IMPLEMENTATION AND CYBERSECURITY PROTOCOLS OF THE CONSOLIDATED AUDIT TRAIL

HEARING

BEFORE THE

SUBCOMMITTEE ON CAPITAL MARKETS, SECURITIES, AND INVESTMENT

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

NOVEMBER 30, 2017

Printed for the use of the Committee on Financial Services

Serial No. 115–61

U.S. GOVERNMENT PUBLISHING OFFICE

31–288 PDF WASHINGTON : 2018

HOUSE COMMITTEE ON FINANCIAL SERVICES

JEB HENSARLING, Texas, *Chairman*

PATRICK T. McHENRY, North Carolina, *Vice Chairman*
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
STEVAN PEARCE, New Mexico
BILL POSEY, Florida
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
STEVE STIVERS, Ohio
RANDY HULTGREN, Illinois
DENNIS A. ROSS, Florida
ROBERT PITTENGER, North Carolina
ANN WAGNER, Missouri
ANDY BARR, Kentucky
KEITH J. ROTHFUS, Pennsylvania
LUKE MESSER, Indiana
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
BRUCE POLIQUIN, Maine
MIA LOVE, Utah
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
DAVID A. TROTT, Michigan
BARRY LOUDERMILK, Georgia
ALEXANDER X. MOONEY, West Virginia
THOMAS MacARTHUR, New Jersey
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee
CLAUDIA TENNEY, New York
TREY HOLLINGSWORTH, Indiana

MAXINE WATERS, California, *Ranking Member*
CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
MICHAEL E. CAPUANO, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
GWEN MOORE, Wisconsin
KEITH ELLISON, Minnesota
ED PERLMUTTER, Colorado
JAMES A. HIMES, Connecticut
BILL FOSTER, Illinois
DANIEL T. KILDEE, Michigan
JOHN K. DELANEY, Maryland
KYRSTEN SINEMA, Arizona
JOYCE BEATTY, Ohio
DENNY HECK, Washington
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
VICENTE GONZALEZ, Texas
CHARLIE CRIST, Florida
RUBEN KIHUEN, Nevada

KIRSTEN SUTTON MORK, *Staff Director*

SUBCOMMITTEE ON CAPITAL MARKETS, SECURITIES, AND INVESTMENT

BILL HUIZENGA, Michigan, *Chairman*

RANDY HULTGREN, Illinois, *Vice Chairman*
PETER T. KING, New York
PATRICK T. MCHENRY, North Carolina
SEAN P. DUFFY, Wisconsin
STEVE STIVERS, Ohio
ANN WAGNER, Missouri
LUKE MESSER, Indiana
BRUCE POLIQUIN, Maine
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
ALEXANDER X. MOONEY, West Virginia
THOMAS MacARTHUR, New Jersey
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
TREY HOLLINGSWORTH, Indiana

CAROLYN B. MALONEY, New York, *Ranking Member*
BRAD SHERMAN, California
STEPHEN F. LYNCH, Massachusetts
DAVID SCOTT, Georgia
JAMES A. HIMES, Connecticut
KEITH ELLISON, Minnesota
BILL FOSTER, Illinois
GREGORY W. MEEKS, New York
KYRSTEN SINEMA, Arizona
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
VICENTE GONZALEZ, Texas

CONTENTS

WITNESSES

THURSDAY, NOVEMBER 30, 2017

APPENDIX

IMPLEMENTATION AND CYBERSECURITY PROTOCOLS OF THE CONSOLIDATED AUDIT TRAIL

Thursday, November 30, 2017

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CAPITAL MARKETS,
SECURITIES, AND INVESTMENT,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to notice, at 10:06 a.m., in room 2128, Rayburn House Office Building, Hon. Bill Huizenga [chairman of the subcommittee] presiding.

Present: Representatives Huizenga, Hultgren, Poliquin, Emmer, MacArthur, Davidson, Budd, Hollingsworth, Maloney, Sherman, Scott, Foster, Vargas, Gottheimer, and Gonzalez.

Chairman HUIZENGA. The committee will come to order. The Chair is authorized to declare a recess of the committee at any time. This hearing is entitled, "Implementation and Cybersecurity Protocols of the Consolidated Audit Trail."

And I want to thank our guests and witnesses for being here today.

I now recognize myself for 5 minutes to give an opening statement.

Until now there has been no single database that provides comprehensive and readily accessible data about market orders and executions across securities markets. Regulators tracking suspicious activity or investigating unusual events had to collect and aggregate large amounts of data from different markets and participants.

Regulators needed one system that would permit them to track orders and executions across securities markets. The thinking was that a consolidated audit trail system or database that would help regulators keep up with new technology and trading patterns in the market would fit the bill.

That is why, following the Flash Crash of 2010, the Securities and Exchange Commission (SEC) adopted a rule to require self-regulatory organizations (SROs), including national securities exchanges and the Financial Industry Regulatory Authority (FINRA), to develop and implement the Consolidated Audit Trail, or CAT, as a data repository to collect and accurately identify every order from origination through its entire lifecycle, including any cancellation, modification, and trade execution for all exchange-listed equities and options across the U.S. markets.

In January 2017, the SROs selected Thesys Technologies, LLC to build the CAT as the Plan processor, and the SROs were to begin reporting trade and order data to the CAT on November 15 of 2017, of this year. Exactly 1 year later, beginning in November 2018, the SEC's order currently will require broker dealers to submit data, including certain sensitive customer information, to Thesys, the CAT Plan processor.

Many have voiced concerns about the cost of building and implementing such a system. Initial rough estimates by the SEC expect the CAT to carry a one-time implementation cost of $2.4 billion, in addition to a $1.7 billion cost in ongoing annual reports, which will be passed on to customers.

Most troubling, however, is the amount of personally identifiable information, or PII, that will be required to be collected by the CAT, in my opinion. Not only will CAT be collecting such data points as Social Security numbers, addresses, and dates of birth for individual customers, but it will also gather identifiable proprietary transaction data that could potentially be reversed engineered and used for nefarious activity, such as market manipulation.

Let's not forget even the SEC was the victim of a data breach of highly sensitive personally identifiable information. April of 2016 the GAO identified weaknesses regarding information security protocols at the SEC and noted that the Securities and Exchange Commission's failure to implement an agency-wide data security program. Additionally, the SEC's own internal assessment, initiated once Chairman Clayton came on board, found that the agency had inadequate controls and that there were serious cyber and data risks.

Concerns regarding data security are not unfounded. In September of this year, we learned of a software vulnerability in the test filing component in the SEC's EDGAR—or electronic data gathering, analysis, and retrieval system. Because of this lapse in security, hackers were able to gain access to highly sensitive material, including the names, dates of birth, and Social Security numbers of two individuals.

A recent report from the Government Accountability Office highlights how the EDGAR data breach only underscores what is now even of greater concern: The sufficiency of risk control mechanisms for the SEC approved in the Consolidated Audit Trail. The CAT system will be the most comprehensive repository of market data we have ever seen for all exchange-listed equities and options across all U.S. markets. Some have indicated that this database will be the world's second-largest single database, only behind the National Security Agency.

I continue to express very serious concerns about the security of such extraordinary amounts of personally identifiable information being collected and held by the CAT, as well as who might have access to such confidential and sensitive information. I think that is a vital question.

While the CAT may be a helpful resource for the SEC and even the SROs once fully implemented, insufficient data security controls will only undermine confidence in our markets.

Today's hearing will examine the status of the CAT's implementation and the adequacy of existing data security protections re-

garding the storage and use of CAT data by entities that are part of the CAT operating committee, the CAT Plan processor, and the SEC. It will also example whether additional cybersecurity protocols are necessary to properly safeguard collected data, including that PII—personally identifiable information.

Additionally, the hearing will examine a discussion draft legislative proposal that we have titled, "The American Customer and Market Information Protection Act," which would require the SEC, each SRO that is a participant of the CAT NMS (national market system) Plan, and the CAT Plan processor to develop comprehensive internal risk control mechanisms to safeguard and govern the security of information reported, stored, or accessed from the CAT.

The legislation would prohibit the CAT Plan processor from accepting data until it develops such risk controls and the SEC certifies those controls. The legislation would also prohibit the SROs from accessing CAT data until each entity develops risk controls and the SEC certifies them, as well. Last, the discussion draft would require the SEC to conduct a cost-benefit analysis on the CAT's use of PII, as well as report to Congress whether such information is a necessary input for the CAT, the risks posed to investors by using that information, and alternatives that the SEC could consider.

The importance of cybersecurity cannot be overstated. The ability of the SEC to safeguard nonpublic financial information and other highly sensitive data is paramount because it instills confidence in our markets.

The Federal Government—namely, the SEC—cannot afford to get this wrong. In fact, SEC Commissioner Michael Piwowar recently commented regarding CAT that, quote, "deadlines are important, but the SEC has one chance to get this right. We have to make sure we have everything locked down. We can get it done, or we can get it done right. We need to get it done right," end quote.

I couldn't agree more.

And I look forward to hearing from our distinguished panel today.

So with that, the Chair now recognizes the Ranking Member for a very generous 5 minutes as well, as I went over for a bit. And the gentlelady has 5 minutes, as well. Thank you.

Mrs. MALONEY. You had a lot to say and it was all important.

And I thank you for holding this important hearing and for all of our panelists for being here today with us.

The so-called Flash Crash in 2010 was an extraordinary and terrifying event in which markets simply went haywire. They experienced a sudden inexplicable crash and then recovered most of their losses just as quickly.

The entire episode lasted only 36 minutes, but it had a lasting effect on investor confidence in our markets. And I have always said that markets run more on confidence than they do on capital.

In the aftermath of that wild-day market, participants, regulators, and Members of Congress were all asking the same questions: What happened, and why did it happen?

To answer those questions the SEC and CFTC (Commodity Futures Trading Commission) attempted to reconstruct all of the trad-

ing activity that occurred that day. This should have been a relatively straightforward exercise to the agencies with oversight of the stock and futures market, but it took the agency over 4 months to issue a report on the Flash Crash, and even then the report was inconclusive.

Why did it take the agency so long? Because they didn't actually have a comprehensive system in place to collect all of the information about the trading that takes place in U.S. markets.

And I must share with you, when Fuld, head of Lehman, was testifying on the financial crisis I asked him, "What is the one thing that we could do that would prevent it in the future?" And it was to collect this trading information and have it in one place. So this is an important project for the stability of our markets and our economy.

Instead, they were relying on a patchwork of audit trails operated by individual exchanges or other trading venues. And each of these audit trails had different types of information, which made it very difficult to track orders that were routed from one exchange to another.

As a result of all of this, the SEC proposed to create the Consolidate Audit Trail, or CAT, which would serve as a comprehensive record of all trading activity in the U.S. equity markets. The SEC proposed the CAT back in 2010, and 7 years later we still do not have a fully functioning audit trail.

We can go to the moon, but we can't figure out how to have a fully functioning audit trail. I would say that this is an American scandal.

The creation of the CAT has been subject to endless delays and too many missed deadlines to count. The CAT was supposed to go live 2 weeks ago, on November 15th. But at the last minute the exchanges charged with implementing the CAT requested another delay and stated that they could not start submitting data to the CAT on time.

SEC Chairman Clayton rejected the exchanges' request for another delay, but the reality is that even though the deadline has passed the CAT is still not up and running. I completely support Chairman Clayton in his demand to start right now.

Some market participants have raised concerns about data security due to the large volume of confidential information that will be stored in the CAT. The plan for the CAT, which was approved by all of the exchanges and the SEC, does include data security standards, and I will be interested in hearing whether our panel believes these security data standards are strong enough or need to be enhanced.

So I want to thank all of the panelists for appearing today.

And I yield back my time, and I am under budget and on time.

Chairman HUIZENGA. If you—

Mrs. MALONEY. That is what we need the CAT system to be—

Chairman HUIZENGA. Yes, yes.

Mrs. MALONEY. —Right?

Chairman HUIZENGA. If you average it out we took our 10 minutes, so—

Mrs. MALONEY. OK.

Chairman HUIZENGA. Thank you. Appreciate the gentlelady's attention to this.

And today we welcome a great panel. Appreciate them all being here.

First we have Mr. Mike Beller, CEO of Thesys Technologies, LLC. We also have Chris Concannon, President and Chief Operating Officer of the Chicago Board of Options Exchange.

Welcome.

We have Tyler Gellasch, Executive Director of Healthy Markets Association. And last but certainly not least, Lisa Dolly, who is the CEO of Pershing, LLC.

And we welcome our panel. Thank you very much.

And with that, Mr. Beller, you are recognized for 5 minutes.

STATEMENT OF MIKE BELLER

Mr. BELLER. Thank you, Chairman Huizenga, Ranking Member Maloney, and members of the subcommittee, for inviting me to testify.

The Consolidated Audit Trail is a vital step forward to dramatically improve the regulation and protection 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, the parent company of Thesys CAT, which is the Plan processor designated by the CAT NMS Plan. I am a technologist and financial technology business executive with over 30 years of industry experience.

In 2010, in response to the Flash Crash, the Commission began working on a rule to develop the CAT. As Chairman Clayton recently stated, "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."

The SEC's final rule was adopted with bipartisan support in July 2012. In accordance with the rule, in February 2013 the SROs, acting together as CAT NMS, LLC, issued an RFP for a firm to be designated as the Plan processor to build and operate the CAT system.

We were one of over 30 companies that expressed an intent to bid. November 2016 the SEC unanimously approved the CAT NMS Plan, and in January 2017, after a 4-year bidding process, Thesys Technologies was selected as the Plan processor.

On April 6, 2017, only 7 months ago, Thesys Tech and CAT NMS reached a contractual agreement, known as the Plan Processor Agreement, and Thesys established a subsidiary known as Thesys CAT to execute its responsibilities under that agreement.

When we began this process we viewed the CAT as an opportunity to apply our expertise to meaningfully upgrade the regulatory infrastructure of the markets. This is a powerful expression of our mission of better markets through technology.

The CAT improves on existing systems by significantly increasing the information available to regulators, allowing them to better track orders and identify the individuals involved in trading activity. And we believe the CAT will drastically reduce the amount of time and effort required to find and stop bad actors in the market.

From the outset we have focused on cybersecurity as a unique challenge and responsibility in the context of CAT. While cybersecurity was our priority in developing a CAT solution, the 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 30 years ago on November 2nd of 1988, when systems I managed were attacked by the first wide-scale Internet worm, the Morris Internet Worm. In 1988 there were only approximately 80,000 computers on the Internet and the worm spread from one computer to another through the Internet with ease.

The analogy I often use is that at the time none of us had good locks on our doors, but the Internet was like a small town 30 years ago, and we could perhaps be excused for not locking our doors and not expecting anyone to break in. But times have changed.

The Internet is now a global platform connecting billions of people. Very often, when building systems, firms focus heavily on securing the perimeter, making sure there are good locks on the doors; but once the perimeter security is breached systems inside the wall are entirely too vulnerable, as we saw in the case of the Equifax breach.

In developing our solution for the CAT, we adopted best practices, using multi-factor authentication and encrypting all data, both at rest and in transit between systems. But beyond that, we determined to build the system with a security-first mindset, where cybersecurity is not an afterthought but is built into the systems and processes from the start.

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 when it happens.

So in conclusion, we at Thesys believe that the CAT is an important step forward in the regulation of our markets. From the time we signed the contract 7 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 CAT's technical and operational components.

We look forward to deploying and operating the CAT with all stakeholders having confidence that the system is safe and secure and having had sufficient time to discharge their various requirements and responsibilities.

Thank you again for inviting me today, and I look forward to answering your questions.

[The prepared statement of Mr. Beller can be found on page 42 of the appendix.]

Chairman HUIZENGA. Thank you.

With that, Mr. Concannon, you are recognized for 5 minutes.

STATEMENT OF CHRIS CONCANNON

Mr. CONCANNON. Thank you.

Mr. Chairman, members of the subcommittee, I am Chris Concannon, President and Chief Operating Officer of Cboe Global

Markets. I have over 20 years of experience as an exchange executive, trading firm executive, and a regulator.

Cboe operates six national securities exchanges consisting of four options exchange and four equity markets. We operate the largest U.S. options exchange; we are the second-largest U.S. equities exchange operator. Cboe also operates a U.S. futures exchange, the largest European exchange, and a foreign exchange platform.

I would like to thank the subcommittee for inviting me to testify today regarding the Consolidated Audit Trail, or CAT.

In August 2012 the Securities and Exchange Commission adopted rule 613 under the Securities and Exchange Act of 1934 to require securities exchanges and FINRA to submit a national market system plan to create a consolidated order tracking system. The primary rationale behind the establishment of the CAT was to improve upon and consolidate a regulatory framework that at the time was supported by disparate audit trail sources.

The SROs initially submitted a CAT Plan to the SEC on September 30, 2014. The Commission approved the CAT Plan on November 15, 2016.

For several years, including during the last year since that approval, the SROs have been working diligently on execution of the CAT project. This has entailed, among other things, a comprehensive bidding process to determine the operator of the CAT Plan processor, selection of the CAT Plan processor, negotiations of a contract with the chosen entity, and commencement of the building of the CAT itself.

Accomplishing each of these steps is no small feat, given that there are over 20 SROs operated by multiple holding companies that must effectively agree every step of the way.

Per the milestones set forth in rule 613, the Plan processor was selected in January of this year. And the development of specific details in the CAT design framework, including data submission layouts and, in particular, security protocols, have taken some time.

Pursuant to rule 613, the phase one implementation of the CAT reporting process was due to go live on November 15th of this year, 1 year from the approval order. Unfortunately, work on the CAT is not complete.

In planning for the completion of the CAT project, the SROs have taken into account the heightened need to maximize the CAT's security planning and protocols, given the recent proliferation of data breaches that have occurred and the highly sensitive nature of the data that will be stored in the CAT. The SROs have also thoroughly consulted and forecasted with the CAT Plan processor and considered ample feedback from industry participants on deliverables and expectations.

The proposed revised schedule takes into account these factors, as well as forecasting based on detailed framework plans.

We continue to work toward expeditiously completing the CAT project. Indeed, our efforts on the CAT have been substantial. To date, Cboe has spent over $10 million on CAT, we have over a dozen employees regularly involved in the CAT project, and we have spent approximately 30,000 man-hours on CAT.

I commend the subcommittee for conducting this hearing and for continuing to focus on ensuring that the CAT is developed efficiently and effectively while insisting that the data security around the CAT is vigorous and robust. I am concerned about the risks associated with storing PII in the CAT database and can assure you that Cboe is very interested in working with the Commission and other stakeholders on exploring alternatives around PII as a necessary component of CAT.

While I recognize there are benefits to be derived from the CAT, I also must point out that costs associated with this project likely are ultimately funded by investors. We are committed to building the CAT as currently contemplated and remain committed to maintaining a strong regulatory program.

While the CAT buildout continues, please let there be no doubt that our existing surveillance and regulatory framework is robust and our markets are well protected. Indeed, the U.S. financial markets are the most efficient and liquid markets in the world and the regulatory framework around those markets, led by the SEC, is second to none.

The CAT will be an important component of that framework, and we look forward to the completion of a smart, secure, and efficient CAT system.

Thank you for the opportunity to appear before you today. I am happy to answer any questions.

[The prepared statement of Mr. Concannon can be found on page 50 of the appendix.]

Chairman HUIZENGA. Thank you.

Mr. Gellasch, you are recognized for 5 minutes.

STATEMENT OF TYLER GELLASCH

Mr. GELLASCH. Thank you.

Chairman Huizenga, Ranking Member Maloney, and other members of the subcommittee, thanks for having us here today. I am the executive director of a trade association of those investors, the pension plans, and investment advisors who believe that informed market participants and regulators are essential for healthy markets.

Almost exactly 7 years ago—next week—then staffer Kara Stein staffed a hearing across the Capitol where the SEC and CFTC chairmen assured the public and our bosses that the Consolidated Audit Trail was going to be up and running by now and not be billions of dollars that had been projected in their recent proposal, and we are now still years away from that.

We are ostensibly here to talk today about data security, but rather, I will assert that this hearing is really about whether for-profit market participants, some of whom may have the most to lose by the creation of the CAT, are able to exploit a convenient public fear to continue to deny regulators the basic tools to police the markets. After years of delays and exemptions, they have simply run out of other excuses.

