its volume defined license with ARCHIT. We wish Sparkle much success and would welcome Sparkle's need to upsize its license. And we expect that to be the case as Sparkle just yesterday announced the commercial availability of its QuantumSafe interconnect, which is secured by ARCHIT across 20 Equinix International Business Exchange data centers in Europe, the Americas, and Asia, where Equinix managed solutions are offered. Sparkle's QuantumSafe internet is now available to enterprises, carriers, and hyperscalers seeking QuantumSafe protection for their cross-site VPNs, hybrid infrastructures, and distributed multi-client environments. Sparkle indicated that it expects to expand the offering across the broader Equinix ecosystem. To paraphrase Joe Crawford, VP of Equinix Managed Service, it is innovative, quote, integration of next-generation security directly into the environment where dense ecosystem of customers build and scale their digital infrastructure. This is an exciting development for Sparkle and Archive. In regards to other telecom network operators, recently ARCIT teamed with ARCIT, excuse me, Colt Technology to deliver a quantum secure wide area network to help protect ANK Travel Group from the future risks presented by quantum computers, including the threat presented by Harvest Now Decrypt Lato. ANK owns a portfolio of premier travel brands, including Abercrombie & Kent, Crystal, and Cox & King's. ANK's

brands provide travel adventures in more than 100 countries across the world and rely on a secure global network to keep customers, employees, and travel partners connected. Colton Arcade will now keep ANK travel group customers and the customers' data and communications protected from the quantum threat. Large telecommunications networks are a significant opportunity for our encryption solutions, and we're engaged in late-stage dialogue and demonstrations with several, including one in the U.S., However, our encryption solutions are broadly applicable beyond T1 telecommunications networks. The lightweight software nature of our product allows deployment of all layers of a network and almost any device, regardless of size or power. Our solution is also crypto-agile in that it can be mixed and matched with other cryptographic modalities, including post-quantum algorithms. The flexibility of our software encryption solutions has been manifest in our activities with defense organizations. Implementations range from a defence contractor securing communications of a government defence research network to a defence contractor securing tactical control of drone platforms for a European Ministry of Defence, from large networks to small devices. It takes time to win contracts in the government and defence space. That said, we are making tangible process. We believe a renewal and upsizing of our largest US defence-related contract is imminent, further establishing a track record which we can build upon. Also on May 1st, a partner, which is the leading technology and innovation solution provider to the aerospace and defense industry, renewed and upsized its contract with ARCIT by almost 90%. Together, we bid in contract to opportunities to military organizations with a heavy emphasis on Europe. Our opportunity set in the government and defense markets is the strongest it has ever been. The breadth of demonstration and bid activity is significant. We expect further progress in this key target market and expect to see further results in the second half of the fiscal year. We continue to grow our go-to-market partnerships. During the first half of the fiscal year and more recently, we've added three new partnerships to grow our opportunities in the telecommunications market, and just this week signed our first partnership agreement for ArcGIS Encryption Intelligence Solution. Specifically, we announced. a strategic collaboration with Six Wind to deliver highly scalable, quantum-safe encrypted virtual private network or VPN business services. Six Wind products enable telecom service providers and enterprises to build and manage efficient, scalable, secure, and sustainable networks. Secondly, a strategic collaboration with RAD to deliver a joint quantum-safe encryption solution for telcos, enabling them to offer quantum-safe business services such as site-to-site and site-to-cloud VPNs, as well as data center interconnect or DCI. RAD is a global leader in networking edge solutions. Further, ArcGIS was selected to join the Temoratory portfolio as a scale-up partner. A joint venture between Vodafone Group and Technoport, Luxembourg's national tech incubator, Tomorrow Street's ecosystem brings together innovative young companies and scales their technology solutions across Vodafone's global ecosystem. ARKIT is the first quantum security company to join the portfolio. And finally, on May 19th, ARKIT signed a partnership agreement with the European Specialist Cybersecurity Provider for ARKIT's encryption intelligence products. Our product will be the cornerstone of strategic PQC migration activities within financial services. Go-to-market partnerships drive product awareness and are an important source for lead and bid generation. They are a force multiplier for our kit. We expect to see revenue opportunities come through these partnerships. From my vantage point, the important vectors for success are convergent. Those vectors are market need, the right products, and customer traction. The need to migrate to a post-quantum cryptographic security posture has significantly increased with rapid advancement in quantum computing. Leading industry players are now sounding the alarm. We are no longer the modest voice raising awareness. Big industry voices are in full cry. We have the right products to enable CISOs and CTOs to understand their current cryptographic security posture and upgrade to quantum safe encryption. We are seeing product take up in our key markets of telecommunications and government and defense. Circling back to my remarks from our fiscal year and 2025 earnings call, the key message was that the momentum was building in the market and for the company in 2025. The first half of fiscal year 2026 has seen a continuation and amplification of momentum. We're excited about the building demand for post-quantum cryptography, and we believe in the products and solutions which we offer. With continued focus and hard work, I expect our up and to the right momentum to continue. With that, let me turn the call over to Nick Poynton. Thank you, Nick.

