IMPLEMENTATION AND CYBERSECURITY PROTOCOLS OF THE CONSOLIDATED AUDIT TRAIL

November 30, 2017

Mike Beller
Chief Executive Officer of Thesys Technologies, LLC

Thank you Chairman Huizenga, Ranking Member Maloney, and Members of the Subcommittee for inviting me to testify. The Consolidated Audit Trail ("CAT") is a vital step forward to dramatically improve the oversight, regulation, protection, and enhancement of the U.S. capital markets, and I applaud the Committee for organizing this hearing and playing an active oversight role in this area for the benefit of all investors.

My name is Mike Beller and I am the Chief Executive Officer of Thesys Technologies, LLC ("Thesys Tech"), the parent company of Thesys CAT LLC, which is the Plan Processor designated by the CAT NMS Plan. I am a technologist and financial technology business executive with over thirty years of experience working in many aspects of information technology including software development, telecommunications, and information security. I earned degrees in Electrical Engineering from Cornell University and Columbia University. I began my career in the 1980s at Bell Communications Research -- the Research and Development arm of the telephone companies -- where I performed research in a number of areas related to computing and communications, including techniques for protecting mobile telecommunications through the advanced use of cryptography. I subsequently co-founded a startup company focused on applying computing and communication technology to improve the efficiency of the outside-the-office activities of field service and field sales personnel. In 1999, I joined Tradeworx, the parent company of Thesys Tech, as that company's Chief Technology Officer. Over the subsequent eighteen years, I architected, developed, operated, and managed information systems used by a wide variety of participants in the capital markets, including trading systems, data analysis systems, risk management systems, and regulatory technology systems. These systems have consistently advanced the state of the art in terms of performance, scale, and security, while providing cost effective solutions for our customers, including large banks, broker-dealers, buy side institutions, and the U.S. Securities and Exchange Commission ("SEC" or "Commission"). In 2015, I became Chief Executive Officer of Thesys Tech, and it is in this capacity I appear before you today.

Thesys Tech was formed in 2009 as a subsidiary of Tradeworx. The intent was to take the extensive capital markets technology base that had been developed at Tradeworx for its own asset management business and to commercialize that technology for use by other financial services companies. Thesys Tech initially deployed a fully-hosted high performance trading platform, with systems located at each of the facilities that housed the U.S. equities exchanges, allowing firms to more efficiently access the markets. That platform currently processes approximately six percent of U.S. equities trading volume, and approximately fifteen percent of Canadian equities trading volume. Thesys Tech subsequently expanded into exchange or "Matching Engine" technology,

providing fully hosted systems to Alternative Trading Systems ("ATSs"), and allowing those companies to focus on their core businesses while our team ensures their platform is functional, scalable, and reliable. Over the years we have assembled a staff with many experts in electronic trading and technology -- people who have been among the innovators of electronic trading from its early days. Many individuals in the company have decades of experience in electronic trading technology and compliance, as well as a strong grounding in the related areas of "big data" management and information security. This talented and diverse core of experts, dedicated to our mission of improving markets through the use of technology, is our unique differentiator.

In 2010, in the wake of the May 6 "Flash Crash" market event, we met with members of the SEC staff and learned about technological challenges they were having in analyzing market data. As one of the first adopters of the cloud in finance, we realized that the cloud-based big data financial analytics we used within our firm could help the SEC and other regulators in protecting our capital markets. When the SEC subsequently put out a Request for Proposal for a market data analytics system, we responded with a proposal for a state of the art cloud-based analytics system. The SEC ultimately adopted our proposal, and the system is now known as the Market Integrity Data Analytics System ("MIDAS"). This past Fall, the SEC expressed renewed confidence in us as the provider of this important system, extending the term of the MIDAS contract with annual options to renew through 2022.

Going back to 2010, in the immediate wake of the Flash Crash, the Commission also began working on a rule to develop the CAT -- a modern system to track comprehensive information associated with U.S. equities and options trading. As Chairman Clayton recently stated, "[s]imply put, the CAT is intended to enable regulators to oversee our securities markets on a consolidated basis—and in so doing, better protect these markets and investors."[1]

The SEC's final rule -- Rule 613[2] -- was adopted with bi-partisan support in July 2012. In broad strokes, the rule requires the SROs to jointly submit a plan -- called an NMS plan -- to create, implement, and maintain a consolidated audit trail. The CAT improves on existing systems by significantly increasing the information on listed options, by providing additional details for better tracking orders as they traverse the markets, and by adding the ability to identify the individuals involved in trading activity. I believe the CAT will drastically reduce the amount of time and effort required to find and stop bad actors in the market.