The exchanges and FINRA have not offered any significant new information as to why the provider that they selected and the expectations and standards that they set are somehow inadequate, other than repeating the words "cybersecurity risk," "PII," and

"breach" as many times and in as grave of tones as they can muster. I don't know why the next major market participant—or the next major market event or manipulation will happen, but I can safely say that they will, and the real question is whether or not you are going to give the regulators the tools that they need to enforce and protect investors.

Today, private market participants have a much more comprehensive view of the markets than the regulators tasked with overseeing them. Currently, if regulators want to see who is conducting trading they have to ask FINRA, who then asks the broker dealers for the personal identifying information. So the broker dealers have it and it is just the regulators who don't.

But because there is no automated way to link the trading and the underlying beneficial owner, there is actually very little chance to identify and stop sophisticated market abuses without a whistleblower. In fact, it is only those who are not smart enough to spread around their trading who get caught.

And in fact, we only need to look at the Flash Crash to see how this all works or doesn't. The Flash Crash was concerning for a lot of reasons. And it was months before the SEC or CFTC figured it out, and that is concerning in its own right.

But it wasn't until 5 years later that we learned the role of one market manipulator outside of London in his parent's basement—5 years later, and that was only because of a whistleblower.

By using the NMS Plan process to build the CAT, the SEC essentially outsourced every function for it, including who is going to pay. It puts some of the parties who stood to lose the most from the CAT's existence in charge of creating it.

The SROs were supposed to have the CAT Plan by April 2013. When they weren't going to meet the deadline they asked for an extension; they got it. When they weren't going to meet the new deadline they asked for another extension; they got it.

More years, more exemptions, more delays. Now we are finally about ready to have it, and we have reached the moment where it is about ready to happen, and it is not going to happen either. And the excuse is data security.

After 7 years of planning and hundreds of meetings and tens of thousands of hours for some of these folks, what the heck have they been doing if not worrying about data security? Interestingly, they have been. They set detailed security protocols and information-handling, some that actually SIFMA (Securities Industry and Financial Markets Association) and others have called the gold standard.

So I am not aware of any allegations that Thesys can't meet the standards that the SROs set or that the standards themselves are somehow inadequate.

The legislation this committee has passed and is now considering would unquestionably delay the CAT and leave it tied up in legal complexities and red tape for years—frankly, if it doesn't kill it entirely. The new bill would prevent Thesys from accepting data until the SEC certifies that its required internal risk control mechanisms.

To be blunt, do we really think the SEC are the experts on data security right now? Isn't that why—part of the reason why we are here?

But there are dozens of other questions, including the adequacy: What is the SEC going to do? What is the standard? Are they going to test the adequacy of those mechanisms? Does that somehow inoculate Thesys from liability if there is a breach because the SEC blessed it?

The bill would also require an entirely new and duplicative cost-benefit analysis and a report to Congress on the need for identifying information. That is not forwarding the process. That is not talking about data security. That is the primary reason for the CAT, to figure out who is doing the trading.

I also want to take a couple of seconds here to point out that that is not the only thing that is delayed. Who is going to fund it is also delayed. The SEC has delayed that decision until January 2018, and I am sure you will be surprised to learn that the exchanges have decided to try to push most of that burden onto the broker dealers, not themselves.

Longer term, I hope you push for the Consolidated Audit Trail to be implemented without delay to include futures, and I hope you end the NMS Plan process that got us into this mess.

Thank you.

[The prepared statement of Mr. Gellasch can be found on page 61 of the appendix.]

Chairman HUIZENGA. Ms. Dolly, you are recognized for 5 minutes.

STATEMENT OF LISA DOLLY

Ms. DOLLY. Thank you, Chairman Huizenga, Ranking Member Maloney, and distinguished members of the subcommittee, for the opportunity to testify today on behalf of SIFMA and share our views on the implementation plan for the Consolidated Audit Trail.

My name is Lisa Dolly. I am the CEO of Pershing, which is a bank of New York Mellon company. Pershing is custodian for over 6 million U.S. institutional and retail clients, and we safekeep, on behalf for those clients, more than $1.5 trillion in assets.

This subcommittee's review of CAT implementation is incredibly important and timely. There is a great value in a workable, secure CAT, but the implementation issues remain largely unaddressed and incomplete. Quite frankly, there is concern remaining over the security of privacy issues.

When the CAT is fully operational, as mentioned before, it will capture all customer and order event information for equities and listed options from the time of execution, becoming one of the world's largest databases. In fact, every day the system will take in over 58 billion records—orders, executions, quotes—and will maintain this to become a 100 million-data point database for institutional and retail investors and their unique customer identifying information.

So despite the unprecedented amount of sensitive information being stored in the central repository and the associated data protection concerns, the technical specifications that have been released to date do not, alarmingly, include many details around data

security and protection. And as the SROs' initial reporting deadline approached and passed, Thesys had not yet hired a chief information security officer, who would be responsible to review and implement the data security policies and procedures to ensure the protection of CAT data, as required by the CAT NMS Plan.

The SEC and the SROs should make the case that PII is actually necessary for CAT. If sensitive identifying information is included in the CAT, then the SEC and the SROs must provide better assurances on the data security than they have to date. Financial firms and regulatory agencies share a common goal in securing and protecting the data entrusted to them by clients and financial institutions, and this issue trumps everything else.

In addition to the question of the uses of CAT data, all of the 22 SROs and the SEC will be allowed to download any or bulk data from CAT into their own systems, and the NMS Plan requires the CAT to accommodate up to 3,000 users' access to that data. As a result, the protection of the data depends not only on the security of the CAT system but also the security of each of the SROs plus the SEC.

SIFMA believes the draft legislation being discussed today would benefit the protection of this information. At this point, we think there should be a delay in the CAT implementation to allow the SEC to examine the need to include PII in the CAT, and if the SEC decides that such information is necessary it is absolutely imperative that the CAT's data security protocol be strong and secure.

The CAT NMS Plan should also be amended so that no PII or identifying trade data can be extracted from the CAT processor. Rather, the regulators should perform surveillance within the CAT security perimeter.

A delay is also required to allow additional time for the broker dealers' CAT implementation. Once the technical specifications have been finalized, broker dealers should have a minimum of 12 months to complete the implementation and testing based upon final specifications.

Going forward, a collaboration among industry participants, the SROs, and Thesys could really provide the opportunity for CAT to be informed by the insights and interests of all those affected and all the market participants so they can be incorporated and provide for a successful CAT construction and implementation. There is still time to get this right.

In conclusion, SIFMA appreciates the interest of the subcommittee and is supportive of further efforts to legislate improvements to the CAT. And I thank you for the opportunity to testify and look forward to answering your questions.

Thank you.

[The prepared statement of Ms. Dolly can be found on page 54 of the appendix.]

Chairman HUIZENGA. Thank you, Ms. Dolly. Appreciate that.

And with that, I will recognize myself for 5 minutes for questioning.

Many, including myself, have raised concerns about cybersecurity and the protection of data submitted to the CAT. Apparently some believe that it is, quote, "just to exploit convenient public fear." I don't believe that is the case. As you know, the CAT NMS Plan re-

quires a plan processor to appoint a chief information security officer who will be responsible for creating and enforcing appropriate policies, procedures, control structures.

Mr. Beller, in your statement you said that Thesys developed three principles that guided the design of the CAT database. Specifically, you say, quote, "third and most importantly, the CAT must be secure," close quote.

If cybersecurity is top of mind for you and Thesys, why has a chief information security officer not been hired to date?

Mr. BELLER. Thank you, Chairman.

The selection and approval of a chief information security officer is an activity that is collaborative between Thesys, as the Plan processor, and the SROs acting as CAT NMS. As yet, we have not agreed on a candidate.

The role is a very challenging role to fill that has expectations in policy areas, in technology areas, in management areas. And we are working collaboratively to find the right person to fill that role. Our recent activities together lead me to believe that we should come to a positive conclusion shortly.

Chairman HUIZENGA. OK.

Mr. Concannon, is this simply private companies trying to, quote, "exploit convenient public fear" for the concerns that you have been expressing?

Mr. CONCANNON. I think the evidence is pretty clear that we are not exploiting public fear when we see so many breaches that have taken place, including our own Government, which has been breached multiple times. And some of the most sophisticated agencies of our Government have been breached.

So when I think about the information that we have planned under the current construct to put into the CAT, I am more than concerned that we are putting—in fact, all of your Social Security numbers, as designed, will be in the CAT. And so we all sitting around this table should be concerned how we protect that information.

Chairman HUIZENGA. Has Thesys presented any CISO (chief information security officer)—he—Mr. Beller said it is a collaborative process. Have they presented any candidates for that CISO position? And if so, why have they been rejected or not—

Mr. CONCANNON. First of all, that entire space is very difficult to find candidates. It is one of the hottest employee spaces. We have had difficulty trying to attract cyber specialists.

So it is a very difficult role to fill. This is a senior cyber expert that we are trying to find.

We have looked at candidates. We have a very high standard. All of the exchanges and SROs have a very high standard, and we are using our own cyber professionals to evaluate, and they have an even higher standard of one another.

So we have evaluated candidates and we have rejected candidates.

Chairman HUIZENGA. OK. Since the CISO has not been put in place and this agreement hasn't happened under the Plan, would SROs really actually be able to begin reporting trade data to the CAT?

Mr. CONCANNON. The SROs are subject to numerous rules. Data protection is covered by Reg SCI (Regulation Systems Compliance and Integrity).

Chairman HUIZENGA. So there may be—and just to get to that there may be the physical ability, but is there the legal ability? Is that what you are saying?

Mr. CONCANNON. In fact, there is the physical ability today. We can put our data in the current CAT system.

Chairman HUIZENGA. So I could collect all of your Social Security numbers and put them in my phone. Would that make you feel OK?

Mr. CONCANNON. It would not make me feel—

Chairman HUIZENGA. You would be OK with that? I loan my phone out to my kids once in a while. Is that—I think we made the point that just because you can do something, we have to make sure that it is prepared on that. And I am curious who actually verifies that Thesys is complying with all the cybersecurity requirements, as well.

Mr. Beller or Mr. Concannon or Ms. Dolly?

Mr. BELLER. So there is a—the Plan itself lays out a very robust framework for security and a bunch of audits and approvals that must be completed in order for the CAT to go live and operate. We need to collaboratively select the chief information security officer.

The chief information security officer then has a fiduciary duty, actually, to the SROs via CAT NMS, LLC. So that duty actually trumps that person's duties to Thesys CAT itself.

Chairman HUIZENGA. And presumably the SEC, or no?

Mr. BELLER. I don't know of anything in the Plan that places an expectation that the CISO reports to the SEC. This, I think, has to do with how the Plan is structured and the relationship of the SROs to the SEC, so maybe—

Mr. CONCANNON. I have had a rule throughout my career that nothing trumps the SEC.

Chairman HUIZENGA. Spoken like a truly regulated entity.

OK. So I am over, but let me just encourage you to move forward, both of you—collectively, not you individually, but collectively. We need to get this CISO in place so that we can start meeting with that.

I am well over, but I recognize the Ranking Member for 5 minutes.

Mrs. MALONEY. Thank you. And I join you in saying that we have to get this CISO appointed. I suggest that we have a hearing on this every month until we get them appointed and hear what the success of it is.

Let me tell you, the stock market is exploding and many people are putting their faith and hope in it. And I think if we had a crash it would totally destroy the confidence of Americans in the system. So I think this truly, is probably the most important thing we could do in our Capital Markets Subcommittee.

Where is Thesys located? You beat out 30 major companies. Where is your headquarters?

Mr. BELLER. Our headquarters is in New York City, and we have offices in Charleston, South Carolina additionally.

Mrs. MALONEY. OK. And where are you developing the CAT system? In New York City?

Mr. BELLER. In both locations.

Mrs. MALONEY. In both locations. And why is it taking so long?

Mr. BELLER. The CAT is taking a long time because it is a complex system with multiple stakeholders who need to act collaboratively in order to get this complex system up and secure. We obtained the contract to build the CAT 7 months ago and in that time have built out an organization, developed technical specifications, built out pieces of the CAT and the security program, and put them in place. And there are some items that remain that have to be done collaboratively by the stakeholders, including—

Mrs. MALONEY. I think we should have a collaborative meeting once a month and bring in all the stakeholders with the SEC and see how we can get an agreement so we can move this thing forward. I think this is a priority for our Nation.

I would like to ask Mr. Gellasch, you noted that the CAT was developed in response to the Flash Crash, and certainly the CAT will help the SEC reconstruct another market crash like the Flash Crash. But apart from helping to reconstruct market crashes, will the CAT help the SEC perform their normal day-to-day oversight functions? What will the CAT allow the SEC to do that it cannot do today or that it is doing very inefficiently today?

Mr. GELLASCH. Thank you for that question.

A couple of things. One is most people talk about the Flash Crash as the precipitating event for the audit trail. That is actually a little bit untrue, and here is why: As far back as early 2009 there was an effort underway to understand who large traders were and who was actually engaged in trading. And in fact, there was a large-trader reporting regime that preceded the Consolidated Audit Trail, and the Consolidated Audit Trail proposal was released on May 26th of 2010.

The SEC didn't write that several-hundred-page document in 3 weeks. The SEC doesn't do anything that fast. So I would say the Consolidated Audit Trail itself came together after the Flash Crash, and certainly that was the precipitating event in providing public feedback.

The reason why the underlying concern existed even before the Flash Crash was because the SEC and FINRA—neither know who conducts trading in our capital markets. So the current audit trial systems tell you who the broker is but not whose trading underlies it.

What does that mean? So assume for a moment you have those who—for example, a market manipulator engages with a couple of different brokers and trades in a couple of different venues—perhaps equities and maybe in options. Those things would not be seen in a coherent way.

And so because you don't know who is doing the trading, the manipulations get lost in the noise of the markets. That is why it takes a whistleblower to find market manipulation cases.

FINRA has incredible surveillance now that did not exist 7 years ago either. They have actually put in—99.5 percent of equities trading goes into FINRA's pipe for surveillance. But even with that it is still only the stupid who get caught.

Mrs. MALONEY. OK. I would like to ask you what do you think of the proposed legislation that would prohibit the CAT from accepting personally identifiable information under the SEC has—unless the SEC has conducted a cost-benefit analysis? And is the collection of personally identifiable information necessary for a system like CAT?

Mr. GELLASCH. Well first, the whole point of the CAT is to find out who is doing the trading, and you have to have a certain amount of basic information about them in order to do that. Now, there are a number of ways that could be done.

One would be to have all the personal identifying information in it. Another could easily be legal entity identifiers, which the CAT declines to do—doesn't do. I might argue that might be a more elegant way of solving some of these issues.

But the cost-benefit analysis suggested by the proposed legislation, to me that cost-benefit analysis was done in 2009, 2010, 2011, it was done in 2012 in the final rule for this. So it was done as part of the large-trader reporting analysis; it was done as part of the Consolidated Audit Trail analysis.

It is long past settled that we actually need to know who is doing the trading in our markets. So I would argue that that is actually just to frustrate the purposes here.

I 100 percent agree with trying to make sure that data security is important, and they should have someone there in that role. But it also requires cooperation.

When we talk about what is taking so long to get this up and built, they have had it 7 years—or 7 months they have had the contract. They were involved in designing the specifications for years before that, along with the SROs, but that was only after several years of the SROs designing the specifications.

Mrs. MALONEY. OK. My time is up.

I would be inclined to join the gentleman with his legislation if he removes the cost-benefit analysis, which, according to your analysis—2009, 2010, 2011—is past settled. I think this is a critical, critical issue.

After the financial crash in 2008, the Flash Crash, everybody said, "We have to know this information." If we care about the future of the financial system of our country we have to get this system up and running.

All of you are going to be part of making that happen.

I would like to get, if I could real quick, Mike Beller, to get from you exactly the elements that you will be collecting, send it to the committee. And I would like a monthly report on whether or not you have gotten the person assigned. Let us know or I will be calling you directly, because I think this is incredibly important to our financial security and to our country.

I yield back.

Chairman HUIZENGA. The gentlelady's time is expired.

And the Chair right now recognizes the Vice Chair of the committee, Mr. Hultgren from Illinois, for 5 minutes.

Mr. HULTGREN. Thank you, Chairman.

Thank you all. Grateful that you are here.

It was stated that the SEC doesn't move too quickly. I think that is an understatement. And a big part of the delay has—it was over

2 years, I think, that this has stuck within SEC, so it is not just industry but there are other bureaucracy problems that are a challenge, as well.

Mr. Concannon, I wonder if I could—first, welcome. Glad you are here. Thanks for your work.

And if I can address my first couple of questions to you, I wanted to get your opinion on making sure the cybersecurity standards we are discussing today are really enforceable.

As you know, the CAT operator is contractually obligated to be compliant with Reg SCI. Is there any reason to not make this a statutory requirement? Would this be an improvement to the discussion of the bill?

And then also, do you believe compliance with Reg SCI, NIST (National Institute of Standards and Technology) standards, and other cybersecurity protocols would improve if the CAT operator were required to register with the SEC?

Mr. CONCANNON. It is a great question.

So Reg SCI is probably one of the most powerful rules I have seen by the SEC in a long time. The requirements that come with Reg SCI, because they are based on the NIST standards and they are global standards, require a great deal of work and a great deal of technical work included in that.

So all of the SROs, all the exchanges have to comply with Reg SCI and, by definition, our vendors have to be in compliance with Reg SCI standards. So it would makes sense if the CAT was—obviously it has to be compliant with Reg SCI because of our own obligations and our vendor, but it would make sense if they were even a Reg SCI entity and registered with the SEC.

That is really how the SIP, the securities information processor, where all the quotes come from our markets, is currently an SCI entity, as we call it. So it would make sense that others in the NMS Plan, including the surveillance part—and more importantly, if they are carrying all this critical information—not just PII, but proprietary trading information is critical information that needs to be protected—it would make sense that everybody in the chain is a Reg SCI registered entity.

Mr. HULTGREN. Thanks. I am going to shift a little bit, but stay with you, Mr. Concannon, if I could.

I was hoping to see if you could speak to some of the opportunities and challenges of data standardization. I understand all the exchanges and broker dealers could potentially report data in different formats, which would make it extremely difficult for the CAT operator to transform this data—these data sets into useful information for its users.

What steps should be taken to be sure data standardization processes are as frictionless as possible? It seems like this could be an opportunity to minimize costs. I wonder if you have any thoughts on that.

Mr. CONCANNON. Yes. This is a critical element that is less talked about because it is in the technical details of how orders are—and information is sent into really any database that we use for surveillance today.

We outsource all of our surveillance, or some of our surveillance and market manipulation requirements to FINRA, where they have

become the master of normalization or data standardization. All of the exchanges and the brokers have different order types. There are thousands of different order types that we have registered with the SEC, unfortunately.

Each order type becomes a new standard, a new piece of information for surveillance purposes. If we don't standardize all those order types it makes surveilling that database very difficult. So it is critical to performing adequate and superior surveillance to have data normalization or data standardization.

Mr. HULTGREN. Thank you.

Ms. Dolly, if I can address to you, this database, as we are talking about, is going to contain every stock quote and trade in America. Apart from safeguarding personal information, what protections are being used to ensure the security of trading and quoting data?

This information could be firm-specific and theoretically could be used to reverse engineer broker dealer strategies to serious detriment of not just the broker dealer but also the client and ultimately to the markets themselves.

Also, this could all happen without a breach of the CAT. This is something we recently discussed in the committee when there were allegations of SEC staff illegally accessing trading source codes. Thousands of people have access to this data.

Do you and does SIFMA share this concern? What do you believe should be done to address these concerns?

Ms. DOLLY. Our company doesn't really trade on a proprietary basis, but I do represent 6 million individual investors and institutions, and I can tell you that it is critically important and a very large concern of theirs how we handle their information and how we protect it.

And I believe to date it is not just the chief information risk officer that hasn't been hired; I don't believe that proper procedures and policies and actually the Plan around securing that data has been shared, and so I don't have comfort around that yet.

Mr. HULTGREN. Thank you all.

I yield back.

Chairman HUIZENGA. Gentleman's time has expired.

With that, the Chair recognizes the gentleman from Georgia, Mr. Scott, for 5 minutes.

Mr. SCOTT. Thank you, Mr. Chairman.

Ms. Dolly, I read your testimony and it is very interesting, and I agree with you. But I would like for you to highlight, if you could, when you did in your report some serious data security implementation concerns. Of course, paramount was the one in which the failure of the CAT system processor's not having a chief information security officer in place before the first reporting deadline.

