eMemory 2Q25 Earnings Call Transcript

August 15th, 2025, 16:00-17:00 Taiwan Time

OPENING REMARKS

Dr. Charles Hsu, Chairman

Good afternoon, everyone. Thank you for joining our earnings call. One of the key questions we hear from investors is about our position in AI—why it isn't more visible today, and will we have a place in the future?

Let's take the smartphone market as an example. Our IP is often introduced starting from the second or even much later generation of a chip's development. Over time, as more customers adopt our technology for similar chips, the scope of applications expands. Even today, as smartphone process nodes continue to advance, we are still introducing our solutions into new application chips.

In the HPC and AI domains, we will replicate this proven model. So far, we have been designed into chips covering CPUs, AI accelerators, DPUs, Smart NICs, SSD controllers, BMCs, PMICs and more to come. As of Q2 this year, we have achieved over 110 tape-outs related to PUF technology. In the second quarter, we began to see royalty contributions from mass production by a major Taiwanese networking company, and we expect more significant moving forward.

At the same time, to prepare for the AI-driven transformation of our industry, we are implementing the largest operational reform since our founding — laying the foundation for the next 10 years and beyond. Our operational efficiency will improve substantially, and we believe the results will be worth the wait.

We are grateful to the colleagues who have built the strong foundation of the company since its inception, and we are also committed to ensuring a smooth transition and succession to meet the opportunities and challenges of AI-driven industry change—this is the core spirit of this year's reform.

Next, I'd like to introduce our new CFO, Joseph Hsia, who will walk you through the Q2 financials. Joseph holds an MBA from Yale, and is both a CFA and CPA charterholder. He previously worked at BCG, where he led operational improvement projects for several leading technology companies. Joseph, please.

FINANCIAL RESULTS

Joseph Hsia, Financial Officer

Q2 2025 Financial Results

Good afternoon, everyone. Now, let's begin with our 2025 second-quarter financial results.

The second-quarter revenue was nine hundred and thirty-seven million NT dollars (NT$ 937 mil), up 2.7% sequentially and up 4.9% year-over-year. Revenue in U.S. dollars was thirty million (US$ 30 mil), representing a 7.1% increase from the previous quarter and a 7.3% increase year-over-year.

Operating expenses were three hundred and ninety-one million NT dollars (NT$ 391 mil), up 0.3% sequentially but down 1.8% year-over-year.

Operating income was five hundred and forty-six million NT dollars (NT$ 546 mil), with an increase of 4.5% sequentially and an increase of 10.2% year-over-year.

Operating margin increased by 1 percentage point sequentially and increased by 2.8 percentage points year-over-year to 58.3%. Impacted by a foreign exchange loss of ninety million NT dollars (NT$ 90 million) this quarter, our net income totaled four hundred million NT dollars (NT$ 400 mil), experienced a decrease of 13.4% sequentially and a decrease of 15.8% year-over-year.

EPS for this quarter was 5.36 NT dollars (NT$ 5.36).

Revenue across Different Streams

Next, let's move on to revenue contributions by licensing and royalty.

Licensing in the second-quarter accounted for 34% of the total revenue, up 32.4% sequentially and up 6.1% year-over-year. In U.S. dollar terms, this represents a sequential increase of 39.8% and a year-over-year increase of 10%.

Royalties in the second-quarter contributed 66% of the total revenue, decreasing 7.9% sequentially but increasing 4.3% year-over-year. In U.S. dollar terms, this represents a sequential decrease of 4.6% but a year-over-year increase of 5.9%.

Total revenue for the second-quarter increased by 2.7% compared to the previous quarter and increased by 4.9% compared to the previous year. In U.S. dollar terms, total revenue rose 7.1% sequentially and 7.3% year-over-year.

For the first half of 2025, the licensing and royalty revenues are as follows:

Licensing in the first half accounted for 30.2% of the total revenue, up 5.7% year-over-year. In U.S. dollar terms, licensing revenue grew 5.9% year-over-year.

Royalties in the first half contributed 69.8% of the total revenue, increasing 10.5% year-over-year. In U.S. dollar terms, royalty revenue increased 8.4% year-over-year.

Total revenue for the first half increased by 9% compared to the previous year. In U.S. dollar terms, total revenue grew 7.6% year-over-year.

Revenue by Technology

With that, I will comment on our revenue contribution by specific IPs.

NeoBit accounted for 18.8% of total licensing revenue in the second-quarter, increasing 5.6% sequentially but decreasing 18.6% year-over-year. In U.S. dollar terms, its licensing revenue increasing 10.6% sequentially but decreasing 16.5% year-over-year. Royalty from NeoBit accounted for 26.4% of total royalty, down 4.3% sequentially but increasing 3.3% year-over-year. In U.S. dollar terms, its royalties down 1.9% sequentially but up 3.9% year-over-year.