[1] *See* Chairman Jay Clayton, Statement on Status of the Consolidated Audit Trail, dated November 14, 2017, available at https://www.sec.gov/news/public-statement/statement-status-consolidated-audit-trail-chairman-jay-clayton

[2] 17 CFR 242.613 – Consolidated Audit Trail; Adopting Press Release no. 34-67457, dated July 18, 2012.

The SROs, acting together as CAT NMS, LLC, issued a Request for Proposal for a firm to be designated as the "Plan Processor" – to build and operate the CAT system -- in February 2013.[3] We were one of over thirty companies that expressed an intent to bid.[4] We viewed the CAT as an opportunity to apply our advanced high-performance technology to meaningfully upgrade the regulatory infrastructure of the markets -- a powerful expression of our mission of "better markets through technology". Having experienced the shortcomings of the existing regulatory regime (including OATS and other systems), we decided that a fresh approach was required.

We developed three principles that guided our design. First, the CAT should be easy to report to. The largest cost of any regulatory system is the burden it places on its reporters. By minimizing that burden, we can minimize the overall cost of the system to the industry. Second, the CAT should be a fully functional system allowing regulators to monitor and analyze the markets. Third, and most importantly, the CAT must be secure.

It was clear to us from the very beginning of the bidding process that the CAT would be a significant target for cybercriminals. In the first year of developing our solution, the massive Target and JP Morgan data breaches both occurred, compromising the data of tens of millions of individuals. We determined it was necessary to take a highly sophisticated approach to cybersecurity, in order to ensure that our solution was up to the task of protecting this very valuable information about our markets. Over the years, in the process of designing and developing our system, we advanced the state of the art in applying technology to the financial markets, particularly in the areas of big data, financial analytics, and the application of cryptography to securing financial data.

In July 2014, CAT NMS winnowed the field down to six finalists, and in November 2015, they named the three finalists: Thesys Tech, FINRA, and SunGard Data Systems. In November of 2016, the SEC unanimously approved the CAT NMS Plan,[5] and in January of 2017, Thesys Tech was selected as the Plan Processor -- with the

[3] *See* Release No. 34-71596 - Joint Industry Plan; Order Approving Proposed National Market System Plan Governing the Process of Selecting a Plan Processor and Developing a Plan for the Consolidated Audit Trail - dated February 21, 2014, page 4 ("The Participants published the RFP on February 26, 2013"), available at https://www.sec.gov/rules/sro/nms/2014/34-71596.pdf

[4] *Id.* ("Thirty-one firms submitted an intent to bid in response to the publication of the RFP").

[5] *See* Release No. 34-79318 - Joint Industry Plan; Order Approving the National Market System Plan Governing the Consolidated Audit Trail - dated November 15, 2016, page 979 ("IT IS THEREFORE ORDERED…that the CAT NMS Plan (File No. 4-698), as modified, be and it hereby is approved and declared effective…"), available at https://www.sec.gov/rules/sro/nms/2016/34-79318.pdf

responsibility to build and operate the CAT under the direction of CAT NMS.[6] On April 6, 2017, Thesys Tech and CAT NMS reached a contractual agreement, known as the Plan Processor Agreement ("PPA"), and Thesys established a subsidiary known as Thesys CAT LLC to execute its responsibilities under that agreement.

Thesys CAT has its own management team, separate from Thesys Tech, in order to provide information barriers between CAT-related activities and other activities of Thesys Tech. The Chief Compliance Officer of Thesys CAT is Shane Swanson, a financial services executive with extensive experience as a financial markets leader, including prior experience as General Counsel and as Chief Compliance Officer of financial services firms, and as an operating executive of a division of a multinational bank. Its Chief Operating Officer is Ed Watson, a finance executive with decades of experience at tier one banks and other financial institutions. In addition, Thesys Tech the parent company of Thesys CAT ensures that Thesys CAT achieves the vision set out in our bid.