Also, I have been getting some calls from some of our friends in industry for a further delay of the November 2018 reporting deadline, and I would like for you, if you could share with us that aside from maybe a full delay, could you talk about what can be done in the short term, in the next couple of months, that would make firms like yours and, quite honestly, all of us in America sleep a little better? Because there is some struggling as to how far to

delay, what to delay. What can we do right now, what—in order to do this?

Ms. Dolly, as you go through this, we do have people who may be tuning in on C-SPAN, American people. "What is CAT," they are probably saying. And of course we know it is the Consolidated Audit Trail, but if you could walk us through that, too, what we are talking about here and some suggestions from you as to what is most immediate that we need to do.

Ms. DOLLY. If I missed any of those questions just let me know.

Mr. SCOTT. Sure.

Ms. DOLLY. So I think what we can do immediately is two things, maybe three. But first we need to work together in order to finalize the technical specifications for CAT.

So I mentioned that the implementation deadline of November would be very difficult because firms need at least 12 months in order to implement. We haven't received the specifications to date and we are already a month into this now, so I am down to 11 months to be able to implement. And this is a large project for most firms, and we absolutely need a year to be able to design, create, and construct the solution.

So that delay is not really sticking our feet in the mud; it is just reality that we need at least 12 months in order to be able to implement once we receive the technical specifications. So getting those technical specifications out will hasten our ability to comply and participate in CAT as an industry.

Mr. SCOTT. Let me ask you, you also mention in your testimony a call for a serious cost-benefit analysis. Would that be helpful? And also with that analysis you wanted to add the consideration of whether personally identifiable information, or PII, should even be collected in the first place. Would you comment on that?

Ms. DOLLY. Certainly. I think that there are ways that we can move forward without PII being collected so that the regulators and the SROs can perform the surveillance that they need to perform and should perform to be able to provide for and promote a healthy and secure capital market for both institutions and investors. And it might be a more immediate way forward through the large-trader rule, through the legal entity identifier.

If we could start there that might be a more immediate way, but what I would recommend is the collaborative effort on a way forward between the industry and the SROs and regulators.

Mr. SCOTT. Yes. And I agree with you on that, and I think that is a very, very important point.

Mr. Concannon, in your testimony you acknowledge that the work of CAT is incomplete and you cite data security concerns as a basis for that delay. Could you share with the committee today the efforts being done at the CAT operating committee to implement the data security protocols required by the CAT Plan before November 15th reporting deadline?

Mr. CONCANNON. Great question. So the SROs that are responsible for delivering the CAT have been working diligently now for years, not only designing but also working with Thesys to build and implement. We meet not once a week but several times a week every week for hours on hours, and we have subcommittees that are meeting.

We have built out a group of our own cybersecurity specialists to work, so we are in parallel working on the cybersecurity plan that the CAT will ultimately have while we are also out looking for a cybersecurity specialist to be employed by the CAT. So we are not standing still waiting around for this person to show up. Every SRO sitting at the table is hard at work and they are putting their highest professionals into the CAT process to make sure we deliver this CAT.

Mr. SCOTT. Thank you very much, Mr. Chairman.

Chairman HUIZENGA. Gentleman's time has expired.

With that, the Chair recognizes the gentleman from Maine, Mr. Poliquin, for 5 minutes.

Mr. POLIQUIN. Thank you, Mr. Chairman, very much.

And thank you all very much for being here today.

This is a very, very important issue. All of us here on the committee and here in the public sector have a responsibility to make sure our markets are protected and remain liquid and secure.

This is still America. People like to invest, like to buy part of our economy, and they certainly have—should expect their data to be secure.

And at the same time, I understand that the regulators are in the business of making sure that we have an opportunity, have the tools that we need, the data that we need to make sure you catch bad actors.

I worry about everything. You do that when you come from rural Maine. I worry about our small investors.

Let's say you are a nurse in Lewiston, Maine. And you are a single mom; you have a couple kids. You have aging parents and you see how expensive it is to care or help care for your parents as they get older.

You are trying to save a little bit of money but you don't want to keep it under the mattress and you know you are getting almost nothing in cash, so you say, "I want to buy 100 shares of Walmart and I want to buy it through my local broker, because I like Christmas and I buy my Christmas lights and my ornaments from Walmart, so that is a great way to invest in America."

So I am giving this information to my broker—who I am. He or she puts the order in. You get a confirmation back that, in fact, the trade has been executed at a certain price.

Now, my question to you is the following: If something goes wrong with that mom who is a nurse in Lewiston, Maine with that trade or with her account, does that represent any disruption to our capital markets? I would say probably not.

So my question is the following, is that, look, let's just call a spade a spade. We have a real problem with data security in America, whether it be the Federal Government, whether it be Equifax, or whether it be folks like Wells Fargo who have been misusing very sensitive personal data.

Now, I have a concern that we are building a new system here to make sure we watch out for bad actors who could adversely or illegally influence market trends. I understand that. But you are putting a lot of data in one place—a lot of data in one place. And that concentration—maybe over-concentration—of the data concerns me.

Mr. Gellasch, am I pronouncing your name right, or close enough?

Mr. GELLASCH. Close enough.

Mr. POLIQUIN. Close enough.

How many pieces of data per day would run through the CAT system when this thing is up and running, roughly? Billions?

Mr. GELLASCH. It is close to 60 billion events per day.

Mr. POLIQUIN. 60 billion events per day. OK.

And could someone tell me—Ms. Dolly, maybe you can—tell me why all kinds of sensitive personal information, including Social Security numbers, which are critical to making sure families can proceed with their lives with financial security—whether getting on an airplane, or getting a passport, or getting a job, or getting an interview for a job—why does that information need to be loaded up in one place where we know we have a problem everywhere and we are going to continue to have a problem with data security? Why is that information necessary?

Mr. GELLASCH. So if I can—

Mr. POLIQUIN. Sure. Who wants to take a shot at it?

Mr. GELLASCH. Thank you. So the question is whether or not you need to know who that is or whether or not you need every piece of data about that person that is important to do that traveling along with that information. I would say those two things are different questions.

Mr. POLIQUIN. And what is CAT doing now—what is being done so that the CAT will be up and running when it comes to this data? Is it necessary? Is it overkill? I am talking about for the little investor in rural Maine.

Mr. GELLASCH. Yes. I will say for the little investor—and I will also say, our members are also investors who have a lot of those people investing in them, too, it is their information, as well. So be it a large pension plan or something else, it is also a lot of those people.

And I would say I 100 percent agree the information security is extremely, extremely important. What is equally important for them is to make sure that the market doesn't do something like a Flash Crash, because that will get them to lose their investment; that will also get them to say, "I am not—I am going to put the money under the mattress again instead of buying my 100 shares of Walmart."

And that is what happened after the Flash Crash, actually. A lot of money did come out of mutual funds as a result of that.

So one of the things I think we really need to focus on and say, look, what is the primary objective? The regulator needs to know who is doing the trading. That is a simple need. The regulators have known that now for decades. And they don't have that information.

At the same time, how are you able to do that without having Social Security numbers traveling along with order information?

I would say there actually was a somewhat elegant solution from legal entity identifiers and basic information and cross-referencing that. I thought that that would be a solution. Unfortunately, that is not the way the Plan was developed. That is not necessarily the way this has moved forward.

I do think that FINRA has incredible capabilities on their current surveillance right now, but I think their surveillance team would probably also be the first to tell you that without knowing who is doing the trading they essentially have to have a whistleblower or they have to hit a screen and get very, very lucky.

Mr. POLIQUIN. Thank you, Mr. Gellasch, very much.

Mr. Chairman, thank you for your indulgement. I appreciate it. Yield back my time.

Chairman HUIZENGA. Gentleman's time has expired.

And we are getting some conversations going over here, too, because I think this is a critical point in this whole discussion: What is it that moves markets? Is it the individual investor or is it an institutional investor? And that may be some area where we need to explore that.

So with that, the Chair recognizes the gentleman from Illinois, Dr. Foster, at this time.

Mr. FOSTER. Thank you.

Let's see. I guess this is a question for Mr. Concannon or Mr. Beller.

I assume that there was a rather detailed cybersecurity specification as part of the vendor selection process for this. And did this include things like, the NIST specification for cyber procedures, and so on?

Mr. BELLER. Thank you. The CAT NMS Plan, as published, contains an enormous amount of prescriptive information on security. In fact, I would have to say that it is the most comprehensive information security program that I have ever seen specified in my life.

It includes background checks and fingerprinting of employees and contractors; physical security of facilities; a requirement to encrypt all data in transit and at rest, meaning when it is moving through the system and when it is on computers themselves; to segregate personally identifiable information from all other information; and to ensure that personally identifiable information is not returned as part of the normal use of the CAT. In fact, there are special rules to protect the personally identifiable information so that only specific users can be empowered to have it, and those users must have a need to know, and there are further cybersecurity restrictions there.

So it is a very comprehensive—

Mr. FOSTER. —Personally identifiable information, that is at the firm level, the individual level?

Mr. BELLER. Individual level.

Mr. FOSTER. Individual. So this is like one trader inside a firm, for example.

Mr. BELLER. Yes. Or one customer of a firm.

Mr. FOSTER. Right. OK.

And so I had a question of—your testimony refers to defense in depth, where you have cloud-based storage. When you refer to cloud-based operations does that mean there are other users on the same silicon of this, or do you have a dedicated—will all the CAT information, where—when it gets aggregated, be by itself in a room by itself, or are there going to be one of these things where you are selling computer time to anyone who is interested when—

Mr. BELLER. So some systems of the CAT are completely segregated. All the ones that involve personally identifiable information are completely segregated in data centers—tier one data centers, where the exchanges are located in Illinois and in New York—New Jersey, excuse me. And that data is all strictly in private data centers.

Other data of the CAT, when encrypted, can exist in cloud systems that are inside the United States.

Mr. FOSTER. OK. And the encryption-in-flight is with frequently renegotiated session keys and all this stuff?

Mr. BELLER. Absolutely.

Mr. FOSTER. OK.

Now, you also mentioned the query structure, that when you are querying—looking for abusive trading patterns, or whatever the data set will be used for, that you had some method of querying the data without just returning the entire unencrypted—give me all the trades for Renaissance or someone like that for the last 6 months. Do you have a way of querying it and identifying abusive patterns without actually pulling all the individual data for that?

Mr. BELLER. So let me clarify that the—just want to make sure that it is clear that the regulators, of course, have to do the querying, not Thesys. Thesys has to provide the system that permits the querying.

But in answer to your question, as I understand it, yes, there are extensive query capabilities that allow the regulator to request a very narrow slice of the data very specifically. And to reinforce that I am—I repeat that in general queries against the CAT system will not return PII in any case, that that would be a separate query that would be specifically for authorized—

Mr. FOSTER. A serial number for—that this was an individual. If you are looking at a correlation between things that look like market manipulation, where you have two allegedly separate traders—

Mr. BELLER. Yes.

Mr. FOSTER. —And you are looking for correlations to find out if you are manipulating a price here and making a derivative bet there, or something like that.

Mr. BELLER. Exactly. So there would be a unique identifier for—

Mr. FOSTER. There is a unique identifier, and so and the personally identifiable stuff is the translation of that to Social Security numbers and addresses. OK.

Mr. BELLER. So presumably that would happen—

Mr. FOSTER. Identifying the existence of abusive trading doesn't require knowing who it is, just the pattern.

Mr. BELLER. At that point. The issue becomes figuring out a uniform identifier for the individual requires PII.

Mr. FOSTER. OK. And then you have to understand if this person is actually the brother-in-law of that person, and I—there is no way to not go into addresses and names and other databases to figure that out.

And so eventually a lot of the querying will actually have to get access to, I would presume, to the personally—this—there may be an illusory separation of this, is what I am—for the queries that actually take place.

Let's see, and could you just quickly walk through how his query system would have identified the abusive behavior of this guy in London, whose name I forget, who actually went to jail over abusive trading around the time of the Flash Crash? What queries would have led to that?

Mr. BELLER. So I am not a regulator and wouldn't want to explain how a regulator does their job. The important point that I can state here is that without the ability to identify an individual then the orders just appear to be coming from a broker dealer, and how does one separate one person's trading activity from another?

Mr. FOSTER. OK. Thank you.

Yield back.

Chairman HUIZENGA. Gentleman's time has expired.

With that, the gentleman from Ohio, Mr. Davidson, is recognized for 5 minutes.

Mr. DAVIDSON. Thank you, Mr. Chairman.

And thank you, to our guests. I really appreciate your expertise in this matter, and thanks.

A couple of you talked about how—painted this as some draconian delay effort to sabotage CAT. And as the sponsor of the Market Data Security Act I can assure you that it is not.

Frankly, I can't understand why it wouldn't take a simple memo, if it is as clean-cut as, Mr. Gellasch, as you say it is, as, "Oh, well this has already been done. We have planned for 6 years."

Great. Just send us a memo that says that. Piece of cake. Doesn't even take a week.

But if you want to be thorough, in light of the new director at the SEC coming in and finding after the fact that there are data breaches in the SEC, as you point out, maybe they are not the best—someone is going to certify it. Shall we say that it is the chief information officer at Thesys? No.

Mr. Beller, you have an organization to run, and certainly many other things to accomplish. In the absence of this position being filled, who fills the role now?

Mr. BELLER. So aspects of the role can be filled by other individuals. For example, we have security experts working together to build the security plan, and working collaboratively with the SROs on that. We have technologists who are experts in cryptography developing the cryptographic systems.

But there are parts of the role that have to be fulfilled according to the Plan by a chief information security officer who has certain fiduciary duties and responsibilities, and those we can't—we have no way around.

Mr. DAVIDSON. Does that person somehow mitigate your responsibility as the CEO for everything that happens or fails to happen in your organization?

Mr. BELLER. Not at all.

Mr. DAVIDSON. Mr. Concannon, has Thesys presented any CISO candidates?

Mr. CONCANNON. Yes. We have been evaluating a number of candidates for a period of time, and it is, as I mentioned earlier, it is quite a hard role to fill. It is quite a hard role to find adequate candidates.

Mr. DAVIDSON. What is the wisdom, in your mind, of going forward without someone who owns the responsibility for the security? Is the CEO at Thesys adequate accountability for data security, or should this position be filled?

Mr. CONCANNON. As much as I will hold Mr. Beller responsible for anything that breaks in the CAT, we do need a cyber specialist sitting in the seat.

I want to clarify something. We are very focused on this individual, but it is an entire process that that individual is responsible for.

It is really network security; it is—and then it is also what we call penetration testing. So there has to be a third party that comes in—a professional third party that comes in and tries to penetrate the CAT network. And that is done by all of us—every SRO and hopefully most of the government agencies. We have these third parties that come in and try to hack our networks regularly.

We have to get to that level of capability to ensure that this network that we are building, called the CAT, and all this proprietary information that we are putting in is protected, and even from our own hackers.

Mr. DAVIDSON. Thank you very much for that, because it highlights that it is not as simple as let's—"Yes, we have already been doing that. Let's just send a memo." It is something that would take a review.

I am reluctant to say how long that review should take, whether it is a week or I would expect that it would be a matter of months or weeks, not a matter of months or years, in terms of making sure we have this well thought out.

Ms. Dolly, you point out one of the critical pieces is, in most systems when there is a compromise, one of the most frequent collapses or breaches is inpoint security. There are a lot of inputs into this, and you pointed out that each entity that is involved in launching this product should also have some level of certainty in their data controls.

And Mr. Concannon, you referenced that in a way.

Could you offer your thoughts there, please?

Ms. DOLLY. Yes. As I outlined, the more places that this data resides the more requirements there are and the more complex the security and protection around it needs to be. The more users that have access to it and are able to do things like bulk download creates risk to the folks whose information is in there, and so it just creates more targets.

Mr. DAVIDSON. Thank you for that. And that is exactly it. It is risk-based.

And I think my time is expired, so thank you for your testimony.

Mr. Chairman, I yield.

Chairman HUIZENGA. Gentleman yields back.

With that, gentleman from North Carolina, Mr. Budd, is recognized for 5 minutes.

Mr. BUDD. I am going to yield to the gentleman from Ohio for a few moments.

Mr. DAVIDSON. Thank you.

I just had one additional point there, because what we are asking in market data is that it be a risk-based assessment. And it is systemic, and maybe that has all been designed in.

But when you have voids at the top, when everyone is responsible, as is often the case, no one is. And the concern is that this is going on; the concern is that it has gone on in the regulator, SEC, so doesn't it make sense?

So what would be the downside of making sure that we get the product right? And when I think about it and I hear, "We don't have the instructions," I think about other products like operating systems.

Part of the reason these devices were so successful, when the one that I care to carry more wasn't, is they found people to be able to write apps for it. And so people had to have access to the code. However, having access to the code creates some security risks.

So how do you keep that under control? What is the status of being able to get that and assure us that we have the risk controls, Mr. Concannon?

Mr. CONCANNON. Thank you.

Really I want to clarify one fact that we have been wrestling here and hasn't been mentioned. We have the most robust surveillance mechanism on the Planet. We have professional regulators across the country that are surveilling all of the data, every trade that takes place in our markets.

So we are not—even though some other witnesses mentioned that—risk and there is manipulation going on, we are catching manipulation every day. We are catching manipulation across client accounts; we are catching manipulation across markets and across products. So we have some of the most robust surveillance.

So when I think about getting it right I feel very comfortable that we are very protected. All of our investors are protected by the professionals that are defending our market.

Mr. DAVIDSON. Thank you.

I yield back, Mr. Budd.

Mr. BUDD. Thank you.

Mr. Concannon, to continue, so given the relatively limited Flash Crash activity since 2010 and the clearly increasing risk of cyber incursions that we have seen, it looks to me that the risk calculation concerning the CAT, or the Consolidated Audit Trail, truly changed. It looks like what we are trying to address, the Flash Crash, is less likely, and the problems that a single point of failure would cause are actually more likely.

So is it your view, as well, and can you talk about the way that the risk environment has changed for this project and how that has changed over time?

Mr. CONCANNON. Sure. First of all, there has been this misunderstanding that the CAT somehow stops flash crashes. It has nothing to do with stopping flash crashes. It is a database. It is a database where we house information.

In fact, we had a mini flash crash in August 2015 and we were able to replicate the market behavior very quickly and the SEC was able to issue a report because they actually hired Thesys to write MIDAS (Market Information Data Analytics System), which

is a database that they use to look at the market and study the market and analyze it.

As I think about it, the material, the data that is going into CAT, both in phase one—and eventually PII data, but even just the phase one—is proprietary trading information of not only investors but market makers and proprietary trading firms. And it can be used to manipulate our markets.

So the first phase of CAT is critical data going into a database that we need to protect. And I would agree with you that cybersecurity is the number one concern right now, given all of the evidence that we have seen by some of the most technically sophisticated operators that they, too, were hacked. So we need to have that as our first line of defense while we build this system.

It is OK to take time to get it right because we have the best surveillance mechanisms today provided by the exchanges, the other exchanges that don't sit here, and FINRA.

Mr. BUDD. Thank you, Mr. Concannon.

Ms. Dolly, in the remaining time I have, you note in your testimony that the draft CAT specs have been released today. They don't have a lot of detail on data security and protection.

So in your opinion, what is missing in regards to what has been released so far?

Ms. DOLLY. Really just about everything. We haven't received very much around cybersecurity and the protection that we would demand and need to protect institutional and retail clients. So I don't believe that has been issued to date, and it would be a responsibility, I would imagine, of the CISO when they are hired.

Mr. BUDD. Thank you, Ms. Dolly.

I am out of time. Yield back.

Chairman HUIZENGA. Gentleman's time has expired.

But we are hoping, if it is all right with our panelists, to do a quick second round, as well, if you have the time and the ability to stay. There is interest on—I think on our side as well as the minority's side. We do have one more person, I believe.

Mr. Gonzalez, are you prepared?

Mr. GONZALEZ. Yes.

Chairman HUIZENGA. You are recognized for 5 minutes.

Mr. GONZALEZ. Thank you.

The question is for Mr. Beller, and the question is, the CAT Plan expressly requires that the CAT include industry standard data controls, including the cybersecurity framework established in the National Institute of Standards and Technology. Can you describe the specifics of the aspects of the CAT design that provide protections for personally identifiable information, such as customer data, that will be reported to the CAT?

Mr. BELLER. Thank you for the question. Absolutely.

