waterstechnology

Moonshots Shelved

BANKS LOOK TO HOME-WORKING TECH DURING THE PANDEMIC, SHELVING BLEEDING-EDGE PROJECTS

waterstechnology.com

September 2020

waterstechnology

INNOVATION EXCHANGE

September 9 – 22, 2020
Globally online

A global virtual exchange connecting leaders and experts discussing the future of data and technology in capital markets

events.waterstechnology.com/innovation-exchange

Editor-in-Chief Anthony Malakian
anthony.malakian@infopro-digital.com
Editor at Large Max Bowie
max.bowie@infopro-digital.com
European Editor Jo Wright
joanna.wright@infopro-digital.com
Editor, Asia Wei-Shen Wong
wei-shen.wong@infopro-digital.com
Senior Reporter Josephine Gallagher
josephine.gallagher@infopro-digital.com
European Reporter Hamad Ali
hamad.ali@infopro-digital.com
Reporter Rebecca Natale
rebecca.natale@infopro-digital.com
Reporter Mariella Reason
mariella.reason@infopro-digital.com
Head of Editorial Operations Elina Patler
elina.patler@infopro-digital.com

Global Content Director Victor Anderson
victor.anderson@infopro-digital.com
+44 (0) 207 316 9090
Commercial Director Ince Saleem
Tel: +44 (0) 20 7316 9258
ince.saleem@infopro-digital.com
Business Development Executive Sonja Patillo
Tel: +1 212 776 8083
sonja.patillo@infopro-digital.com
Account Manager Daniel De-Bruce
Tel: +44 (0) 20 7316 9126
daniel.debruce@infopro-digital.com

Marketing Manager Louise Sheppey
tel: +44 (0) 20 7316 9476
louise.sheppey@infopro-digital.com
Design Lisa Ling

Corporate and Single Subscriptions
US: Barbara Faiman tel +1 646 736 1852
info@waterstechnology.com

Global Brand Director Katie Palisoul
katie.palisoul@infopro-digital.com
Global Editorial Director Duncan Wood
duncan.wood@infopro-digital.com
Managing Director David Pagliaro
david.pagliaro@infopro-digital.com

Infopro Digital Head Office
Fifth Floor,
133 Houndsditch
London EC3A 7BX
United Kingdom
tel: +44 (0) 20 7316 9000
fax: +44 (0) 20 7930 2238

Infopro Digital US
55 Broad Street, 22nd Floor
New York, NY 10004
tel: +1 646 736 1888

Infopro Digital Asia
Unit 1704-05
Berkshire House, Taikoo Place
25 Westlands Road
Quarry Bay
Hong Kong
tel: +852 3411 4888

Infopro Digital Customer Services
tel: +44 (0) 1858 438 800

WatersTechnology (ISSN 1068-5863) is published monthly (12 times a year) by Infopro Digital Risk Limited. Printed in the UK by Stephens & George Print Group, Dowlais, Merthyr Tydfil, Wales.

Far Side of the Moon

At the start of 2015, then-UBS chief information officer Oliver Bussmann sat down with *WatersTechnology* for a wide-ranging profile. One of the things he was most keen to talk about was the promise of blockchain, saying, "I genuinely think that blockchain will massively disrupt the buy and sell sides, payment streams, and settlement alike, to the point where you can see that these things behave in totally new ways in five years."

Well, five-and-a-half years after we published that profile, we're still waiting for that massive disruption in the capital markets, and from the sounds of it, blockchain projects—and other projects that involve emerging technologies—may be put on the back burner for quite some time.

This month's cover story (*see page 32*) looks at how banks are allocating their IT budgets in a Covid world, and finds that CIOs and CTOs are devoting their attention to projects that facilitate remote working, and turning their backs on so-called ambitious moonshot projects meant to have longer-term payoffs for their organizations.

In the cover story, Bussmann says that big, multi-year transformation projects are being put on hold at tier-one banks as "investment priorities have changed significantly since the beginning of the year."

Right now the game is about keeping the lights on and using duct tape to plug the floor boards. But technologists, by nature and by demand, are innovative, and one thing that the pandemic has laid bare is the need for innovative solutions to unthinkable problems.

