Applicant: Synthro Inc.
U.S. Application Serial No. 88468735
Mark: FOAM

The examining attorney has refused registration on the Principal Register because the examining attorney believes the mark is confusingly similar to NEURAL FOAM (U.S. Registration No. 4291132). In support of the refusal, the examining attorney has submitted the following evidence (1) the similarities between the compared marks and (2) the relatedness of the compared goods and services. The examining attorney stated that the applicant may present arguments in support of registration by addressing the issue of potential conflict between the applied-for mark and the above referenced mark. Applicant believes that the examining attorney has failed to make a *prima facie* showing of likelihood of confusion.

Similarities between the marks

The examining attorney argues that applicant's mark does not create a distinct commercial impression from the registered mark because it contains some of the wording in the registered mark and does not add any wording that would distinguish it from the registered mark. Applicant agrees that the applicant's mark contains the word FOAM just as the mark NEURAL FOAM.

However, the NEURAL FOAM mark contains the word NEURAL which alone distinguishes it from the applicant's mark. The term NEURAL, in the context of computing, is often used in connection with networks and is defined as a "computer model designed to simulate the behavior of biological neural networks, as in pattern recognition, language processing, and problem solving, with the goal of self-directed information processing". Neural computation. (n.d.) *Random House Kernerman Webster's College Dictionary*. (2010). Retrieved September 20 2019 from https://www.thefreedictionary.com/Neural+computation.

The word "neural", and its derivatives, is commonly used by other products and services to indicate products related to artificial intelligence or machine-learning technology. See Attachment 1.

As such, any reasonable consumer would understand that the NEURAL FOAM mark is distinctly related to a highly technical field of computing and creates a distinct commercial impression from the mark FOAM alone.

The word NEURAL also distinguishes the cited mark from FOAM because the word NEURAL is more dominant. One feature of a mark may be recognized as more significant in creating a commercial impression. Greater weight is given to that dominant feature in determining whether there is a likelihood of confusion. *In re National Data Corp.*, 753 F.2d 1056, 224 USPQ 749 (Fed. Cir. 1985); *Tektronix, Inc. v. Daktronics, Inc.*, 534 F.2d 915, 189 USPQ 693 (C.C.P.A. 1976). *In re J.M. Originals Inc.*, 6 USPQ2d 1393 (TTAB 1987); TMEP §1207.01(b)(viii). Since the dominant portion of the cited mark is NEURAL, the first element to be articulated by the consumer, this first element is likely to have an impact on the overall commercial impression of

the mark. The applied-for mark has no corresponding first element and therefore lessens any likelihood of confusion.

Further, NEURAL FOAM is based on an advanced anomaly detection algorithm using unsupervised neural networks for real-time data clustering. It "uses artificial intelligence to cluster massive amounts of data into its simplest, natural structure without a single rule." NetworkWorld, 2011: https://www.networkworld.com/article/2220926/red-lambda-aims-to-tackle-big-data-security.html. See Attachment 2. The term FOAM in this context alludes to the data clusters determined by the NEURAL FOAM algorithm.

The applicant's mark, FOAM, represents a system of digital content containers used to display, share, and interact with media such as URLs and common file types. The term FOAM in this context evokes the structure of a system in which these containers are designed, like bubbles, to interact and proliferate with ease.

In each case, the term FOAM is metaphorically used to describe the organization of data into groups. However, the nature of the data, the purpose of its collection, and the methods by which it is organized are distinct. NEURAL FOAM alludes to data clusters determined by a neural network algorithm. The applied-for mark, FOAM, refers to the nature of digital spaces designed to behave in a foam-like interactive manner.

The use of the word FOAM in this case is similar to the use of the word BOBBER, *In re Farm Fresh Catfish Co.*, 231 USPQ 495, 495-96 (TTAB 1986) (holding CATFISH BOBBERS (with "CATFISH" disclaimed) for fish, and BOBBER for restaurant services, not likely to cause confusion, because the word "BOBBER" has different connotation when used in connection with the respective goods and services). *In re Farm Fresh Catfish Co.* the word BOBBER was found to have different meanings when used in connection with the different goods or services. The same is the case here as described above.