From the time we signed the contract seven months ago, we have been hard at work assembling our team, working with the SROs and the industry to develop specifications, and building out the technical and operational components of the CAT -- the information systems, the security plan and operations, the participant specifications, the industry specifications, and the help desk. We look forward to deploying and operating the CAT, with all stakeholders having appropriate confidence that the system is safe and secure, and having had sufficient time to discharge their various requirements and responsibilities.

All of which brings us to a key topic of today's hearing – cybersecurity. As I mentioned earlier, from the very beginning of our conception of a CAT solution, we have focused on cybersecurity as a unique challenge and responsibility in the context of the CAT.

While cybersecurity was our priority in developing a CAT solution, this project was hardly our introduction as professionals to the critical importance of cybersecurity. I personally was introduced to the issue in a very visceral way almost thirty years ago, when systems I managed were attacked by the first wide-scale internet "worm" -- the Morris Internet Worm – on November 2, 1988.[7] In 1988 there were only approximately 80,000 computers on the entire internet, and the worm spread from one computer to another through the internet with ease. The analogy I often use to describe the spread

[6] *See* Selection of Plan Processor for the National Market System Plan Governing the Consolidated Audit Train, dated January 18, 2017, page 1 ("…the Selection Committee of the CAT NMS Plan selected Thesys Technologies, LLC…as Plan Processor for the CAT NMS Plan…"), available at https://www.sec.gov/divisions/marketreg/rule613-info-notice-of-plan-processor-selection.pdf

[7] *See* United States v. Morris, 928, F.2d 504, 506 (2d. Cir. 1991) ("On November 2, 1988 Morris released the worm from a computer at the Massachusetts Institute of Technology."), available at https://scholar.google.com/scholar_case?case=551386241451639668

of the Morris Worm is that, at the time, none of us had good locks on our doors. But the internet was a "small town" thirty years ago, and we could perhaps be excused for not expecting anyone to break in.

Times have changed. They have really changed. The internet has transformed over three decades from a platform for research, to a platform for casual communication, to ultimately become a platform for global communication and commerce, connecting more than three billion of the planet's seven billion inhabitants. And in that same period, typical commercial or government computing systems have grown from connecting to only a few thousand users through dedicated networks, to global systems that interact daily with millions of users via the internet. The immense "connectedness" of the internet means that today systems with very sensitive information are directly or indirectly connected to billions of individuals around the globe.

It is certainly the case that cybersecurity has evolved extensively during this time. Methodologies and technologies have been developed and applied, and standard approaches such as the National Institute of Standards and Technology ("NIST") Cybersecurity Framework[8] have evolved to guide organizations. But it is also clearly the case that the practical application of cybersecurity has fallen woefully short on many notable occasions. Often these missteps are the result of mistakes in the application of accepted approaches. But to some extent, it may also be the case that commonly accepted approaches may fall short when applied to the most sensitive targets. The vast majority of cybersecurity protocols focus heavily on "perimeter security" -- ensuring, in the parlance of my earlier example, that there are very strong locks on the doors, and very solid walls and doors. But often, once the perimeter security is breached, systems inside the wall are entirely too vulnerable. This is the sort of problem that occurred in the recent Equifax breach -- where the outer perimeter was breached due to a vulnerability in an externally facing web server. Once the attacker was inside the Equifax network, a number of other vulnerabilities, including insecure network design, insufficient use of encryption, and ineffective breach detection, led to one of the largest known breaches of Personally Identifiable Information ("PII").

In developing our solution for the CAT, we determined that, as a baseline, we needed to adopt the best controls available, using two factor authentication, and pervasively encrypting data both when stored on systems and in transit between systems, and we needed to ensure that we had best practices to ensure security procedures are adhered to. We adopted the NIST Cybersecurity Framework, the same one we use to secure

[8] *See* National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, dated February 12, 2014, available at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf; Framework for Improving Critical Infrastructure Cybersecurity, draft Version 1.1, dated January 10, 2017, available at https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.1-with-markup1.pdf

the MIDAS system. But beyond that, we determined to build the system, and our organization's culture, with "security first" -- where information security is not an afterthought, but is built into the systems and processes from the start. In particular, we presumed that any system's "door locks" can ultimately be breached, and designed the system with that possibility in mind. By building encryption technology into the very storage and query systems of the CAT, from the ground up, we have designed a system that not only has a very strong perimeter, but if breached, has an array of extra protections to limit the information a cybercriminal can obtain, and to make it easier to detect a breach if it happens. We believe our forward thinking on the matter of cybersecurity greatly supported our bid to become the Plan Processor. We take the responsibility of securing our markets very seriously and, by working with our key subcontractors and partners, including IBM, we have the expertise, experience, and skills to ensure the CAT data is protected.