It's also important to remember this: Companies like UBS and Deutsche Bank—executives from which are interviewed for the story—had already made significant investments in remote-working solutions prior to the pandemic, freeing up resources and time to dedicate still to moonshots, while others play catch-up. In either case, now isn't a time to stand still—it's a time to envision what you want your organization to look like in the future, and figure out how innovation can get you there.

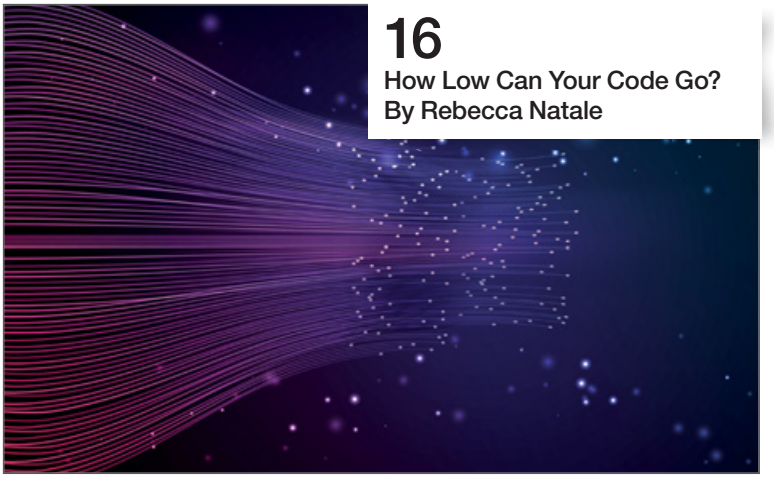
I also think that moonshot projects are still in the works at banks across the globe, even the ones that were unprepared for Covid-19. It's just that those banks—which could be described as stodgy when it comes to innovation—are, and have been, relying on vendors to do the heavy lifting. Rather than build a Charles River-esque order and execution management system (OEMS), State Street bought the company. RBC didn't build an operating system into which to pop its internal OMS; it partnered with OpenFin. Banks aren't building video conferencing technologies, they're licensing the technology from providers like Symphony.

Rest assured, there are plenty of capital markets businesses shooting for the moon; they're just not always the ones calling the shots. wt