Relatedness of Goods and Services

The examining attorney argues that the broad wording of the NEURAL FOAM description and, presumably, the overlapping words "data management" in the Class 9 description of registration of the NEURAL FOAM mark and the Class 9 and 42 applications for FOAM demonstrate relatedness of the goods. While the word FOAM is indeed common to both marks, the nature and purpose of the goods, and the users and customers of the goods are distinct. As a result the likelihood of confusion is absent.

NEURAL FOAM is an algorithm technology component used to process data within a product previously called MetaGrid and now called Risk Hunter. See Attachment 2. FOAM is a

standalone product. As such, while the word "data management" appears in both marks, the purchasers of the products would not confuse the two marks since the purchaser of any product including NEURAL FOAM would be purchasing the product named Risk Hunter. The FOAM mark identifies a standalone product, not merely a component.

Reasonable consumers of the products would not be confused as purchasers of the Risk Hunter product are not capable of purchasing a standalone product known as NEURAL FOAM. Any purchase of the NEURAL FOAM technology is solely as a component of Risk Hunter.

NEURAL FOAM is an analytical engine that analyzes collected data. Users passively use NEURAL FOAM which operates in the background. Risk Hunter has separate features for data collection upon which the NEURAL FOAM technology operates in an automated fashion applying artificial intelligence. The resulting analysis of the data assists the users in making decisions regarding an enterprise's internal network security operations.

FOAM is a standalone product platform for visualizing and interacting with data. It allows users to collect, organize, search, annotate, and share digital content within storage containers called bubbles. FOAM does not analyze data or deliver results, but requires users to selectively import and organize media objects in ways that can facilitate the human interpretation, discovery, or synthesis of information. The user is actively engaged in use of the FOAM product.

In short, the difference in the nature and purpose of the goods would be apparent to any reasonable purchaser:

- NEURAL FOAM is a component of a product and cannot be purchased alone. FOAM is a standalone product intended to be purchased alone;
- NEURAL FOAM is an algorithm technology which operates without human intervention applying artificial intelligence. FOAM is a platform that requires users to curate data; and
- NEURAL FOAM is intended to produce analytics upon which users make decisions relating to an enterprise's internal network security operations. FOAM enables individual users and groups to curate and engage with digital collections for personal or social purposes.

In addition, the customers of each product are different. Users and purchasers of Risk Hunter are information technology professionals who intend to use the NEURAL FOAM component in order to defend their network infrastructure. FOAM can be used by individual consumers or groups and the purpose is to collect, organize, search, annotate, and share human-curated content. The purchasers of the product of which NEURAL FOAM is a part are sophisticated purchasers who exercise extra care with regard to purchasing networking and security products. In re N.A.D. Inc., 224 U.S.P.Q. 969, 971 (Fed. Cir. 1985); In re Ship, 4 U.S.P.Q.2d 1174, 1176

(TTAB 1987). They are unlikely to confuse a product for content creation, curation, and sharing with a product for defense of the network infrastructure.

Accordingly, the applicant requests that the examining attorney not reject the applicant's mark based on refusal under Section 2(d) of the Trademark Act.

Attachment 1

Other Neural Products

NeuroSolutions
http://www.neurosolutions.com/
The NeuroSolutions product family is leading-edge neural network software for data mining to create highly accurate and predictive models using advanced preprocessing techniques, intelligent automated neural network topology search through [...] distributed computing.

NeuroShell Trader
http://www.wardsystems.com/index.asp
Artificial intelligence, genetic algorithm and neural network software for trading, predicting, forecasting, classification and optimization

Neural Designer
https://www.neuraldesigner.com/ & https://www.neuraldesigner.com/solutions/solutions-retail
Neural Designer is a machine learning platform that helps you discover relationships, recognize patterns, predict trends and find associations from your data.

NeuralWare
https://www.neuralware.com/index.php/products
The NeuralWorks Predict Engine [...] incorporates advanced, automated data preparation facilities and neural network training methodologies that permit end users to create and deploy high-performing neural networks even without in-depth knowledge of neural network technology.

Qualcomm Neural Processing SDK
https://developer.qualcomm.com/software/qualcomm-neural-processing-sdk
The Qualcomm Neural Processing SDK is engineered to help developers save time and effort in optimizing performance of trained neural networks on devices with Snapdragon....