So first to point out that the—there are extensive cybersecurity requirements in the Plan. One of them is that the Plan processor has to build the system in accordance with the National Institute of Standards and Technology, or NIST, cybersecurity framework, which explains whole areas of control groups around many different aspects of security. It is a comprehensive plan and we are building to that structure.

With respect to personally identifiable information in particular, there are an extra set of requirements that are specific to that data as opposed to or as distinguished from other data in the system. There is a special role-based access control that a regulatory user of the CAT is not necessarily permitted to access the PII except on a need-to-know basis. So that means there are extra access controls in the system that allow you to—allow an administrator to determine that an individual can be allocated access to that data or not, separate from access to the system.

It is stored in separate areas, actually in separate physical data centers, and not stored in the cloud. It is encrypted in transit, at rest. There is an audit trail specific to the access to personally identifiable information over and above the auditing of everything else that happens. And in general, record displays in the CAT, they don't display the personally identifiable information.

I also want to point out that personally identifiable information won't be collected in the CAT until phase two, when—not—it will not be collected in the initial deployment of the CAT, which only, in its initial phase, takes data from the participants themselves, which are the exchanges and FINRA.

Mr. GONZALEZ. Thank you.

I yield back.

Chairman HUIZENGA. Gentleman yields back.

With that, the gentleman from California, Mr. Sherman is recognized for 5 minutes.

Mr. SHERMAN. Ms. Dolly, what would it take for you to be comfortable resuming implementation of CAT, and what would it take for those of us whose data is in the hands of your customers to also be comfortable?

Ms. DOLLY. I would be much more comfortable if we understood what the technical specifications were so that we could make certain that we could build the house that we are being asked to build. If we don't know what we are building it is a little bit difficult to make certain that we meet the obligations.

The second is that I would like a robust discussion around whether PII is actually necessary, or can we use patterns and other data so that we could identify things that may create uncertain markets or unsecure markets and be a risk to our markets, yet not create such a large database of personal information that is subject to cyber risk and other.

And I would certainly be open to figuring out a way—a collective dialog that would help us to move implementation forward with insight and influence by all participants. We all have, quite frankly, a vested interest in a secure and healthy capital market, but we also have a vested interest and we have an actual duty to protect clients' and investors' private information.

Mr. SHERMAN. Mr. Beller, I wonder if you could shed some light on how Thesys and the committee are approaching the hiring of a chief information officer. I assume you are recruiting someone with world-class experience in cybersecurity.

Mr. BELLER. Absolutely. We have engaged a prominent recruiter. We have 24 candidates under consideration, if I recall correctly just from memory. It could be changing day to day. A number have already been initially interviewed and we are now in the process of

setting up interviews that would include both Thesys CAT personnel and SRO personnel.

Mr. SHERMAN. Also, Mr. Beller, we should be focused on improving the data available to regulators without requiring market participants to engage in costly duplicative reporting. How do you tend to construct CAT so that the existing system, like OATS (Order Audit Trail System), can be retired as soon as possible after CAT is up and running?

Mr. BELLER. So it is our opinion that one of the real positive aspects of the Consolidated Audit Trail is it allows the retirement of several existing systems, one of which is OATS. And as I understand it, FINRA has published an explanation of the process by which, once the CAT has come up and is running and has, according to them, measured certain reporting quality standards, then they would be retiring OATS.

Mr. SHERMAN. Ms. Dolly, is that a system that works for your members?

Ms. DOLLY. Yes. That would be fantastic if we got to that point so we didn't have duplicative reporting requirements.

Mr. SHERMAN. Mr. Beller, could you provide a summary of Thesys' expertise with respect to management and security of market data, including expertise in responding to cyber attacks?

Mr. BELLER. Certainly. I personally have been involved with cybersecurity for an extended time. There is some information in my prepared testimony.

In fact, as a researcher in the Bell Communications Research, which was the research organization of the telephone networks back in the day, I myself did research on the application of cryptographic protocols to securing communications.

I have been involved in building such systems over—systems in the capital markets for quite a long time now. And one example of that—of course, it is not just me. My company has a large number of capital markets technology experts with a great deal of cybersecurity expertise.

We have, for example, deployed the MIDAS system for the Securities and Exchange Commission starting in 2013. In fact, we received the contract in August 2012 and within 6 months had a system up compliant with the National Institute of Standards and Technology security framework and meeting all requirements required by that framework, and had authority to operate.

That system has been operating for 5 years and we were recently renewed, showing renewed confidence in us.

Mr. SHERMAN. Thank you.

My time is expired. I yield back.

Chairman HUIZENGA. Gentleman's time has expired, but we are going to move to a second round.

And I will recognize myself here for 5 minutes to continue the conversation. A little bit of what Mr. Davidson was talking about, but certainly what the Ranking Member and I were talking about up here.

Ms. Dolly, I would like to know, are retail investors typically involved in market manipulation?

Or maybe, Mr. Concannon, you can address that, as well.

Ms. DOLLY. I don't know necessarily how to answer that question. I am sure they could be, but in the past there—it has been more of an institutional mechanism. For example, algorithms and trading platforms that kick off at certain points in a market movement generally have contributed more and are able to swing the market more, certainly, than a retail investor.

Could there be a bad actor that is a retail investor? Of course. But the average retail investor, as described before, is not necessarily going to be able to move the market.

Chairman HUIZENGA. Mr. Concannon?

Mr. CONCANNON. Yes. In fact, when you look at the data—and Mr. Gellasch mentioned the large-trader ID—if we were to implement a large-trader ID we would probably capture the majority of what I will call the surveillance alerts that our regulators are seeing day in and day out. So retail investors generally are not involved in manipulation. There are retail investors that obviously get caught up in insider trading, and we capture those quite quickly.

We are seeing an increase of—

Chairman HUIZENGA. So just on that point, so you don't need PII at that point, that data, to necessarily catch somebody who is doing insider trading?

Mr. CONCANNON. To be clear, we, the market and the regulators, always get PII. So the PII exists in the regulatory framework.

Chairman HUIZENGA. But it wouldn't have to go into a database—

Mr. CONCANNON. We don't need it—

Chairman HUIZENGA. —To catch those inside traders.

Mr. CONCANNON. —In the surveillance. There is not a surveillance mechanism in the U.S. that is surveilling Social Security numbers to look for insider trading.

Chairman HUIZENGA. So have there been alternatives really considered? Mr. Gellasch talked a little bit about this large-trader ID, which has been talked about.

Why could we not just do that—assign a certain threshold and above has to have this ID, then use that, load that into the database. It would seem to me that that covers what the SEC is trying to get at; it covers the tracing of market manipulation and other things; yet, it doesn't expose individual retail investors, Bill Huizenga going out and buying 300 shares of, pick it, Gentex or, Steelcase, or whatever it might be—good West Michigan companies.

A, I am not moving the market. B, I am not using any manipulation into that, but I am exposed. And information is the gold—personal information is the gold of the modern era, as I always say. And if we know that there is a—that the safe has been cracked and we say, "cat burglar got away, or maybe we even caught the cat burglar but let's just load some more gold into that vault," which we know has been breached, why would we continue to do that?

So—

Mr. CONCANNON. There was a question in that—

Chairman HUIZENGA. Yes. Here is the question—

Mr. CONCANNON. I understand the question.

Chairman HUIZENGA. OK.

Mr. CONCANNON. The answer is there are alternatives to the current design of PII in the CAT, and I was encouraged by Chairman Clayton's recent statements, and he continues to make those statements that he is open to looking at alternatives on PII in particular. Among the industry and some regulators we have talked about a large-trader ID solution as a fairly—

Chairman HUIZENGA. Which could be an individual, right? If it is—

Mr. CONCANNON. It can be a professional trader—

Chairman HUIZENGA. —Buying huge, massive blocks as an individual.

Mr. CONCANNON. This is a method that is used in the futures market. There is a concept of large-trader ID. It follows every order into the surveillance system so you can track the large trader based on their activity.

So yes, there are solutions that are being kicked around to avoid having that PII information in the database.

We will always get access. Regulators have ample access to PII information under the blue-sheeting technology that we have.

Chairman HUIZENGA. When it comes to enforcement?

Mr. CONCANNON. Right.

Chairman HUIZENGA. I am going to get to you.

But real quickly, Mr. Beller, you are including PII because you are required to include PII, correct?

Mr. BELLER. That is absolutely correct.

Chairman HUIZENGA. OK. So if we come back and, working with the SEC, or legislatively we say, "Hey, let's develop a separate system," you have no problem being able to do that?

Mr. BELLER. Absolutely.

Chairman HUIZENGA. All right.

I am over my—I am going to try to do that. The Ranking Member, I would—believe would go to Mr. Gellasch here, but I am—with that, my time is expired.

Mrs. MALONEY. OK. If anyone would like to respond to the Chairman's statements—Mr. Gellasch, why don't you start and anybody else who wants to respond.

Mr. GELLASCH. Thank you for the opportunity. I wanted to actually echo and agree.

Frankly, the FINRA had proposed using a large-trader ID reporting system as part of the Consolidated Audit Trail many, many years ago and actually wrote a white paper on precisely that point. I think when you convert to a different model like that two things have changed since that time.

One is, what is the purpose in the abstract? Where do you set those thresholds, becomes a very, very, very important question in terms of volume thresholds and those types of things. I do think that there is significant opportunity there to reduce risk, perhaps, while still capturing the bulk of concerning things.

Two, there actually is a system that would be valuable in the legal entity identifier—again, one that was not included with the CAT but something that I would argue should be included in the CAT.

And I will actually make a third point, which Mr. Concannon brought up, which is that a system similar to that is used in the futures market, and I would argue remarkably effectively.

Mrs. MALONEY. Thank you.

Mr. Beller, you noted in your testimony that the CAT is subject to very robust cybersecurity standards. Have you actually completed your work on implementing these cybersecurity standards yet?

Mr. BELLER. The work is not complete, and we have discussed today some of the key elements that are missing. And one of the most important is the naming of a chief information security officer who has very specific roles in the completion of the process.

Mrs. MALONEY. If the exchanges started submitting data to the CAT today would that information be protected?

Mr. BELLER. I believe that the Plan requires us to go through some steps before we can accept data.

Have we built a technical system that can receive and secure data? Yes, I believe so.

The Plan requires us to go through a number of steps to certify that, and those are collaborative steps between us and the SROs: Naming the CISO, approving all appropriate cybersecurity policies, and having what is called an independent third-party audit of both the code—that is to say the software code—and the third-party penetration testing. Those things all are steps that are required and they haven't been done as yet.

Mrs. MALONEY. Mr. Gellasch, in your written testimony you pointed out that the CAT bears many similarities to FINRA's Order Audit Trail System, or OATS. Can you walk us through some of those similarities? What are the similarities to OATS?

Mr. GELLASCH. Yes. So the Order Audit Trail System actually itself was a response to a crisis in market surveillance, actually, and created in the 1990's for that purpose.

And what it does is it is a comprehensive audit trail system, but it doesn't include beneficial owner information; it doesn't include the types of precision you need to conduct modern surveillance. It was a product of the late 1990's.

And it is the—you glue that together. What FINRA does is they glue that together with the consolidated prop feeds to really get an understanding. And they do fantastic surveillance, but without the benefit of the beneficial owner.

So trying to figure out who is doing the trading isn't in OATS, but it would be in the Consolidated Audit Trail. But conceptually they are remarkably similar.

They are also remarkably similar in something Ms. Dolly spoke about earlier, which is how many people access the system and how many people are inputting into the system. One of the greatest challenges with the Consolidated Audit Trail, it is not just the folks who get to access the data; it is actually one of the greatest challenges is something she has touched upon, which is the folks putting in the data.

When you have thousands of folks putting data into a system a lot can go wrong. And that is actually one of the great challenges.

And again, FINRA has been doing this a very long time, and actually that—they have learned from that over now several decades, and that—all of that knowledge has actually gone into, I think—

Mrs. MALONEY. So that is a very important point, so I want to go back to Mr. Beller.

Who is going to be putting the data in, Mr. Beller, into your system? Who is going to have—be putting that data in?

Mr. BELLER. The broker dealers will each be responsible for transmitting their data into the CAT on a daily basis.

Mrs. MALONEY. And the basic difference between CAT and OATS, again? What is the basic difference between them?

Mr. BELLER. Oh, was this to me?

Mrs. MALONEY. I am talking to Gellasch right now, yes.

Mr. GELLASCH. Sorry. Most important to me is knowing who is doing the trading. And as Mr. Concannon referenced, the—

Mrs. MALONEY. In other words, you don't know who is doing the trading in OATS, right?

Mr. GELLASCH. You don't know who is doing the trading.

Mrs. MALONEY. OK.

Mr. GELLASCH. That is right. All they can say is whether or not it is principal or not, and so they—you don't know who the beneficial customer is.

Mrs. MALONEY. OK. Going back to the point of Ms. Dolly real quick, she says there is duplication.

So in your view, is the CAT necessary in light of the similarities to OATS? I am talking to you, Mr. Gellasch. Her point is there is too much duplication.

Mr. GELLASCH. Sorry, I—

Mrs. MALONEY. Do you think it is necessary? Is the CAT necessary?

Mr. GELLASCH. One of two things I think is absolutely necessary. What I thought when people started this process of building the Consolidated Audit Trail in 2009, before it was even released, was that you could—the thought was to upgrade OATS: OATS 2.0. And most of the industry thought that was what would happen.

We have gone down a very different path now where we are creating the Consolidated Audit Trail and maybe retiring OATS. But in either outcome it is a critically important and necessary step to understand who is doing the trades in an automated way so that the regulators can actually see, in an automated way, who that is.

Mrs. MALONEY. Thank you.

Chairman HUIZENGA. Gentlelady's time has expired.

With that, the Vice Chairman, Mr. Hultgren, for 5 minutes.

Mr. HULTGREN. Mr. Concannon, just real quick, can't they already get that information off the blue sheets?

Mr. CONCANNON. Yes. To be clear, all the client information is available through blue sheets within 24 hours.

Mr. HULTGREN. Yes. That is what I thought.

Mr. CONCANNON. And there has been a—more of a recent challenge for the regulators because what they are finding is certain traders, professional traders, usually sitting outside this country, are using their family account information to open up accounts to start manipulating markets. So today our regulators are already finding cross-market and cross-account manipulation. Having those

identifiers flow through the CAT is helpful, but the bad actors have already found a way around that.

Mr. HULTGREN. Right.

Mr. Beller, I wonder if I could address to you, your testimony and discussion generally is focused on preventing intrusions into the CAT database and also mitigating data loss in the event of such an intrusion. As you know and as we have talked about, the SROs and the SEC would be able to download data from the CAT into their own systems.

I wondered, how can you protect the data once it has left your database that you have designed? It seems that once it is on another server that it would be susceptible to all the vulnerabilities that your cybersecurity efforts were designed to protect it against once it has left your database there. Wouldn't preventing the downloading of this information greatly reduce the risk of a data breach?

Mr. BELLER. Certainly we cannot control the data once it leaves the system. The Plan does call for the chief information security officer of the Plan processor to review the procedures that the SROs use to protect the data.

We, in our original vision for the CAT and the vision that we are executing on, want to build a system that has as much functionality as possible on the platform so that the SROs can do their work on the platform and not have a great need to remove the data. But the Plan does require them to have the ability to remove the data.

Mr. HULTGREN. Seems like there is an obvious risk there that we need to continue to talk about and figure out.

I am going to wrap up my time with Mr. Concannon and Ms. Dolly. And you have talked about this; Chairman Huizenga brought this up, but just maybe a little bit more. How could unauthorized access of identifiable proprietary transaction data be used for market manipulation if it even could? And wouldn't unauthorized access to identifiable proprietary transaction data run counter to CAT's goal of instilling market confidence?

Mr. CONCANNON. So my biggest concern—and you raised it in your question, and it has nothing to do with PII. It has to do with the proprietary trading information of our members. These are firms who have spent millions of dollars developing just basic market-making code on how their market-making models perform.

There are going to be people, bad actors that want access to that. And they can reverse engineer the information from the data in the database, and then they can trick the market-maker code to do bad things. And they can profit from that.

And we see it every day. There are people that don't have access to the data that are trying to make market-makers lose money, and we are finding that behavior. But if they get access to that unique information it is much easier.

Mr. HULTGREN. Yes.

Ms. Dolly, any last thoughts?

Ms. DOLLY. I don't know if this is manipulation of the market, but it is certainly manipulation of the investor: When access is penetrated what we have seen is that—what we call account takeovers, where bad actors come in and they are able en masse to be

able to collect information that is personally identifiable, and even if it is simply their investing account they can go in and execute orders that would benefit them from a profitability perspective.

Mr. HULTGREN. Yield back the balance of my time to the Chairman.

Chairman HUIZENGA. Gentleman yields back.

With that, the Chair recognizes Mr. Vargas from California for 5 minutes.

Mr. VARGAS. Thank you very much, Mr. Chairman. Appreciate the opportunity.

A question to Mr. Gellasch. You were saying that you expected there would be an OATS 2.0 as opposed to a—that we would go down this different avenue that we now have. So I would ask you this, then: Why is it so important that we know who is doing the trading? Is it because of—if you could expand a little bit on that, is it because of market manipulation, or because of data breach? Why is that?

Mr. GELLASCH. Yes, and I actually—this was something that Mr. Concannon also briefly touched upon. If you have the opportunity I encourage you to ask your staff, or you personally, to go speak with the market surveillance folks at FINRA. It is an incredibly impressive team that oversees the markets.

And one of the most disturbing things I learned when I was a securities defense lawyer and had a number of firms as our clients, and I focused on trading cases—market manipulation cases, in fact. And one of the things that was really disturbing to me when I went to work for the government was I met with Tom Gira and the FINRA folks who are still there and they were able to show me how they—the trails went cold.

They could see abusive trading; they could see manipulations. And the trails disappeared. And increasingly so if you were to have those conversations or your staff were today, they would disappear often in China, or Eastern Europe, or other places outside of the United States.

And one of the things that is very, very, very hard to do is to track trading across markets. So they have gotten very, very good at trying to reverse engineer patterns. They have hundreds of them trying to reverse engineer patterns to basically solve a problem that would be readily solved and much more likely and consistently solved if they actually knew who was doing the trading in the first place.

Mr. VARGAS. Would anyone else like to comment on that?

Mr. CONCANNON. Yes. Just in terms of the trail going cold, just to clarify—it isn't quite aware of how it works, unfortunately FINRA doesn't have the jurisdiction nor do the exchanges and the other SROs against an individual. And so those cases are passed to the SEC and the SEC then has full jurisdiction to go after individuals that perform manipulation. We have jurisdiction over only our members to prosecute our members.

Trail going cold means there is an individual trader in a foreign jurisdiction trading in our markets doing bad things and it is at the hands of the SEC to go and prosecute that individual. That is very hard for them to do. When they think about all the resources that they have, there are a lot of bigger things for them to go after.

And so trails do go cold, but we have rules in place now that will actually shut off the firm that actually allowed that individual into our market. So there is more detriment now because of some of the rules—recent rules that we have passed, where you lose complete access if you let bad actors into our market.

Mr. VARGAS. Mr. Gellasch, yes, sir?

Mr. GELLASCH. I might respond all of that is fantastic, and the market access rule is the one he is referencing, and others. I think that those are absolutely fantastic developments.

The trouble is, again, in order for those things to happen you have to know that the manipulation is happening, and so when you look at some firms that may have thousands of customers all trading at real time, a lot of these manipulations actually just get lost in the noise, whereas if you are able to identify the individuals or individual firms they wouldn't.

Mr. VARGAS. OK.

Mr. Gellasch, last to you, there are some people that believe that because of data breaches that the opponents of CAT say that things should be slowed down. Could you comment on that? Because we have known now for a long time there have been cybersecurity problems since 2010, I believe.

Mr. GELLASCH. Yes. Cybersecurity has actually been a significant concern for the years even before the Consolidated Audit Trail.

And since then we—most recently we are certainly focused on Equifax and the SEC's decades-old EDGAR system, but we can go back in time, right? We can go back in time to things like Target with credit cards, or we can go back to JPMorgan Chase, or we can go back to a number of other very large—some of the most sophisticated firms in the world who, by the way, also have extremely valuable databases.

Now, let's be clear: Is a database that may be worth billions of dollars and tens of billions of dollars to someone who wants to do bad things a bigger target than one that is worth maybe several billion dollars? The answer is yes.

In both instances however, there is a pretty strong incentive and a pretty significant data risk associated with that. I think that those have existed now for years.