Anthony Malakian
Editor-in-Chief

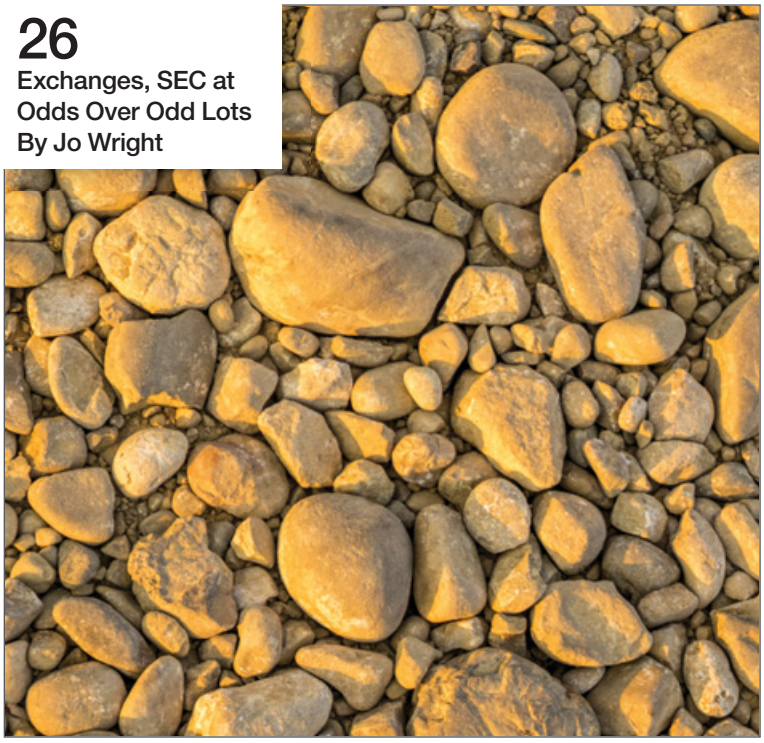
waterstechnology

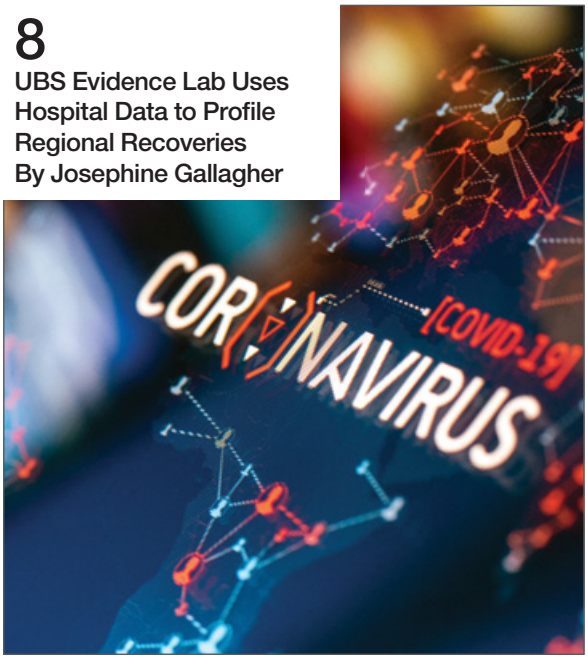
Contents

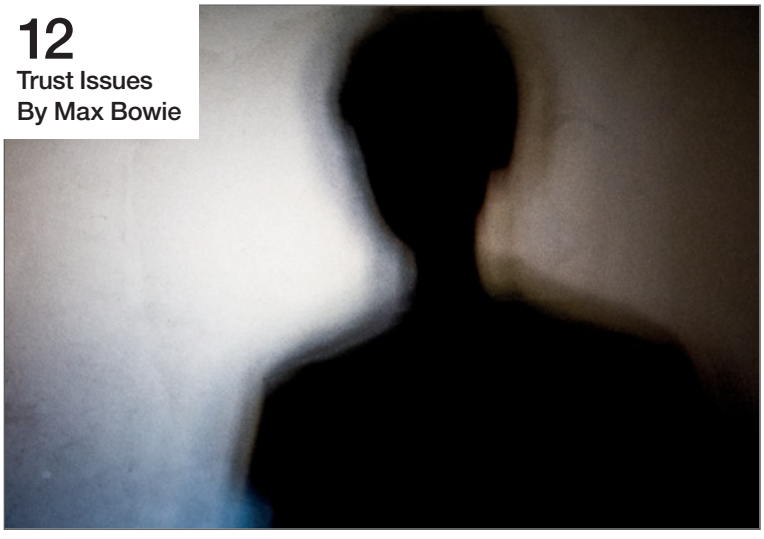


16
How Low Can Your Code Go?
By Rebecca Natale

20
Cryptography's Quantum Threat
By Hamad Ali







Covid Could Cause US Regulators to Rethink Surveillance

Not having specific requirements and procedures for firms to refer to ended up putting some funds in a tough place during the pandemic's early days. By Rebecca Natale

At the height of the pandemic as the markets were rapidly fluctuating, US trading firms were having to both manage a remote workforce, as well as manage new types of compliance risks. When compared to their European counterparts, US regulators have not been as prescriptive when it comes to procedures to ensure surveillance for working remotely, thus firms were flying blind while managing their coronavirus response. As a result, it might cause a rethink at some of the US regulatory bodies in order to better fall in line with European guidance.

For example, since the Covid-19 pandemic first began disrupting the markets in March, the Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) has observed areas of heightened risk that it says firms should be focusing on.

In mid-August, the OCIE issued a risk alert titled "Select Covid-19 Compliance Risk and Considerations for Broker Dealers and Investment Advisers" in which it lays out these six areas: protection of investor assets; supervision of personnel; fees, expenses, and financial transactions; investment fraud; business continuity; and protection of sensitive information. The OCIE is the SEC's examining body; its mission is to ensure market integrity and investor protection, partly by monitoring risks. This was the OCIE's sixth risk alert since April; for comparison, it issued six alerts in all of 2019, five in 2018 and 2017, and four in 2016.

In Covid-19 times and beyond, firms have a long and potentially transformative journey ahead of them.