Neural Network Compiler
https://www.latticesemi.com/Products/DesignSoftwareAndIP/AIML/NeuralNetworkCompiler
Compile Neural Networks developed in common development frameworks, such as TensorFlow, Caffe or Keras, for implementation onto Lattice CNN and compact CNN Accelerator IP cores.

Attachment 2

NEURAL FOAM DESCRIPTION

1. Techli, 2012:
https://techli.com/red-lambda/39122/

Florida-based big data and security company Red Lambda is going for a triple play. The company has positioned itself at the intersection of information security, big data, and business analytics since Red Lambda CTO Robert Bird came up with a more automated way to secure and manage a campus resident network of over 10,000 students while he was the Director of Network Services at the University of Florida in 2003. Now, Red Lambda's products span three growing market segments: grid computing, parallel streaming storage, and artificial intelligence.

Three years after Bird's success at the University, Bird and three colleagues received a National Science Foundation grant to develop an advanced anomaly detection algorithm based on unsupervised neural networks for real-time data clustering. This early work was the basis for Red Lambda's patent-pending Neural Foam™, which applies grid computing power to analyze, classify, and visualize massive volumes of data on the fly.

Red Lambda redefined its product strategy in 2010, and made an integrated solution called MetaGrid the core of its offering. MetaGrid is a unique, software-based grid platform that unifies disparate point solutions such as SIEM, firewalls and IPS, tying them all together. The grid platform delivers the scale, speed and storage needed to make disparate solutions and silos of data work together, overcoming historic technology barriers to providing intelligence and automation within large network infrastructures.

2. NetworkWorld, 2011: https://www.networkworld.com/article/2220926/red-lambda-aims-to-tackle-big-data-security.html

One of the really interesting pieces to me of MetaGrid is what Red Lambda calls Neural Foam. Again from their web site, Neural Foam is:

[**Prepare to become a Certified Information Security Systems Professional with this comprehensive online course from PluralSight. Now offering a 10-day free trial!**]

MetaGrid's patent-pending *Neural Foam*™ uses artificial intelligence to cluster massive amounts of data into its simplest, natural structure without a single rule. Neural Foam's unique ability to continuously learn all knowledge and anomalies from **any data, over any timescale, event by event** revolutionizes operations. In one pass, MetaGrid makes it possible to see every aspect of an infrastructure, from the most normal activity, to threats, to things that only happen once or differ by a single unusual bit. Quite simply, it's the ultimate weapon against the unknown, inside or out.

3. Red Lambda FAQs, 2014 (PDF):
https://www.slideshare.net/ZiadIla1/red-lambda-faq

1. Is security and operations where Red Lambda is starting?

Yes. The core technology of the grid platform and the analytics engine, which is called Neural Foam™, uses generalized algorithms that can be applied to any broad scale computing, business intelligence, or data mining task. They can be used in a traditional way, such as analyzing a customer database, or applied to more forward-looking applications involving many disparate data sources—for example, analyzing social media and incorporating that into trend analysis. We focused on security and network operations out of the gate because our team has such deep talent there. Our customers immediately saw exciting potential in other areas, and we explored them.

2. What is Neural Foam?

Neural Foam is our artificial intelligence engine, which powers analytics in MetaGrid. Neural Foam is a universal, automatic data-mining engine, meaning it can be applied to any kind of data. Neural Foam discovers meaningful patterns, anomalies, and correlations, without prior knowledge or training period. It operates automatically, so you really just have a quality and performance trade-off in terms of tuning the software.

3. What kind of expertise is required to operate? Do you need to be a data scientist?

Neural Foam democratizes data mining and requires no data mining experience. Our mission is for customers to get productive, actionable results immediately, not focus on getting a PhD in computer science.

4. BusinessWire, 2011: https://www.businesswire.com/news/home/20110928006573/en/Red-Lambda%25E2%2580%2599s-MetaGrid-Software-Transforms-Security-Operations

MetaGrid is a new software application that runs on the company's AppIron™ Grid Platform and is designed to unify operational silos and situational awareness, visualize and analyze network security and operational anomalies, and automate IT operations.

- *Unify* – Big Data creates big challenges when it comes to unification of operational data. Centralized and appliance-based solutions fall short in their ability to process petabytes a day of operational data. As a result, salient data is often siloed, filtered-out or excluded all together in order to reduce the load and "backhaul" requirements. MetaGrid leverages AppIron's grid architecture and GridStream relational stream processing to move the computation to the data and not the other way around.