Frankly, that is part of the reason why I find it interesting that I am on the panel defending the standards, protocols, requirements, and contract requirements that the SROs built into the Plan when they designed it along with Thesys and other data security experts, but that is where we are. They actually were very, very good about this and they have been for years, and they still are.

What is interesting to me is to understand that they selected Thesys just a few months ago and it was only over the last several years—

Chairman HUIZENGA. Gentleman's time has expired.

Mr. GELLASCH. —As this was evolving that those requirements were being established.

Mr. VARGAS. My time is expired.

Thank you, Mr. Chairman.

Chairman HUIZENGA. Gentleman's time has expired.

With that, gentleman from Ohio is recognized for 5 minutes.

Mr. DAVIDSON. Thank you, Chairman.

And thank you all for continuing to answer some good questions here so we can solve this problem, or at least be confident that it is solved.

Mr. Beller, under the CAT NMS Plan, who verifies that Thesys is complying with all relevant cybersecurity requirements?

Mr. BELLER. The chief information security officer of Thesys CAT is also a fiduciary of CAT NMS, LLC, which is the consortium put together by the SROs. That duty, that fiduciary duty, overrides all other duties of that individual, and his or her activities are overseen by the operating committee of CAT NMS, LLC.

Mr. DAVIDSON. Thank you for that.

And so when I look at that piece, one of the other pieces is—maybe, Mr. Concannon, you could answer—is what cybersecurity requirements the SEC itself or other users of the database obligated to implement in order to comply with the cybersecurity standards for access?

Mr. CONCANNON. You are putting me in a difficult spot to suggest that the SEC has to have a higher standard of cybersecurity access.

I will use Chairman Clayton's statement. He actually committed to not have anyone at the SEC access the CAT data until he was comfortable that they had the highest standard of cybersecurity protection, because under the CAT Plan the SEC has requested to have almost 1,000 users have access to the database through portals that will be provided by Thesys.

So when we think about the complexity of this system it is not just putting data in a database that people have surveillance access, there are actual people, users, that will have access to this database sitting in front of a terminal in an office.

Mr. DAVIDSON. Yes. Thank you for that. And that goes to one of the inpoint security pieces that is so critical for any access control.

And so one of the things, aside from great protocols and a lot of forethought given to it for years, and including in the specs that were released to even solicit bid references to cybersecurity, some voids still remain. And a lot of the question keeps coming back to personally identifiable information, and I get the tradeoff: If you don't know the beneficial owner, what is to prevent any one person from launching a dozen LLCs and, I know a dozen LLCs but you don't connect the dots.

So you have to know some level of personally identifiable information. But, Mr. Beller you made reference to the fact that when this initially launches you don't have that. So I guess where is that balance supposed to be struck right now? We have talked around the issue a lot: What are the things that could be done while you are going live with the system before you begin to collect PII?

Mr. BELLER. Yes. So the reason there isn't PII in the initial phase of the CAT is because the reporters are just the exchanges themselves, and they are responsible—they receive incoming orders on the basis of what member of their exchanger is sending to them. So that is not—the number of members involved is very, very small relative to the hundreds of millions of personally identifiable information that we are talking about.

In the second phase, where other broker dealers who are customer-carrying broker dealers come in, that is when the PII comes in.

Mr. DAVIDSON. Got it.

Mr. BELLER. And that does give a little bit—that gives extra time that is involved in the building of the CAT before the PII comes in.

Mr. DAVIDSON. So delaying that phase could accomplish a lot, if necessary. Frankly, it can be happening in parallel, not just sequentially.

Ms. Dolly, you mentioned we are just now getting the technical specs. There is a lot of work left to be done.

If there is a change in PII as you are in the process of doing said work, how big of a deal is that for compliance?

Ms. DOLLY. From an implementation perspective?

Mr. DAVIDSON. Correct.

Ms. DOLLY. Yes. We haven't actually gotten to the point where we have the specifications, so getting different specifications would not further delay it. So if we were able to figure out a way to remove PII, even if it was to put some other unique identifier for the client in there so that it was not exposing us, I don't think it would add anything to the implementation plan.

And I also wanted to thank you for sponsoring this consideration of delaying it because we do have to get this right and I think an open and robust dialog around it will help us to get there.

Mr. DAVIDSON. Thank you all.

My time has expired. I yield, Mr. Chairman.

Chairman HUIZENGA. Gentleman's time has expired.

And the gentleman from California, recognized.

Mr. SHERMAN. Ms. Dolly, I am told that there are 58 billion records a day that we transfer to CAT. Does that mean there are 58 billion stock and bond transactions every day?

Ms. DOLLY. No, those are elements of the transaction. So it is the order execution, it is the order details, it is quotes, it is—

Mr. SHERMAN. So if I order my name, my address, the date, OK. How many transactions a day are we talking about being reported? Does any witness know?

Mr. CONCANNON. So the bigger number is the quote and order information in our markets. So if you think about an ETF (exchange-traded fund), a very liquid ETF, there are thousands of quotes per second in an ETF. These are—

Mr. SHERMAN. May not be a transaction; may just be an offer to buy or an offer to sell.

Mr. CONCANNON. Exactly. No transaction, but many, many quotes.

Mr. SHERMAN. So we are only dealing with a few billion transactions every—

Mr. CONCANNON. Yes.

Mr. SHERMAN. Glad our universe is small enough for us to deal with it.

Let's see. Mr. Gellasch, CAT was created pursuant to the National Market System, NMS Plan. Could you describe how the NMS Plan model differs from traditional rulemaking? I know SIFMA has raised concerns that it allows the SROs and the ex-

changes and FINRA to minimize input from other industry participants.

What do you think of how NMS is structured?

Mr. GELLASCH. Yes. Thank you for the question.

I would argue the NMS Plan structure is a vestige of history that has long since passed its usable life. In the 1970's, it was created with the idea of nonprofit SROs. We now have for-profit SROs, and when you have a set of for-profit regulators essentially empowered by the SEC to set the rules for market participants and set the cost structure for market participants, some of whom are their direct competitors, including broker dealers, other execution venues, you have a problem.

So what we have is essentially, we have created a system where a handful of market participants—Mr. Concannon being one of them—essentially are able to dictate the terms of a significant amount not of just market structure but of costs to market participants. And if they agree, for example, with the goals of that—of what they have been tasked to do then they can execute that. However, they can also frustrate that, and that is how we see situations like the Tick Pilot or the Consolidated Audit Trail, I think, drag on for years.

Mr. SHERMAN. Let me shift your attention a bit.

If we delay we might do a better job and we will delay the costs. But if we delay we get the system later.

Today the markets are operating. We don't have a CAT. What is the problem?

Mr. GELLASCH. Yes. I think that is—at some point we have boiled the frog when it comes to the CAT. It has been now 7–1/2 years, and as every major—

Mr. SHERMAN. What abuses are occurring—

Mr. GELLASCH. So this is—

Mr. SHERMAN. —Because we don't have a CAT?

Mr. GELLASCH. Right. So market manipulations are occurring.

I don't know when the next Navinder Sarao is going to cause the next flash crash, or significantly cause the next flash crash. But I do know that prior to him causing the next flash crash he was involved in a number of, what we later found out were, market manipulations.

So once the whistleblower identified the bad actor and regulators were able to use the blue sheet process and others, they were able to reconstruct that he was someone that they could have identified and stopped a long time earlier.

So the answer is I don't know what we are—we are now in a—

Mr. SHERMAN. So it is not that the present system will catch it—the problem too late to stop it; the present system may never tell you that you had a problem.

Mr. GELLASCH. Both.

Mr. SHERMAN. Both.

Mr. Concannon?

Mr. CONCANNON. I would vehemently disagree.

The current system does capture manipulation. We capture it every day. We have hundreds of alerts, if not thousands of alerts, across all of the SROs and across FINRA, which is our not-for-profit regulator that sits at the middle of our markets.

So we are capturing manipulation every day. We are well protected while we build a system that needs to be perfect. We can't make a mistake in building CAT. It has to be perfect.

Mr. SHERMAN. I know my time is expired. I would just say that with the rules of the Cayman Islands, Switzerland, some other places, I would be surprised if you will ever know the beneficial ownership of some of the entities doing the trades.

I yield back.

Chairman HUIZENGA. Gentleman's time has expired.

With that, I would like to thank our witnesses for sticking around, doing two rounds of questioning. I think this was very, very helpful. I think we made some progress.

The Chair notes that some Members may have additional questions for this panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to these witnesses and to place their responses in the record. Also, without objection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

And with that, our hearing is adjourned.

[Whereupon, at 12:04 p.m., the subcommittee was adjourned.]

A P P E N D I X

November 30, 2017

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.

Testimony of Chris Concannon

President and Chief Operating Officer

Cboe Global Markets, Inc.

Before the Subcommittee on Capital Markets, Securities, and Investment

Thursday, November 30, 2017

Mr. Chairman and members of the Subcommittee, I am Chris Concannon, President and Chief Operating Officer of Cboe Global Markets, Inc. I have over 20 years of experience as an exchange executive, trading firm executive, and a regulator. I served as CEO of Bats Global Markets, Inc. prior to its combination with CBOE Holdings earlier this year. Our company's new name is Cboe Global Markets ("Cboe"). We are one of the world's largest exchange holding companies. Cboe operates six national securities exchanges consisting of four options markets, including the largest U.S. options exchange, and four equity markets, comprising the second-largest U.S. stock exchange operator. Cboe also operates a U.S. futures exchange, the largest European exchange and a foreign exchange platform. I would like to thank the Subcommittee for inviting me to testify today regarding the Consolidated Audit Trail ("CAT").

In August 2012, the Securities and Exchange Commission ("Commission") adopted Rule 613 under the Securities Exchange Act of 1934 to require national securities exchanges and FINRA to submit a national market system plan to create, implement, and maintain a consolidated order tracking system with respect to the trading of NMS securities, which would capture customer and order event information for orders in NMS securities, across all markets, from the time of order inception through routing, cancellation, modification, or execution. The primary rationale behind the establishment of the CAT was to improve upon and consolidate a regulatory framework

supported by disparate audit trail sources to allow for superior market surveillance, investigation, enforcement, and market reconstructions and analyses.

The SROs initially submitted the CAT Plan to the SEC on September 30, 2014. The Commission approved the CAT Plan, as amended, on November 15, 2016. For several years, including during the last year since that approval, the 20-plus SROs party to the CAT Plan have been working diligently on execution of the CAT project. This has entailed, among other things, a comprehensive bidding process to determine the operator of the CAT Plan processor, selection of the CAT Plan processor, negotiation of a contract with the chosen entity, and commencement of the building of the CAT itself. Accomplishing each of these steps is no small feat given that there are over 20 SROs operated by multiple holding companies that must effectively agree every step of the way.

Per the milestones set forth in Rule 613, the Plan processor was selected in January of this year, and the development of specific details in the CAT design framework, including data submission layouts and, in particular, security protocols, has taken some time. Pursuant to Rule 613, the phase one implementation of the CAT reporting process (requiring SROs to report data to the repository) was due to go live on November 15th of this year (which is one year after the original CAT Plan approval). However, work on the CAT is not complete. In planning for the completion of the CAT project, the SROs have taken into account the heightened need to maximize the CAT repository's security planning and protocols given the recent proliferation of data breaches that have occurred around the globe, and the tremendously vast amount and highly sensitive nature of the data that will be stored in the CAT repository. The SROs have also thoroughly consulted and forecasted with the CAT Plan processor, and considered ample feedback

from industry participants on deliverables and expectations. The resulting revised schedule takes into account these factors as well as forecasting based on the detailed framework plans.

We continue to work in good faith towards expeditiously completing the CAT project. Indeed, our efforts on the CAT have been substantial. By way of example, consider the following figures:

- To date, Cboe has spent over $10 million on CAT.
- Cboe has over a dozen employees meaningfully involved in the CAT project on a regular basis.
- Cboe has spent approximately 30,000 man-hours on CAT to date.

I commend the Subcommittee for conducting this hearing and for continuing to focus on ensuring that the CAT is developed efficiently and effectively while insisting that data security around the CAT is vigorous and robust. I am concerned about the risks associated with storing PII in the CAT database, and can assure you that Cboe is very interested in working with the Commission and other stakeholders on exploring whether and/or to what extent PII is a necessary component of CAT, and, if so, applicable security protocols. While I recognize there are benefits to be derived from the CAT, I also would like to point out that costs associated with projects like this are ultimately funded by investors. As such, ongoing cost-benefit and risk-benefit analyses are critical to determine whether improvements to the audit trail and the accompanying regulatory benefits outweigh the costs and risks associated with this endeavor.

We are committed to building the CAT as currently contemplated, and remain committed to maintaining a strong regulatory program; however, we are also willing to revisit these issues with the Committee, the Commission and others stakeholders. While the CAT build-out is

completed, please let there be no doubt that our existing surveillance and regulatory framework is robust, and our markets are well-protected. Indeed, the U.S. financial markets are the most efficient and liquid markets in the world, and the regulatory framework around those markets, led by the SEC, is second to none. The CAT will be an important component of that framework and we look forward to the completion of a smart, secure and efficient CAT system. Thank you for the opportunity to appear before you today, and I am happy to answer any questions you may have.

Written Testimony of

Lisa Dolly, Chief Executive Officer, Pershing

on behalf of the

Securities Industry and Financial Markets Association

before the U.S. House of Representatives

Committee on Financial Services

Subcommittee on Capital Markets, Securities, and Investment

Hearing entitled "Implementation and Cybersecurity Protocols of the Consolidated Audit Trail"

November 30, 2017

Chairman Huizenga, Ranking Member Maloney, and distinguished members of the Subcommittee, thank you for providing me the opportunity to testify today on behalf of the Securities Industry and Financial Markets Association ("SIFMA")[1] and to share our views on the implementation of the Consolidated Audit Trail ("CAT"). SIFMA represents a broad range of financial services firms active in the capital markets and is dedicated to promoting investor opportunity, access to capital, and an efficient market system that stimulates economic growth and job creation. This Subcommittee's 's review of the challenges investors, broker-dealers, exchanges, and regulators face with the CAT is incredibly important and timely. While there may indeed be a great value in a workable, secure CAT, the implementation issues we and others have identified over the past few months, and indeed the past few years, remain largely unaddressed or incomplete to the potential detriment of tens of millions of investors.

A History of the Consolidated Audit Trail

In 2012, the Securities and Exchange Commission ("SEC") adopted Rule 613 of Regulation National Market System ("NMS") under the Securities Exchange Act of 1934 ("Exchange Act"). Rule 613 directed the national securities exchanges and FINRA (together, the "SROs") to develop an NMS Plan to create the CAT. When the CAT is fully operational, it will capture all customer and order event information for orders in equity securities and listed options from the time of order inception through execution. With this information, the CAT will be the world's largest data repository for securities transactions, and one of the world largest databases of any type. Every day the system will take in 58 billion records – orders, executions and quotes for the equities and options markets – and will maintain data on over 100 million institutional and retail accounts and their unique customer identifying information. As currently envisioned by the SROs, all of this data would accessible by thousands of users. The CAT data would grow to an estimated 21 petabytes within 5 years – the equivalent of over ten times the content of all U.S. academic research libraries, all in a single database. As it is currently planned, the CAT will contain a significant amount of sensitive information – both personally identifiable information ("PII") of individual customers (such as social security numbers, addresses, and dates of birth) and identifiable proprietary transaction data that could potentially be reverse engineered and used for market manipulation.

SIFMA has supported the development of the CAT and believes that, if successfully designed and implemented, the CAT could be a critical aspect of market infrastructure and regulation. However, the current state of CAT implementation has left some major issues unaddressed. Today, we will focus on three key aspects of CAT implementation that need to be addressed:

- Sensitive Information and Data Security
- Operational and Implementation Hurdles
- The SROs' CAT Funding Model

[1] SIFMA is the voice of the U.S. securities industry. We represent the broker-dealers, banks and asset managers whose nearly 1 million employees provide access to the capital markets, raising over $2.5 trillion for businesses and municipalities in the U.S., serving clients with over $18.5 trillion in assets and managing more than $67 trillion in assets for individual and institutional clients including mutual funds and retirement plans. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit http://www.sifma.org.

Ultimately, these issues result from a flawed process for developing the CAT. We will provide some examples of the problems with the process and ideas for solutions.

Sensitive Information and Data Security

Despite the unprecedented amount of data being stored in the central repository, and the associated data protection concerns, the CAT technical specifications that have been released to date include alarmingly few details on data security and protection. As the SROs' initial reporting deadline approached and passed, Thesys – the CAT system processor – had not hired a Chief Information Security Officer ("CISO") to review the data security policies and procedures to ensure protection of the CAT data, as required by the CAT NMS Plan.

At the outset, the SEC and the SROs should examine the cost and benefit of collecting customer PII and identifiable proprietary trading data in the CAT. Collecting that information in the CAT creates tremendous risk in the event of a breach. As such, the SEC and the SROs should have to make the case that the CAT's collection, storage, and use of PII and identifiable proprietary trading information is required for effective surveillance. It should be possible to build the CAT in a manner that would allow the SEC and the SROs to make follow-up requests for identifying information on an as-needed basis.

If sensitive identifying information is going to be included in the CAT, then the SEC and the SROs must provide much better assurances on data security than they have so far. Financial firms and regulatory agencies share a common goal in securing and protecting the data entrusted to them by clients and financial institutions. However, the current CAT development plan raises serious concerns around data protection and the ability to confidently secure the critical information it will contain. In particular, the draft CAT technical specifications that have been released to date include alarmingly few details on data security and protection. Put simply, we agree with Commissioner Michael S. Piwowar that, "the need for robust protection of customer data trumps all the other issues that have been raised."[2] Keeping CAT Data secure and confidential is of primary importance not only to the efficacy of the system itself, but also to the confidence of market participants.[3] It is therefore critical that the CAT be held to the highest security standards. As the SEC and SROs prepare to move forward with the implementation of the CAT, it is critical that the CAT does not introduce new data protection risks. The SROs and Thesys should leverage the industry expertise to ensure the CAT's data security meets the highest industry standards.

Beyond the fundamental questions of whether this sensitive information is necessary for the CAT to be successful and whether that information will be secure is the question of usage of that information. CAT would allow all of the 22 SROs and the SEC to download any or all bulk data from CAT into their own systems. In fact, the NMS Plan stipulates that Thesys design CAT to accommodate up to 3,000 individual users. As a result, the protection of the data depends not only on the security of the CAT system but also on the security of each of the SROs plus the SEC, all of which will have downloadable access to all CAT data. The first step to strengthen data security should be an amendment to the CAT NMS Plan that prohibits downloading data from the CAT. Rather, SIFMA suggests a sandbox approach – under which the SEC and the SROs access data

[2] Statement on the Joint Industry Plan on the Consolidated Audit Trail ("CAT"), Public Statement by SEC Commissioner Michael S. Piwowar (Nov. 15, 2016).

[3] *See* SIFMA Statement on CAT Plan Proposed by SEC (Apr. 27, 2016)); *available at* http://www.sifma.org/newsroom/2016/sifma-statement-on-cat-plan-proposed-by-sec/.

from within the CAT data security perimeter so that no data ever leaves that perimeter. This solution would provide the SEC and the SROs with access to perform surveillance in a secure and confidential manner, without subjecting that data to the risk of each SRO's security systems.

Implementation and Operational Hurdles

From the time of its adoption, Rule 613 has set an overly aggressive implementation timeline for the CAT. Under Rule 613, the SROs were required to begin reporting to CAT on November 15th of this year, only 12 months after the SEC approved the CAT NMS Plan. Large broker-dealers are scheduled to begin reporting 12 months after the SROs, while the remaining small broker-dealers are set to begin CAT reporting 12 months after that. That schedule was never practical, and it was incorporated into Rule 613 without any consideration of the actual time it would take to build such a complicated system – both in terms of completing the technical specifications and conducting robust testing.

Adding to the burden, the CAT NMS Plan set out a flawed timeline for developing the technical specifications necessary for broker-dealer implementation. The Plan provides that final specifications for broker-dealer trading information were to be complete on November 15th of this year. Even on schedule, that would have left only 12 months between final specifications and implementation, and as we noted previously the SROs have missed the deadline to provide final specifications. Moreover, the final specifications for customer information are still scheduled for May 15, 2018 – only six months before the reporting deadline. The lack of feasibility of these timeframes is evidenced by the fact that the SROs submitted a last-minute request to the SEC to postpone both SRO and broker-dealer reporting. The SROs missed their own reporting deadline and the deadline to provide final specifications when the SEC failed to grant the request.