Nick Poynton | Chief Financial Officer (Outgoing):

Thank you, Andy. For the first half of fiscal year 2026, Arquette generated $623,000 in revenue, as compared to $67,000 in revenue for the similar period in fiscal year 2025. The variance between periods resulted from revenue under a contract with a customer in the Middle East that met late in the first half of fiscal year 2025 and revenue under 11 contracts in the period versus six in the first half of fiscal year 2025. Revenue for the period represents the second consecutive reporting period of growth. With a small data set, it gives credence to Andy's comments when we reported in fiscal year 2025 results that our revenue had troughed as of March 2025 and our expectation is for growth going forward. As I noted, we executed under 11 contracts in the period. For comparison, We executed under seven for fiscal year 2025. Two of the 11 contracts have or are expected to imminently renew and be upsized. Three of our 11 contracts were in the telecom sector and eight for government, defence and enterprise organisations. Our administrative expenses equate to operating costs for those more familiar with US GAAP. Administrative expenses for the first half of fiscal year 2026 rose from $20.2 million for the six months ended 31st March 2025 to $33.9 million for the six months ended 31st March 2026. The variance between periods resulted from an increase in employee-related costs and share-based compensation stemming from a higher headcount during the period, partially offset by a decrease in property costs as a result of the termination of ARCET's previous office lease arrangements and a decrease in foreign exchange expenses. Administrative expenses for the period includes a $12.7 million non-cash charge associated with share-based compensation versus an $800,000 to $2,000 charge for the comparable period in 2025. Operating loss for the period was $33.7 million versus a loss of $20 million for the first half of fiscal year 2025. The variance in operating loss between periods primarily reflects high revenue more than offset by an increase in administrative expenses for the period. For the period, loss before tax from continuing operations was $33.1 million. For the first half of fiscal year 2025, loss before tax from continuing operations was $19.5 million. The variance between periods is primarily due to increased administrative expenses and a lower finance income. As of 31 March, the company had cash and cash equivalents of $28.9 million. However, our cash balance as of 20th of May was $35.9 million. In addition, there are in-the-money warrants outstanding with an exercise expiration of September 2026, which we expect will exercise and provide approximately $13.5 million of additional liquidity to the company. On a personal note, this is my last earnings call with Arquette. as I will be stepping down as CFO at the end of the month. It has been my pleasure working with the ArcIT team for the past five years and building the business, which I believe has a bright future. Rob Russell will be stepping into the CFO role. Rob is a seasoned finance executive with deep expertise spanning investment banking, private equity, and SaaS scale-ups, and more recently served as Chief Financial and Operating Officer at VirtualStock, where he played a central role in the company's successful exit in 2025. Rob began full-time as CFO on May 1st, following two months working part-time to ensure continuity ahead of assuming the CFO role. I'm confident that this measured transition leaves the company's financial stewardship in excellent hands. With that, I will hand the call back to Andy.

Andy Lieber | Chief Executive Officer:

Thank you, Nick. On behalf of the company and board, I would like to thank you for your service. You've been instrumental in building the infrastructure which every company needs to operate and succeed. It's largely the behind-the-scenes work which is critical and efficient to creating a successful organization. We wish you well in your future endeavors. Thank you again. And now I'll hand the call back to the operator for Q&A.

Jonathan | Conference Operator:

Certainly. Ladies and gentlemen, if you do have a question at this time, please press star 1-1 on your telephone. If your question has been answered and you'd like to remove yourself from the queue, simply press star 1-1 again. And our first question comes from the line of Troy Jensen from Cantor Fitzgerald. Your question, please.

Troy Jensen | Equity Research Analyst, Cantor Fitzgerald:

Hey, gentlemen, congrats on all the momentum. Maybe start off here with the one for Andy. I'd just be curious your thoughts on the sense of urgency around kind of Q Day and just, you know, relating that to the slowness that it seems that we've seen on the adoption currently. So any thoughts would be helpful.

Andy Lieber | Chief Executive Officer:

Yeah. Hey, thanks, Troy, and thanks for joining the call. Appreciate the question. So I think as I mentioned in my opening comments, we are seeing obviously some of the very big players in the markets are notably Google, Cloudflare are all pulling forward their predictions of cryptographically relevant quantum computers becoming available. And likewise, at the same time, we've seen the estimate of the number of qubits required to break Shor's algorithm is coming down also at the same time. Hence the revision of those timelines coming forward. I think what's really interesting is today, which literally has happened just before our earnings call, is we've seen people like the Wall Street Journal and others reporting that the U.S. government is taking an active interest in investment into quantum companies. If rumors are believed, it's kind of in the region of $2 billion. To me, I see that as... you know, are we now looking at quantum computing being almost like national infrastructure and the strategic importance of that, and at the same time, aligning that with the needs for organizations, be they defense, public sector, or commercial, to actually be ready for the long-talked-about Q Day, which looks like it's getting closer and closer. I believe now, and you'll see from our encryption intelligence tool, we now have the ability to quantify where are your weaknesses, what are the threats, and what do you need to do urgently to really remedy some of that, but also lay out a timeline to move to a full quantum secure landscape in an organization. I think right now, I liken it a little bit to the original build out of the internet. So you're seeing a lot of the infrastructure providers. So we just talked about people like Equinix, infrastructure provider, telcos, which are providing the cabling. The ground up security, quantum security of infrastructure is happening. And at the same time, Defense regulated industries and also IP rich industries are also leaning into this thinking that they need to get going. So as I said in my comments, I really feel like last year was the year of quantum. This is the year of quantum security. It actually does feel like the year of quantum security.