- *Analyze* – Collecting more data without better visualization and analysis can leave security operations teams overwhelmed rather than informed. Today's signature-based analysis only looks for threats that are known or anticipated – but what about the unknown unknowns? Red Lambda's patent-pending Neural Foam™ represents a breakthrough in knowledge discovery analytics. It's based on a lifelong-learning neural network algorithm that can analyze and reduce billions of data records -- on-the-fly – into a manageable set of clusters, and provides bit-level universal anomaly detection on a timescale that can be years in duration. MetaGrid's data visualization and exploration capabilities make it easy for security operation teams to identify threats and further correlate, classify, drill-down and search data for intelligence or forensic purposes. Neural Foam increases IT operations effectiveness by providing complete situational awareness, dramatically reduced false positives, and an efficient way to zero-in on anomalies that represent real risk to the organization.

5.

- *Automate* – Capitalizing on actionable insights requires the ability to take action quickly. MetaGrid incorporates incident management and a workflow and autonomics engine to provide intelligent automation of threat notification, response, mitigation, and remediation actions.

CloudPro, 2011: https://www.cloudpro.co.uk/saas/1831/red-lambda-eyes-way-crack-cloud-provider-complexity

MetaGrid introduces Red Lambda's patent-pending Neural Foam knowledge discovery analytics to answer this problem.

Based on a "lifelong-learning" neural network algorithm that can analyse and reduce billions of data records on-the-fly into a manageable set of clusters, Neural Foam analytics can be used to provide bit-level universal anomaly detection on a timescale that the firm said could be as long as years in duration. In this way it can increase IT operations effectiveness by reducing the scope of discovery of threat anomalies and false positives.

6. Network Computing, 2011: https://www.networkcomputing.com/networking/red-lambda-security-revolution-or-just-evolution/page/1/2

Red Lambda uses the term "neural foam" to describe its "neural network" analysis approach. Now, original neural networks in artificial intelligence and data mining required significant user training, which is not possible for real-time detection. Instead, Red Lambda does not just examine individual sessions of data; it examines them all
to create clusters of correlated data. IT can compress billions of individual events into a few hundred clusters, identify the virtual fingerprints and display graphically data into a visual form that security analysts can drill down into to determine what anomalous behavior is threat oriented and what is not.

Red Lambda is a software-only company whose foundational product is AppIron, which enables a grid architecture connected to all devices that are subject to potential threats. The architecture enables inbound data streams to be fully processed in parallel, and data only comes to rest after it has been acted upon.

MetaGrid is the software that sits on top of the base operational software engine AppIron and actually does the work, such as detecting operational anomalies. For example, Wikileaks is known for releasing U.S government documents that the government did not want released. In at least one case, the person who accessed the data to give to Wikileaks downloaded gigabits of information. MetaGrid understands the directionality of data and, as such, may have detected that this was an anomalous
situation and stopped it. But MetaGrid does not just analyze real-time data; in one case, it was used as part of a cleansing process to detect anomalous situations in a year's worth of carrier call records, which can amount to billions of records per day.

7. MetaGrid FAQs, 2016 (PDF):
http://cdn2.hubspot.net/hubfs/399330/PDF_Downloads/MetaGrid_FAQ_FNL.pdf

Q. How does MetaGrid detect threats such as a zero-day event if it does not use any rules or signatures?

Neural Foam makes this possible by incrementally discovering all patterns, anomalies, and correlations and automatically measuring similarity to new things. Take a polymorphic or self-modifying virus as an example. Anti-virus vendors create an explicit signature for every version of a virus and have heuristics that can sometimes discover unseen variants if the variation happens in a known way. But Neural Foam finds all variants, regardless of how it modifies itself. If the functionality is similar, Neural Foam not only finds the new variant, but also knows how similar it is automatically without any heuristics or assumptions. We believe assumptions are the root of most security evils.

Q. Does MetaGrid handle zero day detection?

Yes. MetaGrid's patented algorithms (called Neural Foam) discovers all new patterns, trends, or specific exploits The most interesting thing about Neural Foam is that it can find the indicators of compromise in any of the data available – logs, traffic, network info, etc. Neural Foam can find things when no other tool can because it makes no assumptions about what might be important.