Clearly, the implementation schedule must be revisited. There must be appropriate time allocated to reassess and tailor the implementation schedules and milestones in the NMS Plan to make the rollout of the CAT as efficient as possible. Implementation of CAT should include sufficient lead time to enable all reporting firms, including smaller broker-dealers, to establish the internal structure, technical expertise, systems, and contractual arrangements necessary to implement two distinct sets of technical specifications and begin reporting. A reasonable timeframe can only be determined once Thesys has published all the final technical specifications for the reporting of both trading and customer information. The implementation schedule must be designed to provide iterative testing and communications between broker-dealers and the CAT Processor in terms of developing and executing final system specifications and to promptly resolve any open issues.

It is evident that the SROs require assistance with the technical specifications for broker-dealers. The finalization of detailed technical specifications is critical, and they should be released in draft versions to allow for robust iterative feedback from broker-dealers. Once the specifications are finalized, broker-dealers should be given a minimum of twelve months to complete the requirements gathering and analysis, internal design and development, and testing based upon these final specifications. Mandatory testing should follow, and include coordinated industry tests involving industry members, the SROs, and Thesys to allow for the validation of CAT reports, exception reporting and processing, and inter-firm linkages between firms and the exchanges. This should be followed by a trial, phased implementation approach with equities in the first tranche, allowing the industry time to perform error corrections and linkage validations.

This methodology will provide firms with an opportunity to reduce error rates during the trial period prior to onboarding to the CAT. In addition, it is imperative that that the SROs and the SEC work with Thesys during each of the specification development processes to ensure that all necessary data fields are included in the CAT technical specs to facilitate a timely retirement of redundant reporting systems.

SROs' CAT Funding Model

The SROs have proposed a funding model for CAT that would impose a vast majority of the building and operational costs on broker-dealers, without providing any real justification or information about their current receipt and use of regulatory fees from broker-dealers. This approach to the funding model is particularly troublesome given that the SROs include the for-profit exchanges, which have built the funding model to benefit their own commercial interests at the expense of the broker-dealers they regulate and compete with.

What is the cost. The SEC estimates that it will cost $92 million to build the CAT central repository and $135 million annually to operate it, and the SROs have proposed to charge a fee to broker-dealers to defray those costs. In addition to an SRO fee, the SEC estimates $2.1 billion in overall industry-wide implementation costs for the CAT reporting and $1.5 billion in ongoing annual operational costs. The SEC estimates that total annual cost of the Plan would be $1.7 billion, of which $1.5 billion, or 88%, is allocated to broker-dealers to meet their data reporting requirements. This raises the following initial threshold question: should broker-dealers, which are already burdened with 88% of the costs of the CAT, be responsible for funding any portion of the costs to build and operate the CAT itself?

Problems with the cost distribution. SIFMA has repeatedly raised CAT funding as a critical issue, and the funding proposal in the CAT NMS Plan should have been the product of collaboration between the SROs and the broker-dealers. However, despite the obvious conflict of interest, the SROs created a funding model with no input from broker-dealers. SIFMA and other industry participants repeatedly requested the opportunity to work with the SROs on a reasonable funding model, but the SROs refused those requests and instead attempted to impose a fee structure that was most beneficial to their interests. Moreover, the SROs filed the CAT fee proposals with the SEC for immediate effectiveness without soliciting public comments. If the SROs had engaged in a good faith effort to solicit input on the proposals, then it is possible an appropriate solution could have been achieved. Instead, however, the SROs decided to impose the vast majority of costs and expenses of building and operating the CAT on broker-dealers without considering industry concerns.

The proposals provide insufficient financial details on why broker-dealers, which would be tasked with paying nearly all of the costs and expenses of the CAT, should be subject to any CAT fees, especially in light of the SROs' existing regulatory revenue. In that regard, there should be no new fee for the CAT until market participants are provided with a complete picture as to how regulatory fees are currently allocated, how the CAT fee fits into the existing regulatory framework, and why assessing broker-dealers an additive regulatory fee is necessary to fund the creation and operation of the CAT.

Moreover, the SROs' proposals did not satisfy the requirements of the Exchange Act because they were not an equitable allocation of reasonable fees under Section 6(b)(4) or Section

15A(b)(5). The SROs stated outright in the proposal that they have structured the fee schedule with a goal of imposing 75% of the total CAT costs to broker-dealers. On its face, this is not an equitable allocation of fees for a system that is being created by and for the benefit of the Plan Participants. The only justification provided by the Plan Participants is that the 75%/25% division was chosen to maintain "comparability" across the funding model, keeping in view that comparability should consider affiliations among or between CAT reporters.[4]

SIFMA takes particular exception to the SROs' proposal to use the funding authority to recover their legal and consulting costs in developing the Plan. Specifically, the proposed CAT fees would include reimbursement to the Participants of third-party support fees (historical legal fees, consulting fees, and audit fees), operational reserve, and insurance costs. Those costs are the responsibility of the SROs, which will own and operate the system. There is absolutely no justification for the SROs' proposal that broker-dealers should be responsible for any of the legal and consulting costs that the SROs incurred in developing the Plan. Any CAT fee that the SROs do charge should be determined by an independent third party so that it is transparent and can be determined by an objective standard to be equitable and reasonable.

The SEC shared SIFMA's concerns and suspended the fees while considering whether to approve or disapprove the proposals. In the meantime, the SROs have responded to some of the industry's concerns about the applicability of the fees and amended the proposals. However, the SROs' funding model for CAT continues to be based on imposing 75% of the total costs to broker-dealers.

Issues with the CAT Development Process

In adopting Rule 613, the SEC envisioned close collaboration between the SROs and broker-dealers, with the SROs benefiting from "draw[ing] on the knowledge and experience of [their] members."[5] And in the NMS Plan governing the CAT, the SROs discuss at length their claims of incorporating broker-dealer feedback. These visions are not reality, however, as the SROs largely developed the CAT among themselves and were not open to broker-dealer input on key policy issues. That lack of meaningful collaboration with the industry has led to some untenable proposals that should be of concern to policymakers and the investing public alike. For example:

- The SROs have proposed and utilized a governance structure for CAT that follows the same flawed model that has been used in other NMS Plans, with no meaningful representation by broker-dealers or asset managers. If the SROs had worked with industry members on this issue, we could have developed a workable governance model that avoided the mistakes of the past and potentially would have gotten the CAT up and running more quickly.
- The SROs have proposed a schedule for elimination of systems under which duplicative systems such as the FINRA's Order Audit Trail System ("OATS") could run in parallel with the CAT for years to come with no real sunset date. If the SROs had worked with the broker-dealers on this issue, we could have developed a more practical schedule to eliminate systems within months of CAT becoming operational, reducing cost to all participants by streamlining largely duplicative systems.

[4] *See* Securities Exchange Act Release No. 80710 (May 17, 2017), 82 FR 23639, 23648 (May 23, 2017).
[5] Consolidated Audit Trail, Securities Exchange Act Release No. 67457, at 245 (Jul. 18, 2012).

- The SROs have proposed a funding model for CAT that would impose a vast majority of the building and operational costs to broker-dealers, without providing any real justification or providing any information about their current receipt and use of regulatory fees from broker-dealers. The SEC has agreed with SIFMA and has instructed the SROs to develop a more appropriate funding model. If the SROs had worked with the broker-dealers on this issue or prioritized greater transparency on cost and funding issues, we could have developed a reasonable funding model supported by evidence and analysis well in advance of the CAT going live.

And now, the same exchanges that ran the development process to the exclusion of industry participants are complaining about the state of the development process. Given the ambitious scope of a system like the CAT, industry participants should be active participants in the CAT's ongoing development, rather than having only a limited opportunity to view and comment on proposals that the SROs separately develop with Thesys, the CAT proccessor. SIFMA's member firms have unique expertise and insight that strongly complement that of the SROs while filling in the SROs' expertise gaps on topics such as the details of broker-dealer trading flows. In the absence of any real collaboration on this project, we find ourselves now with the SROs not fulfilling a key reporting deadline of its own – November 15th of this year – and failing to provide the broker-dealer community with the final reporting specifications they were supposed to receive on that same day. Going forward, establishing a true collaboration among industry participants, the SROs, and Thesys will provide the opportunity for the CAT to be informed by the insights and interests of all the affected market participants at a time when they can be readily incorporated without delaying or impeding a successful CAT construction and implementation. There is still time to get this right.

Conclusion

The development and implementation of the CAT have been a disaster. The broker-dealers responsible for reporting to CAT are collectively faced with heightened data security risk, a problematic implementation schedule that is severely behind schedule, and an inequitable funding method that shifts an unjust proportion of costs to broker-dealers. All Americans should be concerned with the unprecedented amount of data that will be reported to CAT, particularly the PII and other sensitive information, and need to ensure the system can adequately protect the data prior to the implementation of CAT. The SEC should reevaluate the need to include customer PII and identifiable proprietary transaction information in the CAT considering the tremendous risks and costs the inclusion introduces. To make the CAT as efficient as possible, the SROs should focus on developing prescribed technical specifications rather than following arbitrary timeframes in the rule. With the SROs' financial interest in defraying most of the costs to broker-dealers, we need to review the funding of the CAT to ensure the exchanges meet their regulatory responsibility as SROs. We appreciate the interest of this Committee in reviewing the CAT and look forward to working with you on this important task.

Testimony of Tyler Gellasch, Executive Director of the Healthy Markets Association

Hearing on *Implementation and Cybersecurity Protocols on the Consolidated Audit Trail*
Before the House Financial Services Committee, Subcommittee on Capital Markets, Securities and Investment

November 30, 2017

Chairman Huizenga, Ranking Member Maloney, and other members of the Subcommittee, thank you for holding this hearing, and for offering me the opportunity to appear before you today.

The Consolidated Audit Trail ("Audit Trail") will be a critical tool for regulators to understand exactly how our capital markets work. But after more than seven and a half years of planning and building, we are still years away from it realizing its potential.

Unquestionably, the design, building, and utilization of the Audit Trail are complex and costly. There are also risks, including both security risks and the risk that this will be just a massive waste of resources. In recent days, many opponents to the creation of the Audit Trail have chosen to focus on some of these risks, without regard to how those risks are being managed and without regard to the benefits of having an Audit Trail.

I would like to share with you five key thoughts today.

- First, the Audit Trail is incredibly important, and long overdue.
- Second, the Audit Trail is not unique in the security and implementation challenges it poses, and the self regulatory organizations and plan processor have spent years ensuring that they meet industry standards and best practices in dealing with those challenges.
- Third, the tortured history of the Audit Trail demonstrates how outsourcing a key government responsibility to a group of for-profit entities easily frustrates important public policy objectives.
- Fourth, the Audit Trail should be implemented and enhanced, including through the addition of futures market data and legal entity identifiers, as well as with refined precision without delay.
- Fifth, the NMS Plan model being used to develop and implement the CAT is deeply flawed, and should be dramatically revised or eliminated.

In the pages that follow, I'll walk through what the Audit Trail is and why it is needed. I'll explore why it doesn't already exist. Finally, I will offer my suggestions as to what Congress and the SEC should do now.

About Healthy Markets

The Healthy Markets Association is an investor-focused, not-for-profit coalition working to educate market participants and promote data-driven reforms to market structure challenges.[1] Our members, who range from a few billion to hundreds of billions of dollars in assets under management, have come together behind one basic principle: Informed investors and policymakers are essential for healthy capital markets.

Since our launch in September 2015, we have become a leading voice for investors in the market structure debates.[2] For more information about Healthy Markets, please see our website at healthymarkets.org.

What is the Consolidated Audit Trail and Why Do We Need It?

In many respects, the Audit Trail will be, when finally implemented, a fraction of what most lay-people would probably think the government already has--a view of what's going on in the markets.

What most lay people don't know, but is widely understood within the financial services industry, is that the oversight of our capital markets is largely disjointed. Historically, as exchanges and different trading venues formed and evolved, they each took responsibility for overseeing trading on their markets. As a result, a disparate framework of audit trail systems has emerged--each of which is focused on the priorities of the responsible regulator.

At the same time, many market participants have built systems to seamlessly view and trade across different venues and different asset classes overseen by different regulators.

---

[1] Prior to joining Healthy Markets as its first Executive Director, I served as Senior Counsel in the United States Senate, as well as Counsel to SEC Commissioner Kara M. Stein. Prior to my government service, I practiced law in the field of securities regulation at leading law firms in New York City and Washington, DC. While in the US Senate, I worked as the lead staffer for several Senate hearings and reports related to the US capital markets, including a post-Flash Crash hearing on the stability and integrity of the markets.

[2] For example, Healthy Markets has:

- Drafted dozens of unique reports and analyses regarding market structure and regulatory developments, including our industry-leading monthly publication, "Market Structure Insights";
- Created two industry-leading "due diligence" questionnaires to assist investors and brokers in evaluating order routing practices and ATS risks; and
- Offered significant input on numerous topics to Congress, the Securities and Exchange Commission, the SEC's Equity Market Structure Advisory Committee, and the Treasury Department through dozens of meetings and comment letters.

For example, consider the options available to modern trading firms that think the US stock market looks like a good investment. They may view E-mini futures contracts or options on those contracts, which can be traded on CME. Or they may trade the SPDR S&P 500 ETF (SPY), or the Standard & Poor's 500 Index (SPX). Or they may trade options or swaps on those. Or they may trade any number of individual securities, options, swaps, or futures that may include one or more related or underlying instruments. Further, the financial instruments themselves may be traded on numerous venues. And the legal entities doing the trading may be regulated by several different US regulators, each with its own jurisdiction, priorities, and requirements.

The good news is that market participants have figured this out-- not just in the US, but around the world. If news in Brussels suggests that a major US company is going to have to pay more in taxes than had been disclosed, then market participants will immediately trade and adjust their prices in all of these related financial products. These firms use extremely smart people and some of the most impressive (and fastest) communications technology in the world. They see the capital markets as a complete picture.

Unfortunately, regulators don't have this view. And they certainly don't have consistent rules to address how trading in these various markets interacts. Instead, the regulators have a patchwork of audit trail systems cobbled together from historical accident and necessity. One of the key current systems is FINRA's Order Audit Trail System (OATS).

That system was originally born out of scandal. In 1996, the SEC brought an action against NASD[3] for "serious deficiencies" in its oversight of trading on Nasdaq, including for failure to take adequate steps in response to collusion and price fixing on its market, failure to enforce the firm quote rule, failure to enforce the trade reporting rule, and failure to enforce NASD membership rules.[4] As one of its remedial measures, the NASD began the development of an "enhanced audit trail."[5]

In 1998, the SEC issued an order approving NASD Regulation's proposal to create the enhanced audit trail, which by then had become known at OATS.[6] OATS is currently operated by NASD's successor, the Financial Industry Regulatory Authority (FINRA). Notably, OATS shares many significant characteristics with the current Audit Trail, but is lacking in breadth and depth of clarity. For example, the underlying beneficial owner is typically not reported. Thus, if a market participant trades using different brokers or accounts, the regulators are hard pressed to identify if the trading activity is related.

---

[3] The National Association of Securities Dealers, Inc. was a self-regulatory organization tasked with overseeing the Nasdaq markets, and is the predecessor to the Financial Industry Regulatory Authority (FINRA).

[4] *In the Matter of National Association of Securities Dealers, Inc.*, Exchange Act Rel. No. 34-37538 (Aug. 8, 1996), *available at* https://www.sec.gov/litigation/admin/3437538.txt.

[5] *Report Pursuant to Section 21(a) of the Securities Exchange Act of 1934, Regarding the NASD and the NASDAQ Market*, Sec. and Exch. Comm'n, *available at* https://www.sec.gov/litigation/investreport/nd21a-report.txt.

[6] Various Orders Relating to the Creation of an Order Audit Trail System, Sec. and Exch. Comm'n, (Mar. 6, 1998), *available at*. https://www.sec.gov/rules/sro/nd9756o.htm.

This creates significant shortcomings, and the lack of consolidation creates even more. In many respects, the existing audit trails fail to contain complete, accurate, accessible, and timely enough information to be truly effective regulatory tools.[7] As the SEC has explained:

> Some of these shortcomings are a result of the disparate nature of the systems, which make it impractical, for example, to follow orders through their entire lifecycle as they may be routed, aggregated, re-routed, and disaggregated across multiple markets. The lack of key information in the audit trails that would be useful for regulatory oversight, such as the identity of the customers who originate orders, or even the fact that two sets of orders may have been originated by the same customer, is another shortcoming.[8]

When I joined the US Senate staff in 2009, improving the known deficiencies in tracking orders was one of my priorities. It made no sense to me that private market participants--some of whom were my former clients--had a much more comprehensive view of the markets than the regulators tasked with overseeing them. The SEC staff was interested in working on it, but they also were struggling with a lot of other things at the time, such as digging out from the financial crisis and helping with what would become the Dodd-Frank Act. Not to mention, funding was tight.

That said, the SEC knew that all of the regulators had very large blind spots--most notably, they weren't able to see who was actually trading in any coherent way. In fact, just a few weeks before the Flash Crash, the SEC proposed a large trader reporting system, which was designed to help the SEC identify and obtain "certain baseline trading information about traders that conduct a substantial amount of trading activity."[9] When the SEC finalized its large trader reporting system in 2011, the first paragraph of its introduction began with:

> The Commission's ability to analyze market movements and investigate the causes of market events in an expeditious manner, as well as efficiently conduct investigations of regulated entities and bring and prosecute enforcement matters, is influenced greatly by its ability to promptly and efficiently identify significant market

---

[7] *Consolidated Audit Trail*, Sec. and Exch. Comm'n, Exchange Act Rel. No. 34-67457 (Jul 18, 2012), 77 Fed. Reg. 45722 (Aug. 1, 2012), (CAT Final Rule), *available at* https://www.gpo.gov/fdsys/pkg/FR-2012-08-01/pdf/2012-17918.pdf.

[8] CAT Final Rule.

[9] *Large Trader Reporting System*, Sec. and Exch. Comm'n, Exchange Act Rel. No. 34-61908, 75 Fed. Reg. 21456 (Apr. 23, 2010), *available at* https://www.sec.gov/rules/proposed/2010/34-61908fr.pdf. This system, which was implemented by Rule 13h-1 and Form 13H, requires large traders to get a unique identifier, which they are required to share with their broker-dealers, so that their trading activities across venues can be more readily identified and tracked. *Large Trader Reporting*, Sec. and Exch. Comm'n, Exchange Act Rel. No. 34-64976 (Jul. 27, 2011), 76 Fed. Reg. 46960 (Aug. 3, 2011), (Large Trader Reporting Final Rule), *available at* https://www.sec.gov/rules/final/2011/34-64976fr.pdf.

> participants across equities and options markets and collect uniform data on their trading activity.[10]

The large trader reporting requirement was intended to supplement the existing audit trails, which provide regulators with the identity of the broker-dealers involved. However, if the SEC wants to dig deeper into trading-related activity, then they have to rely on FINRA to engage in a formal request to the broker-dealer to identify the underlying customers, known as the "blue sheet" process.[11] For their parts, the underlying broker-dealers are required to "know your customer," including by collecting key personal identifying information, such as Social Security numbers and Tax Identification numbers.[12] Of course, traders that are not broker-dealers have posed a unique challenge.

This "blue sheet" process is extremely valuable, if regulators already know of the trades, individuals or firms they want to examine. But it is also cumbersome, and often ineffective. Most importantly, it requires the regulator to know what it wants to investigate before starting it. This is a very significant weakness to market surveillance.

FINRA currently oversees the vast majority of market surveillance for the equities and options markets. It has extremely sophisticated "patterns" that screen for potentially abusive trading activity for the vast majority of equities and options exchanges in the US. FINRA's surveillance covers 11 of the 12 active equities exchanges (meaning its cross market program covers over 99.5% of U.S. equity market activity) and it provides regulatory services for all 15 U.S.-based options exchanges (with cross-market surveillance for 10 markets covering approximately 65% of options contract volume).

However, despite this broad coverage, when trading activity is spread across different brokers and venues, it is nearly impossible to detect in any automated way, unless the trading activities exhibit obvious similarities (e.g., they are always with the same counterparties). Thus, despite the best efforts of FINRA and the best systems currently available, without an automated way to link trading activity to the underlying beneficial owners, there is very little chance to identify and stop sophisticated abuses without the assistance of a whistleblower.