> "Vendors can't go in and adjust alert parameters. When volumes and volatility spiked, a lot of firms were completely unprepared to go in and adjust their surveillance or alert parameters. They didn't even know what parameters to adjust it to—infinity?"
> **Danielle Tierney, Greenwich Associates**

Danielle Tierney, a senior adviser on market structure and technology at Greenwich Associates, believes that the SEC may be laying the groundwork to enact more specific regulation with exact procedures that more closely aligns with the EU's Market Abuse Regulation (MAR) and the Markets in Financial Instruments Directive (Mifid II). For example, US regulation on mobile phones used in trading is vague, at best, whereas MAR and Mifid II directly address those devices in their communications monitoring requirements, Tierney says.

"It's been up to firms to self-regulate. It's been up to firms to say, 'Okay, it's a pain to have all this mobile surveillance functionality, and roll out all these devices, and it costs money.' But also, if we don't monitor any of these mobile devices that employees are definitely using for work, then they're basically just whistling past the graveyard until someone does something really, really bad," she says.

Tierney says US trading firms are not far behind EU firms in how they surveil and monitor in practice, but without specific requirements and guidance to fall back on in March, some funds were put in a position during the pandemic's early days. At that time, the adviser spoke with turret providers and infrastructure providers to get a sense of how working from home was being handled, and they told her that only about a one-third of firms had been prepared for the catastrophe.

"There were a lot of outages," she says. "So what you had the first couple weeks of March was firms reaching out to the SEC and the CFTC and saying, 'Hey, just so you know, we have not been in compliance.'"

While the pandemic has fueled a new wave of surveillance tech from vendors, their clients may not have been as proactive as they should have been with the regtech systems they had in place. Tierney says maintenance of those systems proved to be a sharp pain point for firms whose staff were mostly working from home.

"Vendors can't go in and adjust alert parameters," Tierney says. "When volumes and volatility spiked, a lot of firms were completely unprepared to go in and adjust their surveillance or alert parameters. They didn't even know what parameters to adjust it to—infinity?" wt

Ion Forced to Split Broadway, Keeping FX Business

The remedy will satisfy the UK competition watchdog—but "a big defeat" for the acquisitive tech giant.
By Luke Clancy

Trading systems giant Ion will split up Broadway Technology—the rival it acquired in February—to allay concerns the deal would erode competition in the market for fixed income trading software.

An initial review by the UK's Competition and Markets Authority concluded on July 7 that a months-long probe was warranted. In a further report, published on August 7, the CMA revealed Ion's proposed remedy—an undertaking to keep only Broadway's foreign exchange business and find a buyer for the firm's fixed income franchise.

The CMA's report says this "may allow a suitable purchaser to compete effectively in the supply of sell-side front-office systems for fixed income electronic trading, worldwide and thus restore the competitive constraint provided by Broadway that would otherwise be lost following the merger."

It's not known whether a purchaser has already been found. Ion did not immediately respond to a request for comment.

The CMA's decision will be welcomed by some banks, who have watched Ion's trail of acquisitions transform it into one of the world's largest front-office tech vendors. With dealers under pressure to cut costs in recent years, negotiations with Ion have become a growing source of frustration.

One e-trading executive describes the planned sale of Broadway's fixed income assets as "a big defeat" for Ion.

The CMA's report says the divestment will be achieved through "the sale of the entire share capital of Broadway … to a suitable purchaser and the transfer back to Ion of the Broadway FX business." A buyer will be deemed suitable if it satisfies criteria laid out in the CMA guidance. A suitable purchaser must have the "financial resources, expertise, incentive and intention to maintain, operate and develop the divestment business as part of a viable and active business in competition with the merged entity in the relevant market."

Owing to the fact that certain members of Broadway's staff including senior management are not transferring as part of the proposed undertakings, the CMA says it will also need to "ensure that the nominated buyer has the necessary expertise to address any technical and/or management gaps from within its own organization."

There are not many firms that tick these boxes, according to an executive at one trading software vendor. "There are only a handful of firms that spring to mind, and all of these will see how the fixed income market is evolving, with banks increasingly building their own technology modules which support differentiation, then plugging the gaps with specialist fintechs," he says.

Last year, a group of European and UK banks began assessing the viability of a DIY alternative to Ion.