NeoFuse accounted for 39.4% of total licensing revenue in the second-quarter, up 6.3% sequentially and up 25.5% year-over-year, or, in U.S. dollar terms, rising 12.1% sequentially and 29.8% year-over-year. In terms of total royalty revenue, NeoFuse royalties decreased by 10.3% sequentially but increased by 4.1% year-over-year, accounting for 70.5% of total royalties. In U.S. dollar terms, royalties fell 6.8% sequentially but increased 6.2% year-over-year.

PUF-Based Security IPs contributed 14.7% of licensing revenue, increasing 176.3% sequentially and increasing 24.7% year-over-year. In U.S. dollar terms, this represents an increase of 199.0% sequentially and 32.4% year-over-year. Its royalties accounted for less than 1% of total royalties, down 5% from the previous quarter but up 238% from the prior year. In U.S. dollar terms, royalties were flat sequentially but surged 216.7% year-over-year.

MTP technology accounted for 27.1% of total licensing revenue, increasing 77% sequentially but decreasing 3.1% year-over-year. In U.S. dollar terms, licensing revenue grew 86.2% quarter-over-quarter and edged up 0.1% year-over-year. Royalty from MTP accounted for 3% of total royalties, up 30.4% sequentially and increased by 15% year-over-year, or, in U.S. dollar terms, up 34.4% sequentially and 16.2% year-over-year.

For the first half of 2025, the revenues by technology are as follows:

NeoBit licensing revenue decreased by 3.9% but royalty increased by 11.3% year-over-year, accounting for 24.4% of the total revenue. In U.S. dollar terms, licensing revenue decreased by 4.6% but royalty increased by 8.6% year-over-year.

NeoFuse licensing revenue increased by 10.7% and royalty increased by 10.2% year-over-year, contributing to 63% of the total revenue. In U.S. dollar terms, licensing revenue increased by 10.1% and royalty increased by 8.3% year-over-year.

PUF-based security IP licensing revenue increased by 14.2% and royalty increased by 346.5% year-over-year, accounting for 3.5% of the total revenue. In U.S. dollar terms, licensing revenue increased by 17.7% and royalty increased by 322.2%year-over-year.

MTP technology licensing revenue increased by 2.7% year-over-year and royalty revenue increased by 7.2%, accounting for 9.1% of total revenue. In U.S. dollar terms, licensing revenue increased by 3.3% and royalty increased by 5.4% year-over-year.

Royalty Revenue by Wafer Size

Now, let's look at royalties for 8-inch and 12-inch wafers.

8-inch wafers accounted for 40% of royalties, down 13.4% sequentially and down 2% year-over-year.

12-inch wafers contributed 60% of royalties, down 3.8% sequentially but up 8.8% year-over-year.

In total, 160 product tape outs were completed in the second-quarter. We will provide more information in the management report.

Next, I'll invite our president, Michael Ho, to share our future outlook.

FUTURE OUTLOOK

Michael Ho, President

Good afternoon, everyone. In the following section, I will address our future outlook.

Regarding licensing revenue: We anticipate that licensing revenue will continue its growing momentum due to very strong demand from both foundries and fabless customers for our IPs.

As for royalty revenue: We expect royalty revenue to continue its growth trend as the accumulated tape outs in the pipeline that are moving into production. Particularly, we have started receiving PUF royalties which will accelerate our royalties growth momentum in the future.

For New IP technologies:

1. Our new Post-Quantum Cryptography has been fully developed and certified under NIST's CAVP program, covering the published FIPS 203 (ML-KEM) and FIPS 204 (ML-DSA) standards. This marks the official launch of our full-stack PUF_{PQC} architecture.
2. On TSMC's N3P process, our NeoFuse OTP, NeoPUF, and PUF-based Root of Trust have been qualified, enabling secure PUF-based solutions for advanced AI, HPC chips, and chiplet designs. We're also advancing development on N3C and N3A processes to serve value-tier products and automotive applications.
3. In partnership with leading foundries, we are advancing the development of 2nm technologies.

This concludes my comments. Next, I will pass the time to Charles.

CHAIRMAN REMARKS

Dr. Charles Hsu, Chairman

(Page 14: Chiplet Supply Chain Secured by NeoPUF)

Today, I'd like to walk you through how PUF technology can secure the chiplet supply chain from end to end. As we know, the shift toward chiplet-based architectures has brought many benefits — greater flexibility, modularity, and performance optimization. But it has also introduced new security challenges, because chiplets may be designed, fabricated, and integrated across different vendors and geographies. This creates multiple attack surfaces throughout the supply chain. By embedding Physical Unclonable Function, or PUF technology, directly into each chiplet, we can establish a hardware-based root of trust that protects against threats from design to deployment.