For example, assume that one trader opens accounts with seven different broker-dealers and then engages in market manipulations on multiple market venues in equities and options. The regulators would see these as likely unrelated activities (from different broker-dealers), and so no investigation would ensue. Even worse, even if the activities somehow triggered the blue sheet

---

[10] Large Trader Reporting Final Rule, at 46960.

[11] For more information on the Blue Sheet process, see FINRA's Frequently Asked Questions, *available at* http://www.finra.org/industry/blue-sheets.

[12] In 2011, FINRA proposed tying the rollout of the Consolidated Audit Trail to the Large Trader Reporting Rule requirements, which would give it the key beneficial owner information for the traders who pose the vast majority of volume in the securities markets. See Letter from Richard Ketchum, FINRA to Carlo di Florio and Robert Cook, Sec. and Exch. Comm'n, Apr. 6, 2011, *available at* https://www.sec.gov/comments/s7-11-10/s71110-91.pdf (attaching FINRA Blueprint for a Consolidated Audit Trail (CAT)).

process, it's not entirely clear all of the activities would be captured or linked back to the same underlying trader.[13] In reality, this activity is likely only identified if there is a whistleblower. In fact, we only need to look to the Flash Crash to see how this all works (or doesn't).

The Flash Crash of May 6, 2010 was a seminal event for the markets and for our regulators. It demonstrated just how vulnerable--and resilient--our markets can be to dramatic, unexpected shocks.

May 6, 2010 started off like an ordinary day. The European sovereign debt crisis, led by Greece, was weighing on the markets, but there wasn't anything significant to distinguish it from the day before. There was no major news.

Nevertheless, beginning shortly after 2:30 pm EDT, in a matter of just minutes, the market whipsawed over 1000 points. As market participants and regulators watched in panic, the markets dropped nearly 9%, causing over $1 trillion in market capitalization to disappear. Then almost as quickly as it was gone, the markets largely recovered just prior to the markets close.

Almost as bizarrely, the declines appeared to be very uneven. Some Exchange Traded Funds and individual companies' stocks suffered the brunt of the decline, while others were almost completely unchanged. S&P 500 stocks were pummeled. For example, the stock price for Accenture dropped from $41 per share at 2:30pm EDT to one cent at 2:47:53pm.[14] A timeline of the events is below in Figure 1.[15]

---

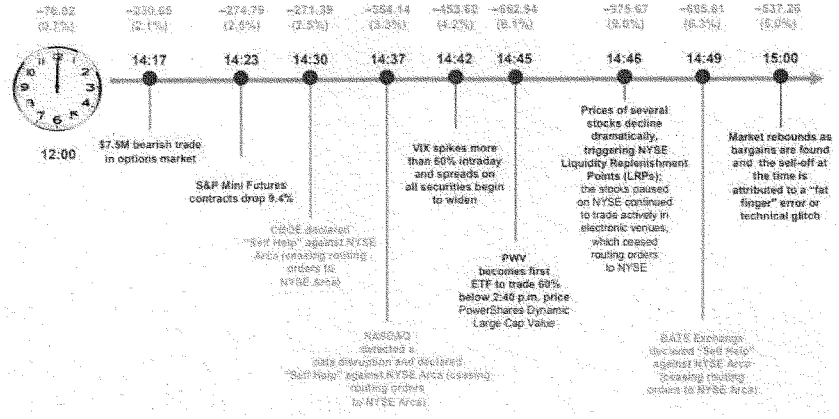
[13] The large trader reporting system is intended to automate some of this process for very large volume traders. However, this still has significant gaps. Large Trader Reporting Final Rule.

[14] Many trades were busted as a result of erroneous pricing including trades in Accenture that were originally executed at fractions of any reasonable pricing. See Matt Phillips, *Accenture's Flash Crash: What's an "Intermarket Sweep Order"*, Wall Street Journal, (May 7, 2010), *available at* https://blogs.wsj.com/marketbeat/2010/05/07/accentures-flash-crash-whats-an-intermarket-sweep-order

[15] Source: Blackrock ViewPoint, Understanding the "Flash Crash", November 2010 *available at* https://www.blackrock.com/corporate/en-ch/literature/whitepaper/understanding-the-flash-crash-nov-2010.pdf

FIGURE 1

Figure 1: May 6 timeline and sequence of events
DJIA change since opening



Sources: Nomura, U.S. Market Microstructure–May 2010; *Wall Street Journal*; BlackRock.

While the markets have experienced precipitous declines during a single day, the May 6, 2010 market event was unique and terrifying.

The Flash Crash touched the very fabric of U.S. market structure, and exacted a huge toll on investor psychology and confidence.[16] But perhaps most troubling was the fact that there was no ability to point to a root cause for the complete evaporation of liquidity and the government regulators were at a loss to explain to the investing public the nature of the vicious market decline.[17] The government took months to figure out what generally happened, and even the Preliminary and Final SEC and CFTC Joint Staff Reports on the subject left a lot of information out.[18] For

[16] For several months after the event, investors withdrew billions each month from their mutual fund holdings. And while some of it could be attributed to the rise in ETFs, not all of the withdrawals were reallocated. This is funding that was "lost" from the US public equity markets. Some of the other impacts on investors were detailed by TD Ameritrade in its report to the CFTC-SEC Committee. See e.g., Statement of Christopher Nagy, TD Ameritrade, before the Joint CFTC-SEC Committee on Emerging Regulatory Issues, (Aug. 11, 2010), *available at* https://www.sec.gov/comments/265-26/265-26-32.pdf. Notably, Nagy has since founded and served as a member of the Board of Directors for the Healthy Markets Association.

[17] See *Preliminary findings Regarding the Market Events of May 6, 2010*, Report of the Staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues, (May 18, 2010), *available at* https://www.sec.gov/sec-cftc-prelimreport.pdf (*Preliminary Joint Staff Flash Crash Report*).

[18] *Preliminary Joint Staff Flash Crash Report*; see also *Findings Regarding the Market Events of May 6, 2010*, Report of the Staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues,

example, the initial reports put significant emphasis on a lone trader misusing a trading algorithm in the futures markets, combined with the actions of high frequency traders.[19] Essentially, trading in a broad-based futures product spilled over to the corresponding broad-based equities product, which then spilled over into individual components. And the futures and options products--which were linked by high-speed traders--were all impacted. This was a useful explanation, but parts of it still didn't make sense to many markets experts.

It wasn't until five years later that we also learned of the role of a single individual trader working from his parents' home in the outskirts of London.[20] Further, that case was not a result of the regulators' ability to detect the wrongdoing, but rather was a result of analysis provided by an outside whistleblower who had analyzed data.[21]

The Commission staff had known that they needed a new way to identify large traders[22] and a new Consolidated Audit Trail before May 6, 2010, but their own lack of knowledge in the aftermath really brought that point home. As the Commission has explained:

> the regulatory data infrastructure on which the SROs and the Commission currently must rely generally is outdated and inadequate to effectively oversee a complex, dispersed, and highly automated national market system. In performing their oversight responsibilities, regulators today must attempt to cobble together disparate data from a variety of existing information systems lacking in completeness, accuracy, accessibility, and/or timeliness—a model that neither supports the efficient aggregation of data from multiple trading venues nor yields the type of complete and accurate market activity data needed for robust market oversight.[23]

I agree.

(Sept. 30. 2010), *available at* https://www.sec.gov/news/studies/2010/marketevents-report.pdf (*Joint Staff Flash Crash Report*).

[19] *Joint Staff Flash Crash Report.*

[20] See, Antoine Gara, *British Trader Navinder Sarao Arrested Over 2010 Flash Crash*, Forbes, Apr. 21, 2015, *available at* https://www.forbes.com/sites/antoinegara/2015/04/21/british-trader-navinder-sarao-arrested-over-2010-flash-crash/#6c1ecb6d2e35.

[21] The trader pleaded guilty to market manipulation in November 2016, more than six years after the Flash Crash itself. *See* Aruna Viswanatha, *'Flash Crash' Trader Navinder Sarao Pleads Guilty to Spoofing*, Wall St. Journal, Nov. 9, 2016, *available at* https://www.wsj.com/articles/flash-crash-trader-navinder-sarao-pleads-guilty-to-spoofing-1478733934.

[22] Large Trader Reporting Final Rule, at 46960 ("Though the large trader rule was proposed before the market events of May 6, 2010, that incident has emphasized the importance of enhancing the Commission's ability to quickly and accurately analyze and investigate major market events, and has highlighted the need for an efficient and effective mechanism for gathering data on the most active market participants.").

[23] CAT Final Rule, at 45723.

Why Don't We Have It Yet?

If the Commission has known it needs a better Audit Trail since 2009, then why doesn't it already exist? After all, when the SEC decided that it wanted more market information after the Flash Crash for study, it sent out a request for proposals, selected a bidder, and had the entire system built within a few years. So what's taken the Consolidated Audit Trail so long?

Essentially, the SEC ceded the vast majority of the responsibility for the development, design, implementation, and maintenance for the Audit Trail to the for-profit exchanges and FINRA. The SEC created a CAT NMS Plan, and then empowered the exchanges and FINRA (the Plan Participants) to do the real work to flesh out the details. At each stage, the SEC asked the Plan Participants to come up with a plan, which the SEC would then deny or approve. And then they would move to the next stage.

There were also significant uncertainties, costs, and conflicts of interest for the very Plan Participants tasked with driving the project forward. Add these together, and it's relatively easy to see how this process was doomed to be slow, conflicted, and inefficient from the beginning.

Slowing Down the CAT: Timeline of Significant Events

The Flash Crash happened on the afternoon of May 6, 2010. Less than three weeks later, on May 26, 2010, the Commission proposed Rule 613 to Regulation NMS.[24] That proposal outlined the creation of a Consolidated Audit Trail, with

> details of the data elements to be collected, to the timing of data transmissions, to specific standards for data formatting. Among its various requirements, the proposed Rule mandated that the NMS plan developed by the SROs must in turn require each SRO and its members to capture and report specified trade, quote, and order activity in all NMS securities to the central repository in real time, across all markets, from order inception through routing, cancellation, modification, and execution. The proposed Rule also mandated that the NMS plan require the creation of unique order identifiers to facilitate the ability of regulators to view cross-market activity, as well as unique customer identifiers to enhance the ability of regulators to reliably and efficiently identify the beneficial owner of the account originating an order or the person exercising

[24] *Consolidated Audit Trail*, Sec. and Exch. Comm'n, Exchange Act Rel. No. 34-62174 (May 26, 2010), 75 Fed. Reg. 32556 (June 8, 2010), *available at* https://www.sec.gov/rules/proposed/2010/34-62174fr.pdf ("Initial CAT Proposing Release").

> investment discretion for the account originating the order, if different from the beneficial owner.[25]

The estimated cost for the creation and implementation of the CAT was $4 billion.[26] Two years and many hearings later,[27] on July 11, 2012, the Commission adopted Rule 613.[28] Rule 613 requires the exchanges and FINRA to plan, implement, and maintain a consolidated audit trail.[29] Put specifically:

> Rule 613 requires the submission of an NMS plan to create, implement, and maintain the first comprehensive audit trail for the U.S. securities markets, which will allow for the prompt and accurate recording of material information about all orders in NMS securities, including the identity of customers, as these orders are generated and then routed throughout the U.S. markets until execution, cancellation, or modification. This information will be consolidated and made readily available to regulators in a uniform electronic format.[30]

Importantly, that final rule did little more than establish the process to create the Audit Trail.[31] After the rule was adopted in 2012, the exchanges and FINRA were required to submit the CAT Plan to the SEC by April 28, 2013.[32]

That didn't happen.

Instead, in February 2013, the exchanges and FINRA declared that they should release a request for proposals (RFP) before attempting to engage in the required economic analysis, including the consideration of alternatives.[33] That month, they requested an exemption from the

---

[25] See CAT Final Rule, at 45723 (explaining the parameters of the Initial CAT Proposing Release).
[26] Initial CAT Proposing Release.
[27] *See, e.g., Examining the Efficiency, Stability, and Integrity of the U.S. Capital Markets*, Joint Hearing of the US Senate Committee on Banking, Housing, and Urban Development, Subcommittee on Securities, Insurance and Investment and the Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations, 111th Cong. (Dec. 8, 2010) ("Reed-Levin Hearing").
[28] CAT Final Rule.
[29] CAT Final Rule.
[30] CAT Final Rule, at 45726.
[31] For example, the Commission changed several elements of the plan (including dropping "real-time" reporting), but then entirely punted on the expected reductions in costs. CAT Final Rule, at 45725-26 (stating that "In light of these changes, the Commission believes that the economic consequences of the consolidated audit trail now will become apparent only over the course of the multi-step process for developing and approving an NMS plan that will govern the creation, implementation, and maintenance of a consolidated audit trail.").
[32] CAT Final Rule.
[33] Letter from Robert Colby, FINRA, to Elizabeth Murphy, Securities and Exchange Comm'n, Feb. 7, 2013, *available at* https://www.sec.gov/rules/exorders/2013/34-69060-letter.pdf.

requirement to file the plan until December 6, 2013,[34] and released a request for proposal soliciting bids to be the CAT Plan processor.[35] The SEC granted the exemption in early March.[36]

The day after the SEC granted that exemption, the exchanges and FINRA hosted a conference for potential bidders outlining the proposal process and requirements.[37] At that conference, the SROs told potential bidders that they would (1) preliminarily select the bidder by July 2013, (2) submit a CAT Plan by December 2013, and (3) select the final bidder "within two months" of the SEC approving the CAT Plan.[38]

Once again, that didn't happen.

Instead, in November 2013, the exchanges and FINRA asked for another temporary exemption from their obligation to submit a CAT Plan.[39] This time, they noted that they had created the entirely new "Selection Plan" process that had not yet been approved by the SEC, and that:

> if the Selection Plan is approved, it will take approximately seven months from the time bids are received to submit the CAT NMS Plan. If the Selection Plan is not approved, bidders will need time to finalize their bids, and the SROs will need additional time to develop an alternative process for reviewing and evaluating bids, formulating the CAT NMS Plan, and selecting the plan processor.[40]

On December 6, 2013, the SEC granted the requested exemption, kicking back the plan deadline to September 30, 2014.[41] During the course of the consecutive exemptions, of course,

---

[34] Letter from Robert Colby, FINRA, to Elizabeth Murphy, Securities and Exchange Comm'n, Feb. 7, 2013, *available at* https://www.sec.gov/rules/exorders/2013/34-69060-letter.pdf.

[35] Consolidated Audit Trail National Market System Plan, Request for Proposal, Feb. 26, 2013 (revised Mar. 4, 2014).

[36] *Order Granting a Temporary Exemption Pursuant to Section 36(a)(1) of the Securities Exchange Act of 1934 from the Filing Deadline Specified in Rule 613(a)(1) of the Exchange Act*, Sec. and Exch. Comm'n, Exchange Act Rel. No. 34-69060, (Mar. 7, 2013), 78 Fed. Reg. 15771 (Mar. 12, 2013), *available at* https://www.sec.gov/rules/exorders/2013/34-69060.pdf.

[37] See Presentation for SEC Rule 613: Consolidated Audit Trail (CAT), SRO Industry Event - Bidders Conference, Plan Participants, Mar. 8, 2013, *available at* http://www.catnmsplan.com/Source/process/p220975.pdf.

[38] *Id.*, at 4.

[39] Letter from Robert Colby, FINRA, to Elizabeth Murphy, Securities and Exchange Comm'n, Nov. 7, 2013, *available at* https://www.sec.gov/rules/exorders/2013/34-71018-letter.pdf.

[40] *Id.*

[41] *Order Granting a Temporary Exemption Pursuant to Section 36(a)(1) of the Securities Exchange Act of 1934 from the Filing Deadline Specified in Rule 613(a)(1) of the Exchange Act*, Sec. and Exch. Comm'n, Exchange Act Rel. No. 34-71018, (Dec. 6, 2013), 78 Fed. Reg. 75669 (Dec. 13, 2013), *available at* https://www.sec.gov/rules/exorders/2013/34-71018.pdf.

the exchanges and FINRA submitted a plan to the SEC as to how they would select the Audit Trail processor,[42] and had it approved.[43]

With the selection process approved, after an extensive year-long vetting and specification process involving more than 30 firms,[44] on March 21, 2014, ten bids were received. On July 1, 2014, that list was narrowed down to six bidders, including both FINRA and Thesys Technologies.[45]

Nearly a year and half after it was initially due, on September 30, 2014, the exchanges and FINRA submitted their first "CAT Plan."[46]

More delays and exemptions would follow.

Throughout 2015, as the exchanges and FINRA got down to the details of the Audit Trail, they sent several exemption requests to the SEC to loosen various technical requirements set forth in the plan.[47] Then, nearly a year and a half after submitting their first CAT Plan, they submitted their amended CAT Plan on February 27, 2016. A few weeks later, the SEC granted the SROs' substantive exemptive requests. Then, several weeks after that, on April 27, 2016, the SEC sent the amended CAT Plan out for comment.[48]

---

[42] *Notice of Filing of Proposed National Market System Plan Governing the Process of Selecting a Plan Processor and Developing a Plan for the Consolidated Audit Trail*, Exchange Act Rel. No. 34-70892 (Nov. 15, 2017), *available at* https://www.sec.gov/rules/sro/nms/2013/34-70892.pdf.

[43] *Order Approving Proposed National Market System Plan Governing the Process of Selecting a Plan Processor and Developing a Plan for the Consolidated Audit Trail*, Sec. and Exch. Comm'n, Exchange Act Rel. No. 34-71596 (Feb. 21, 2014), 79 Fed. Reg. 11152 (Feb. 27, 2014) ("Selection Plan Approval Order"), *available at* https://www.gpo.gov/fdsys/pkg/FR-2014-02-27/pdf/2014-04240.pdf.

[44] The Participants received 31 Intent to Bid forms, during a preliminary review process. Over the course of the year before formal bids were returned, most of the firms withdrew their intents to bid. See, List of Intents to Bid Forms, *available at* http://www.catnmsplan.com/Source/process/p217583.pdf (last viewed Nov. 20, 2017).

[45] See Scott Patterson and Bradley Hope, *Bidders for SEC's CAT System Narrowed to Six from 10*, Wall St. Journal, July 1, 2014, *available at* https://www.wsj.com/articles/bidders-for-secs-consolidated-audit-trail-system-narrowed-to-six-from-10-1404247796. The selection of the winning bidder was actually delayed for another two and a half years.

[46] Letter from Participants to Brent J. Fields, Sec. and Exch. Comm'n, Sept. 30, 2014, *available at https://www.sec.gov/divisions/marketreg/cat-nms-plan-letter.pdf* At that time, the exchanges and FINRA noted that "Since July 2012, [they] have held approximately 509 meetings related to the CAT." *Id.*

[47] See, Letter from Participants to Brent J. Fields, Sec. and Exch. Comm'n, Jan. 30, 2015, available at https://www.sec.gov/rules/exorders/2016/finra-incoming-letter-013015.pdf; Letter from Participants to Brent J. Fields, Sec. and Exch. Comm'n, Apr. 3, 2015, *available at* http://www.catnmsplan.com/wp-content/uploads/2017/03/exemptivesupplement1-allocationsreports.pdf ; Letter from Participants to Brent J. Fields, Sec. and Exch. Comm'n, Sept. 2, 2015, *available at* http://www.catnmsplan.com/wp-content/uploads/2017/03/exemptivesupplement2-accounteffectivedate.pdf.

[48] *Notice of Filing of the National Market System Plan Governing the Consolidated Audit Trail*, Sec. and Exch. Comm'n, Exchange Act Rel. No. 34-77734, (Apr. 27, 2016), 81 Fed. Reg. 30614 (May 17, 2017), *available at* https://www.sec.gov/rules/sro/nms/2016/34-77724.pdf.

With the amended CAT Plan in hand, then it was the SEC's turn to ask for a delay.

The Commission then had 120 days after publication in the Federal Register to act on the CAT Plan. Upon publishing it for comment, the SEC received 22 comment letters (a relatively small number). Nevertheless, the Commission decided that it needed more time to digest the 22 comment letters, and gave itself an extension until November 10, 2016 to act.[49] On November 15, 2016, the SEC finally approved the amended CAT Plan.[50] Of course, by then, the CAT was several years behind schedule.