Additionally, the SEC in its deliberative process, as well as the SROs in their development of the CAT NMS Plan, ultimately promulgated advanced cybersecurity requirements as a part of the Plan.[9] Further, the CAT NMS Plan also requires that the data security standards of the CAT satisfy the applicable provisions of Regulation Systems Compliance and Integrity ("Regulation SCI").[10] Also, while the CAT NMS Plan requires robust protections for PII, we are aware that the SEC is currently conducting a review to assess the importance of PII in the CAT. We await the results of that review in order to inform our actions as the Plan Processor.

[9] With respect to cybersecurity, the CAT NMS Plan requires that the CAT include solutions and controls to ensure the confidentiality and security of the CAT during all communication between CAT reporters and the CAT, data retrieval and extraction, manipulation and transformation including query functionality, loading of data to and from the CAT, and data maintenance. For example, the CAT NMS Plan specifically requires that the CAT have encrypted internet connectivity and that access to the CAT be restricted to a limited number of persons using secure multi-factor authentication with role based access controls. The CAT is required to have a mechanism to confirm the identity of all persons permitted to access the data maintain a record of all such access. All data in the CAT is required to be encrypted at rest and in flight (and any PII stored in the CAT must be stored separately from the other data and access to such PII must be limited to a "need-to-know" basis). Additionally, the CAT NMS Plan requires the Plan Processor to provide a solution addressing physical security controls for any facilities where the above data is transmitted or stored including the requirement that such facilities at a minimum be SOC 2 certified by a third party auditor. All CAT documentation and data must be stored in the United States. The CAT NMS Plan also requires that the Plan Processor conduct and enforce background checks for all of its employees and contractors to ensure the protection, safeguarding and security of the facilities, systems, networks, equipment and data of the CAT. Penetration testing and application security code audits of the CAT must be periodically conducted by third parties to further ensure the security of the CAT.

[10] Regulation SCI, requires the Plan Processor, on behalf of the Plan Participants, to establish, maintain, and enforce written policies and procedures reasonably designed to ensure that the CAT as an SCI system (and those systems, which, if breached, would be reasonably likely to pose security threat to the SCI systems (so-called, the indirect SCI systems)), have levels of integrity, resiliency and security adequate to maintain the operational capability and promote the maintenance of fair and orderly markets. Such policies and procedures should include security standards that conform to current SCI industry standards and contain effective physical and logical security controls to ensure adequate separation between SCI systems and non-SCI systems, detail how the Plan Processor will regularly review, monitor and test the SCI systems (including backup systems) for vulnerabilities, intrusions and disasters, and establish parameters that define the monitoring of system intrusions including taking corrective actions and complying with SCI event reporting requirements. Such policies and procedures should additionally include details regarding the reporting of material SCI systems changes and the performance of SCI reviews to assess internal control design, the effectiveness of the SCI systems, and the policies and procedures themselves. Regulation SCI also requires the Plan Processor to ensure compliance with Regulation SCI by subcontractors by having in place processes and requirements to manage the third-party relationship through appropriate due diligence, contract terms, monitoring, oversight or other methods.

In conclusion, we at Thesys believe that the CAT is an important step forward in the regulation of our markets. As data volumes and complexity continue to increase, the CAT's regulatory transparency will make the markets more robust, support the SROs in their regulatory efforts, and enable the SEC to fulfill its tripartite mission to protect investors, ensure the orderly operation of the markets, and facilitate capital formation. Security is critical to the mission of delivering the CAT, and Thesys is confident it is best qualified to deliver a safe, capable, and cost effective system. Thank you again for the opportunity to speak with you today.