(Page 15: Security Challenges in Chiplet)

Let's first look at the types of security challenges chiplets face. These fall broadly into two categories.

The first category is Supply Chain Security. This includes IP piracy, where proprietary chip designs can be stolen and illegally replicated. There's also the threat of malicious parts — sometimes referred to as 'Trojan' chiplets — which may be inserted during manufacturing and could compromise the entire system. And finally, counterfeit parts, where unauthorized chiplets are introduced into the supply chain, potentially undermining reliability and security.

The second category is Authentication between Chiplets. In a multi-vendor environment, primary components such as cores or accelerators, enabling components like I/O modules, and supportive components such as memory must all be verified to ensure they are genuine and trustworthy. Without strong authentication, malicious or incompatible chiplets could be integrated into the system, compromising performance or security."

(Page 16: NeoPUF for Supply Chain Security)

NeoPUF addresses these supply chain challenges across all three stages of the chiplet lifecycle.

In the design stage, the main risk is IP piracy. Traditionally, hardware unique keys (HUKs) require manual handling, which is vulnerable to leakage. NeoPUF eliminates this risk with its inborn HUKs, removing the need for external key injection.

In the fabrication and packaging stage, one concern is malicious parts being inserted. Here, NeoPUF ensures each chiplet carries its own unique ID, enabling traceability for device management throughout manufacturing.

In the deployment stage, counterfeit parts may attempt to infiltrate the network. NeoPUF can be used to generate cryptographic keys and certificates to authenticate components and maintain supply chain integrity. This end-to-end approach allows us to track and verify every chiplet throughout its lifecycle.

(Page 17: Authentication between Chiplets)

When we talk about chiplet security, it's not just about the supply chain. Each chiplet also needs its own safeguards to protect the way it communicates with the rest of the system. The level of security depends on what that chiplet actually does.

For supportive components, like memory dies, basic security is enough. They don't perform computation, but they still need to be verified by the CPU or accelerator. Basic security is achieved by a hardware root of trust with anti-tampering and secure storage, plus simple one-way symmetric authentication.

Enabling components, such as I/O dies, play a bigger role. They are essential for system operation and interact with other chiplets all the time. To increase to moderate security, unique ID and true random number generator are added, while still using one-way symmetric authentication.

Finally, primary components, such as CPUs and accelerators, act as the brains and engines of the system. These demand the highest level of security: the full set of hardware root of trust functions, and two-way asymmetric authentication to ensure both sides verify each other.

Overall, by matching each chiplet's role with the right level of protection, we can keep the system secure — without adding extra complexity where it is unnecessary.

(Page 18: NeoPUF-based Solutions for Chiplet Security)

This slide shows how NeoPUF-based Solutions come together to secure die-to-die communication in a chiplet system.

At the top right, we have the Memory Die and Control Die. Both store their keys and certificates securely in Secure OTP and use HMAC for one-way symmetric authentication.

The Core Die, which is high value and central to the system, integrates PUFcc for two-way asymmetric authentication and cryptographic operations, establishing a strong hardware root of trust.

The Accelerator Die and I/O Die use PUFrt to provide unique IDs and keys, along with HMAC for session-based authentication. This ensures they can be validated quickly and securely before exchanging data with the core.

By combining HMAC for lightweight authentication, Secure OTP for secure storage, PUFrt for hardware root of trust, and PUFcc for advanced cryptography, NeoPUF delivers a comprehensive, layered defense — securing each chiplet individually, and the entire package collectively.

To summarize — the adoption of chiplets changes the security landscape by introducing new risks at every stage of the lifecycle and at every interface between components. NeoPUF offers a silicon-native, unclonable identity for each chiplet, enabling us to secure the supply chain and authenticate die-to-die communication. By tailoring the security solution to each chiplet's role, we can maintain both security and performance — ensuring that chiplet-based systems remain trustworthy from design to deployment.

This is what I would like to share with you today. Thank you.

Next, we will enter the QA session.

CLOSING REMARKS

Dr. Charles Hsu, Chairman

For more information about our PUF-based security IPs and technology, we encourage you to visit our PUFsecurity website at https://www.pufsecurity.com/ and check out our articles and other materials.

Thank you once again for your patience and support for eMemory. We will continue to work hard on technology and IP innovation and PUF-based hardware security solutions for our customers and bring higher returns for our shareholders. Thank you!