On January 18, 2017, after being involved in the specifications development and bidding process for more than three years, Thesys Technologies LLC was selected by the exchanges and FINRA to be the Consolidated Audit Trail Plan Processor.[51] Revised technical specifications were released on July 6, 2017.[52] The exchanges were set to begin reporting on November 15, 2017.[53]

Requests to Revisit the Funding Structure and Delay Reporting

The determination of who will pay how much for the Audit Trail is still not yet finalized. The decision of how to fund the Audit Trail was pushed off by the SROs until May 2017, when the exchanges and FINRA filed a plan to adopt industry member fees that would fund it.[54] The filing was ostensibly made immediately effective, but on June 30, the SEC temporarily suspended it for further review.[55] Noticeably, the funding plan designed by the exchanges and FINRA appears to place a significant portion of the cost burden on broker dealers, and even the off-exchange, OTC

---

[49] *Notice of Designation of Longer Period for Commission Action on the Proposed National Market System Plan Governing the Consolidated Audit Trail by Participants*, Sec. and Exch. Comm'n, Exchange Act Rel. No. 34-78441 (July 29, 2016), 81 Fed. Reg. 51527 (Aug. 4, 2016), *available at* https://www.sec.gov/rules/sro/nms/2016/34-78441.pdf. The November 10 date was modified to November 15, based upon the date of publication in the Federal Register.

[50] *Order Approving the National Market System Plan Governing the Consolidated Audit Trail*, Sec. and Exch. Comm'n, Exchange Act Rel. No. 34-79318 (Nov. 15, 2016), *available at* https://www.sec.gov/rules/sro/nms/2016/34-79318.pdf.

[51] Letter from Participants to Brent J. Fields, SEC, Jan. 18, 2017, *available at* https://www.sec.gov/divisions/marketreg/rule613-info-notice-of-plan-processor-selection.pdf.

[52] Thesys CAT, *CAT Reporting Technical Specifications for Participants*, v. 1.3, (July 6, 2017), *available at* http://www.catnmsplan.com/wp-content/uploads/2017/03/CAT-Tech-Specs-1.3-for-Publication.pdf.

[53] *Order Approving the National Market System Plan Governing the Consolidated Audit Trail*, Sec. and Exch. Comm'n, Exchange Act Rel. No. 34-79318 (Nov. 15, 2016), 81 Fed. Reg. 84696 (Nov. 23, 2016), *available at* https://www.sec.gov/rules/sro/nms/2016/34-79318.pdf.

[54] Between May 1 and May 26, the exchanges and FINRA filed proposed rule changes to establish fees to pay for the Audit Trail. See *Suspension of and Order Instituting Proceedings to Determine Whether to Approve or Disapprove Proposed Rule Changes to Establish Fees for Industry Members to Fund the Consolidated Audit Trail*, Sec. and Exch. Comm'n, Exchange Act Rel. No. 34-81067, June 30, 2017, *available at* https://www.sec.gov/rules/sro/batsbyx/2017/34-81067.pdf (Funding Plan Suspension Order) (referring to each filing).

[55] Funding Plan Suspension Order.

markets. Not surprisingly, amidst a slew of industry outrage, on November 9, 2017 the SEC extended its time to make the decision until January 14, 2018.[56]

But the funding structure isn't the only key item left up in the air--despite years of preparation. With just a few weeks left to begin reporting, it became clear that the exchanges were not going to meet the deadline of their own plan. They pressed the SEC, now under new Chairman Jay Clayton, for relief. There was a concern--since proven to be well-founded--that the SEC might be less willing to simply acquiesce to another long delay. Thus, the SROs also pressed this Committee and the Senate Banking Committee for relief.

Those efforts were aided by an untimely admission by the SEC in late September that its completely unrelated database for corporate filings, EDGAR, had been hacked a year earlier.[57]

In a hearing on October 4, 2017, Chairman Hensarling pressed SEC Chairman Clayton to "delay [the Audit Trail's] implementation date until the commission can ensure that the appropriate safeguards and internal controls are in place to protect this data."[58] The next day, Messrs. Warren Davidson and Brad Sherman introduced the Market Data Protection Act of 2017 (H.R. 3973). A week later, on October 11, 2017, this Committee passed that bill out of markup by a vote of 59-1. Amongst other things, the bill would require the SEC, FINRA, and the CAT operator (but not the exchanges) to develop "comprehensive internal risk control mechanisms to safeguard and govern the storage of all market data by such entity, all market data sharing agreements of such entity, and all academic research performed at such entity using market data."[59]

Until that happens, the plan operator (Thesys) would be prohibited from accepting data for the Audit Trail, and the requirements for participants (like the exchanges) to submit data to the Audit Trail "shall not apply."[60] However, previously-developed internal controls could be deemed as adequate, provided that they meet the requirements of the "Chief Economist" of the SEC.[61]

In the days that followed, it became clear that the well-intentioned bill had a few significant unintended consequences, and an effort was started to negotiate improvements. For example, the bill wouldn't appear to apply to exchanges. It also could allow for further, indefinite delays by the exchanges and FINRA, or the SEC. And it fails to explain how the SEC's "Chief Economist" is the qualified expert to evaluate the reasonableness of the proposed cybersecurity for these entities.

---

[56] *Notice of Designation of Longer Period for Commission Action on Proceedings to Determine Whether to Approve or Disapprove Proposed Rule Changes to Establish Fees for Industry Members to Fund the Consolidated Audit Trail*, Sec. and Exch. Comm'n, Exchange Act Rel. No. 34-82049, Nov. 9, 2017, *available at* https://www.sec.gov/rules/sro/batsbyx/2017/34-82049.pdf.

[57] Statement of Chairman Jay Clayton, Sec. and Exch. Comm'n, (Sept. 20, 2017), *available at* https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20.

[58] *Examining the SEC's Operations, Agenda, and Budget*, Hearing before the House Financial Services Committee, 115th Cong. (2017) (Statement of Chairman Jeb Hensarling).

[59] Market Data Protection Act of 2017 (H.R. 3973), 115th Cong. (2017) (Market Data Protection Act).

[60] Market Data Protection Act.

[61] Market Data Protection Act.

Nevertheless, efforts to improve the bill collapsed, and on November 13, 2017, the House passed the bill by voice vote.

I understand this Committee may be looking at a revised version of that bill or another, similarly focused, bill to move forward with over the foreseeable future. I have recently reviewed a draft of some legislation that would improve upon the House-passed bill in a number of ways, including by tailoring the data to be covered to that which is "reported to, stored by, or accessed from the consolidated audit trail", and would include the exchanges.

There are still several curious elements to the legislation, however, which I think could significantly frustrate the regulatory goals of the CAT and the SEC. For example, the plan processor couldn't accept data until the Commission certifies that it has the required internal risk control mechanisms. To be blunt, what does the SEC know about data security? Why are they the judge? And why would this have to be done at the Commission level, as opposed to staff? Would it be testing the adequacy of those mechanisms? What are the standards? How would this be different than the already extensive requirements laid out in the technical specification for the Plan Processor in the CAT Plan? Does that mean the SEC would be the guarantor of the adequacy of those mechanisms?

All of these new questions arise, and likely lead to significant secondary and tertiary questions. This creates incredible legal and practical uncertainty, and is also likely to foster new legal challenges, and even more delays.

But perhaps the biggest question arises from the language specific to the personally identifying information (PII). For this information--again which the market participants already have and regulators already have access to--the bill would require an entirely new, and duplicative cost-benefit analysis as well as a report to Congress. That has nothing to do with the adequacy of the security, but rather a re-consideration of one of the primary purposes of the Audit Trail in the first place--to actually know who is doing the trading.

The SEC, FINRA, and past Congressional hearings have demonstrated the basic need for this information. This debate is years past settled. To require this additional analysis and support offers absolutely no value to the regulatory process, but only serves to frustrate it--which I suspect is precisely the objective of some of the proponents.

Current Key Concerns with the Audit Trail--Security and Cost

At the time of the Audit Trail's proposal, there was remarkably little public pushback on the need to create it, nor was there significant disagreement for the proposal to cover a broad swath of the capital markets.

That said, this lack of public resistance was not reflective of stakeholders' significant concerns. FINRA, which operates the OATS system, could easily lose its leading position as the provider of

market surveillance services for the industry.[62] Similarly, the for-profit exchanges have worried about the costs.

Outside of the SROs, some market participants worried that their trading strategies could be discovered, and many worried about the risks of aggregating all of this information in one place. Still others feared that regulators might detect widespread abuses that could further deteriorate market confidence or hurt their revenues. And some market participants worried about costs.

In recent days, there has been a lot of attention paid to the cybersecurity of the Audit Trail. Some have suggested that the SEC should just put everything on an indefinite hold while it reviews the security of the system, Thesys, and those who access the system.

I agree with calls to ensure the security of the system. However, I urge Congress and the SEC to stay cognizant of the facts. And the basic facts are:

- The Audit Trail is similar to existing databases in many respects;
- The Audit Trail has been in development for years pursuant to an SRO-designed and SRO-approved plan;
- The Audit Trail is developed and operated by an SRO-selected vendor; and
- Those seeking the delay have repeatedly asked for and received numerous delays along the way, extending this project for years longer than anticipated.

Some have trotted out spurious arguments to delay or abandon the Audit Trail based on the SEC's recent announcement of a data breach.[63] Of course, the data breach should be a reminder to be acutely sensitive to data security. As the SEC Chairman stated when denying the SROs' most-recent delay request, "protection of the information submitted to the CAT is of paramount importance."[64] That's a sensitivity that should have, and did, exist amongst the SROs, SEC, and potential bidders for the Audit Trail long before the SEC's data breach.[65]

---

[62] I worry about the potential regulatory "race to the bottom" if the exchanges and others are given access to the same dataset, but are allowed to take varied regulatory approaches. Importantly, I question whether any for-profit entities are capable of appropriate surveillance and regulatory operations. This may be because of both their narrow views of issues related to their markets, as well as the basic conflicts of interest between their for-profit business interests and their regulatory obligations. A consolidated, non-profit regulator is a significant advantage over such a flawed system. If the Commission is to allow FINRA to be replaced by other surveillance providers, I would recommend the Commission adopt a number of safeguards, including a distinct set of minimum conduct standards and best practices.

[63] See Statement of Chairman Jay Clayton, Sec. and Exch. Comm'n, (Sept. 20, 2017), *available at* https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20.

[64] Statement on the Status of the Consolidated Audit Trail, Sec. and Exch. Comm'n, (Nov. 14, 2017), *available at* https://www.sec.gov/news/public-statement/statement-status-consolidated-audit-trail-chairman-jay-clayton.

[65] For example, a July 29, 2014 presentation by FINRA on the Audit Trail describes the importance of protecting sensitive industry data. Presentation by FINRA *et. al*, Consolidated Audit Trail, at 2, (2014), *available at* https://www.finra.org/sites/default/files/FINRA%20CAT%20SIFMA%20Presentation%2020140729%20FINAL%20v1%201_0_0_0.pdf (last viewed Nov. 21, 2017).

As for potential concerns with Thesys itself, the company had no relationship to the SEC's decades-old EDGAR database. Thesys has, however, collected, processed, and distributed market data for market participants for years. It has even been retained by the SEC to operate its Market Information and Data Analytics System (MIDAS), which it has operated for years without any known incidents.

I am surprised by the large outcry from the SROs, who just earlier this year selected Thesys as most qualified to build and operate the Audit Trail.[66] But it's also curious because the exchanges and FINRA helped detail the Plan Processor Requirements. Those requirements explicitly state that:

> The following industry standards—which is not intended to be an exclusive list—must be followed as such standards and requirements may be replaced by successor publications, or modified, amended, or supplemented and as approved by the Operating Committee (in the event of a conflict between standards, the more stringent standard shall apply, subject to the approval of the Operating Committee):
>
> - National Institute of Standards and Technology:
> - 800-23 – Guidelines to Federal Organizations on Security Assurance and Acquisition / Use of Test/Evaluated Products
> - 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
> - 800-115 – Technical Guide to Information Security Testing and Assessment
> - 800-118 – Guide to Enterprise Password Management
> - 800-133 – Recommendation for Cryptographic Key Generation
> - 800-137 – Information Security Continuous Monitoring for Federal Information Systems and Organizations
> - To the extent not specified above, all other provisions of the NIST Cyber Security Framework
> - Federal Financial Institutions Examination Council:
> - Authentication Best Practices
> - International Organization for Standardization:

[66] See Letter from Participants to Brent J. Fields, SEC, Jan. 18, 2017, *available at* https://www.sec.gov/divisions/marketreg/rule613-info-notice-of-plan-processor-selection.pdf.

- ISO/IEC 27001 – Information Security Management
[67]

The Plan Processor also "must conduct third party risk assessments at regular intervals to verify that security controls implemented are in accordance with NIST SP 800-53. These risk assessments must include assessment scheduling, questionnaire completion and reporting," and should be reported back to the exchanges and FINRA.[68]

I am not aware of any allegations that Thesys has not met those standards or is otherwise incapable of meeting these expectations. Further, I am not aware of any accusations of how those industry standards that have previously been established (and which can evolve over time) are somehow now inadequate. The exchanges and FINRA have not offered any significant new information since then as to why they now think they need this delay.

In addition, I wish to remind the Committee that the Audit Trail is also remarkably similar to the Order Audit Trail System (OATS), which has long been operated by FINRA. Many lay people don't know that FINRA currently runs a massive audit trail system that requires inputs from a wide array of market participants, just like the Consolidated Audit Trail. That system, which has been operating for decades, is stored in the cloud on Amazon Web Services.[69] And it includes very specific, and commercially highly-sensitive trading details.[70]

In a 2014 presentation by FINRA, DTCC, and Amazon Web Services pursuant to their bid for the Audit Trail, FINRA detailed how

- FINRA collects, links and stores over 30 billion market events per day covering over 90% of the equity market
- FINRA maintains over 2PB of historical data
- FINRA provides data access to
    - 5,000 Registered OATS Users
    - 1,600 Registered Users of the FINRA Online Query Tool[71]

These are remarkably similar to the expectations for the new Audit Trail.

---

[67] CAT NMS Plan Processor Requirements, Appendix D, at 14-15.
[68] CAT NMS Plan Processor Requirements, Appendix D, at 16.
[69] See Presentation of Bob Griffiths and Ranga Rajagopal, AWS Summit: Best Practices Using Big Data on AWS, June 14, 2017, *available at* https://www.slideshare.net/AmazonWebServices/best-practices-using-big-data-on-aws-aws-public-sector-summit-2017.
[70] For trades involved in principal trading or combinations of principal and customers, identification information of the broker-dealer is obviously provided. Additionally, since the implementation of the Large Trader Reporting Rule, key personally identifiable information is readily accessible by FINRA through the electronic blue sheet process for covered persons. *Large Trader Reporting Final Rule.*
[71] Presentation by FINRA *et. al*, Consolidated Audit Trail, at 2, (2014), *available at* https://www.finra.org/sites/default/files/FINRA%20CAT%20SIFMA%20Presentation%2020140729%20FINAL%20v1%201_0_0_0.pdf (last viewed Nov. 21, 2017).

Building a massive audit trail with sensitive and valuable inputs provided by a large number of entities can be done. While the new Audit Trail will include more underlying beneficial owner information, from a data perspective, this change is a quantitative one, not qualitative.[72]

In addition to the data security concerns, perhaps nothing raises the specter of conflict more than the filing by the for-profit exchanges and FINRA on how the Audit Trail is to be funded. In their filing, the NMS Plan participants (1) chose to file the proposals for immediate effectiveness under the Exchange Act and (2) failed to solicit industry input or public comment on the proposed fee model.[73] In fact, SIFMA noted that all but one participant operates as a for-profit company that directly competes with brokers and the proposed fee schedules allocate nearly all the costs to those brokers.[74]

Lastly, some have expressed concerns that the Audit Trail will be largely duplicative of OATS, while also being different--leading to potentially unnecessary compliance costs and risks. To address those concerns, the SROs have already filed with the SEC their intention to retire the OATS system once the Audit Trail is operational.[75] That said, I would caution that OATS should not be retired until the Audit Trail has proven to be an effective tool that is at least as valuable for regulatory surveillance as OATS has been.

What Should Regulators and Congress Do Now?

In my view, the best thing this Committee could do would be to (1) press the SEC to ensure that the Audit Trail is fully implemented without further delay and (2) help the SEC work with its sister agency, the CFTC, to improve the Audit Trail so that it more fully achieves its intended purposes. To do that, it will need to include the futures markets, legal entity identifiers, and greater precision.

The SEC's decision to deny the exchanges' and FINRA's requested one-year exemption means that they are out of compliance with the rule they crafted, and for which they have previously been given several exemptions. This failure to comply empowers the SEC to take enforcement action, if it chooses, against the non-compliant firms.

That said, Chairman Clayton has made it clear that he would not want or expect any firms to report to the CAT Plan operator if they believed that the system was in any way insecure. Put

---

[72] We note that FINRA already has access to the vast majority of information to be required by the Audit Trail, but not in a readily-accessible, automated format.

[73] Letter from SIFMA to Brent J. Fields, SEC, June 6, 2017, *available at* https://www.sec.gov/comments/sr-batsbzx-2017-38/batsbzx201738-1788188-153228.pdf ("SIFMA Letter").

[74] SIFMA Letter, at 2.

[75] *Notice of Filing of Proposed Rule Change to Eliminate Requirements That Will Be Duplicative of CAT*, Exchange Act Rel. No. 34-80799, Sec. and Exch. Comm'n, May 26, 2017, *available at* https://www.sec.gov/rules/sro/nyse/2017/34-80799.pdf.

another way, without formally granting "no action" relief, the Chairman has taken a remarkably similar approach.

Ultimately, the Chairman's decision to deny the requested exemption provides the SEC with, for the first time in years, significant leverage versus the exchanges and FINRA to compel progress on the Audit Trail's implementation. While they all appear to be acting in good faith to begin the required reporting, Clayton will presumably elect to not pursue them for their violations. However, if the exchanges or FINRA appear to be intentionally slow-walking their compliance or otherwise obstructing the objectives of the Audit Trail, he presumably could direct the Commission staff to conduct an investigation, and if authorized by the Commission, take enforcement action.

I believe this will significantly improve the odds of having an implemented Audit Trail within the next 12 months. By way of contrast, if the Chairman had granted the request, or if the Market Data Protection Act of 2017 were to become law as currently drafted, I believe that the CAT would again face multi-year delays.

As a result, I believe that the best course of action for this Committee would be to either (1) significantly revise the legislation or (2) encourage the SEC handle this appropriately through the administrative process. If the Congress elects to press a legislative solution, I would encourage you to (1) narrow the scope to just information regarding the Audit Trail, (2) insert new time limitations to ensure it does not lead to yet more years-long delays, and (3) insert language to improve the Audit Trail, which should include futures, legal entity identifiers, improved precision, and revised governance.

Longer term, I urge you to reconsider eliminating the deeply conflicted process that has led to this extremely delayed result. Put simply, for-profit exchanges should not be empowered by the government to set the terms and the costs of the regulatory apparatus that oversees the markets--including their competitors.

Conclusion

Almost exactly seven years ago, on December 8, 2010, SEC Chairman Schapiro and CFTC Chairman Gensler testified before a joint Senate hearing that they would work together to get the Audit Trail up and running.[76] In the years since that hearing, as major market disruptions and conflicts of interest have come into the spotlight, concerns about the integrity and stability of the U.S. capital markets have only grown. Market participants, experts, and policymakers have clamored for the government to modernize the regulatory apparatus for trading.

---

[76] Reed-Levin Hearing. When pressed by Chairman Levin as to how much it would cost and how long it would take before it was up and running, Chairman Schapiro assured him that it would be well before now. Both Commissioner Stein and I, as the lead staffers in that hearing for Chairmen Reed and Levin, respectively, took those assurances to heart. Unfortunately, despite the best of intentions to get the regulators this basic tool that they desperately need, those predictions have proven inaccurate.

The Consolidated Audit Trail is a necessary, but not sufficient, step towards ensuring that regulators have the basic tools necessary to oversee our capital markets. If the US capital markets are to remain the best in the world, we need it. There will be more major market disruptions and more bad behavior in the future. The question is whether regulators will have the tools they need to identify them, figure out what's going on, and stop them before disaster. Frankly, we need version 3.0 of the Audit Trail. But after more than seven years of waiting, we'll take version 1.0.

Thank you for your consideration and for the opportunity to share my thoughts with you on this important topic for our markets.