Troy Jensen | Equity Research Analyst, Cantor Fitzgerald:

Yeah, interesting. I agree with you on the sense of urgency, and it just feels like we need to have, you know, inflection in some point, right, for all these governments and, you know, telcos and corporations are going to get, you know, kind of quantum ready. But what are your thoughts on, like, the milestones then or the catalysts that we need to walk to investors in the near term here?

Andy Lieber | Chief Executive Officer:

If you just repeat the last bit, I missed the very last bit of the question. Sure.

Troy Jensen | Equity Research Analyst, Cantor Fitzgerald:

Yeah, the milestones that we need to kind of watch to really see, you know, when this catalyst, when this inflection is going to come in the near term. I mean, I'm assuming it's just the technical milestones that need to happen from the quantum companies, but your thoughts on kind of the next catalyst for you guys.

Andy Lieber | Chief Executive Officer:

Yeah, I think just to comment on the quantum availability side, you know, I don't believe that there's going to be a day where somebody says, hey, we've broken short. We've used Shor's algorithm with broken existing encryption. That could be any time in the next two years, according to what CloudFlare and Google are talking about, or kind of in that timeframe. I think for us, it's this recognition. I think a lot of people thought for a while, hey, this is like just moving to a new form of encryption, and hey, we just kind of move on. You think about the previous way that we're securing things with certificates. It was built for a different age. It was built for a very different level of compute power, memory, storage, et cetera. And I don't think people quite understand that it's a bigger job, especially with the amount of data that's machine generated now. So that's why we made a thing talking there about all the way from center to the edge. You think about how many edge devices there are now which are producing masses of data. I think for us, when we use encryption intelligence to say, where do you start and how do you ensure that you are safe on the perimeter working into the core? And then how do you allow to plan to make sure you can migrate the whole organization? You know, I'm not sat here now saying, you know, is my local supermarket worried about being quantum safe? They will be eventually. But I think that urgency is definitely, like I said, in the more defense, public sector, infrastructure providers, those are the ones that are feeling it today and feeling kind of the need to get on top of it.

Troy Jensen | Equity Research Analyst, Cantor Fitzgerald:

Makes sense. And then one other question, or it's probably a multi-point question, just on finances here. So the warrants that you just talked about, 30 million you'll raise, just what's the share count that's going to come with that? Are there other warrants outstanding? And can you just talk about your cash position and the cash burn would be awesome to hear.

Andy Lieber | Chief Executive Officer:

Well, let me turn to Nick first to start that question. I'm sure Rob's got some thoughts on that as well.

Nick Poynton | Chief Financial Officer (Outgoing):

So I think I'll just hand over the cash part of that answer to Rob while we look at the warrants.

Rob Russell | Chief Financial Officer:

Great. Thanks, Nick. And thanks for the question, Troy. So as Nick said earlier, we closed the half year with $29 million of cash in the bank. Today we have in excess of $35 million. That translates to more than 14 months of runway. And then add on top of that, the $13.5 million worth of warrants, which you've mentioned that heavily in the money, and they expire in September, so before the fiscal year end. So what does all of that translate to? We feel very comfortable with our cash position. We believe it gives us more than enough cash to meet our commercial objectives, especially in a market that we believe is moving towards us for the reasons that Andy's outlined.

Troy Jensen | Equity Research Analyst, Cantor Fitzgerald:

Very fair. All right. Well, good luck, gentlemen. Just real quick. I missed the warrants. Yeah, thank you.

Nick Poynton | Chief Financial Officer (Outgoing):

Shall I just jump in? So on the warrants expiring in September 24, that equates to 5.4 million shares, according to the table. Okay. Any other outstanding... There are rather outstanding warrants. I think these are covered in the 20F in some detail and expire over the next two further years. The last one's expiring in September 28th. Okay.

Jonathan | Conference Operator:

All right. Good luck, guys. Thanks, Troy. Thank you. And as a reminder, ladies and gentlemen, if you do have a question at this time, please press star 11 on your telephone. And this does conclude the question and answer session of today's program. I'd like to hand the program back to Andy Lever for any further remarks.

Andy Lieber | Chief Executive Officer:

Hey, thank you, Jonathan. And again, thank you, everybody on the call for joining us today. Or if you're listening on replay, we look forward to speaking with you again following the close of our 2026 fiscal year. Thank you.

Jonathan | Conference Operator:

Thank you, ladies and gentlemen, for your participation in today's conference. This does conclude the program. You may now disconnect. Good day.