Vendors including Axe Trading, smartTrade, and TransFICC are among those that compete with Ion. All are smaller and more specialised. The CMA described Ion as "by far the largest" supplier of fixed income software, with Broadway and Bloomberg as its only significant competitors.

TOC Tick

The CMA says Broadway's fixed income business comprises its brand, share capital, staff related to supporting its fixed income business, current fixed income customers, software including the TOC—Broadway's core platform which forms part of its programming interface—the current Broadway offices, facilities, IT, and infrastructure, as well as its hosting service, Greyspan.

The deal would leave Ion with Barracuda FX, a well-regarded order management system that was acquired by Broadway in April 2019.

Under the proposed undertakings, the following parts of the Broadway business would be transferred back to or remain with Ion: certain members of Broadway's management; the Barracuda FX business; Broadway's FX-only customers; certain Broadway staff required for the FX business; and software that is required to serve Broadway's FX customers.

The purchaser of Broadway's fixed income business would also need to grant Ion a licence to use the TOC. However, this arrangement would be time-limited to no more than three years and for use exclusively in respect of FX, "to facilitate the transfer of Broadway FX customers", and Ion would not have access to the TOC source code. wt

Bloomberg Adds New NLP Capabilities to TOMS

The tool allows traders to search their own data to find trade information specific to them.
By Rebecca Natale

An eternal struggle for technology companies is preparing for long-term disruption while answering the day-to-day needs of customers. For Bloomberg's sell-side solutions business, this meant carving out a group of engineers whose sole focus is building solutions that don't necessarily meet the demands of clients today, but anticipates their needs in a few years as new technologies become democratized, regulations hit, and the world becomes more complex. At the same time, it's the kind of forward-thinking move that can help future-proof the data and tech giant against cutting-edge startups.

As an example of how this unit tries to stay ahead of the curve, it developed a new search functionality that's embedded into Bloomberg's Trade Order Management Solutions Trade Analyzer.

This new question-answer interface is, at its core, an engine that heavily leverages natural language processing (NLP) and machine learning algorithms to deliver answers to questions that are unique to the needs of traders. It aims to reduce the number of clicks needed to search for and within certain datasets, such as querying trade histories with a buy-side customer or looking up missed trades during a given time period, says Robert Simek, head of sell-side analytics at Bloomberg.

Those arduous searches often require going into a blotter and performing a host of manual tasks. Clients would often just export the data, or ask someone else on the desk to curate a report with the answers they sought. As a result, it could take hours or days for a trader to get an answer to what should be a simple question.

As much as an NLP model takes loads of training time and data to understand standard human language—as a simple example, how a month like August may be spelled out or abbreviated, but mean the same thing—the team spent just as long training it to understand phrases specific to the financial domain.

"There's slang that's used: What does a 'completed trade', a 'done trade', or a 'missed trade' mean?" Simek says. "As soon as a trader or front-office user types in a question and gets the wrong answer, they'll never use it again. The level of accuracy and understanding that we need for the product is a really high bar."

From ideation to full production, the project was about a year in the making. The question-answer format is only the foundation, Simek emphasizes, as clients also want to use the interface to ask more analytical types of questions, such as wanting to compare the number of trades they do on platform A versus platform B.

Meeting that demand is where the team will take the project next. Because the machine-learning model learns over time, it can start to get a sense of patterns in questions asked, such as emerging trends, top bonds, or other topics that might require aggregation from multiple databases to get to an answer. As of today, the traditional database structure the tool currently uses requires too much time to answer more analytical questions.

Part of the remaining strategy, Simek says, is moving that data to more modern database structures that allow for more complex queries to yield an instant answer. Traditional relational databases are indexed on a single value—for example, the transaction ID. If a trader wants to ask a question of another column in the database, perhaps looking at counterparties in a particular sector, they'd ask, "Who are our top 5 accounts in the tech sector?," then they would have to scan through every single record to find all the counterparties, group them, and then sum them. That's why it takes too long, Simek says.

It's similar to an Excel grid, he adds. To solve this problem you can use a non-relational database that can group together any data point that is represented in your dataset and make the data available much quicker then scanning all the records.

Today, as regular consumers, traders can easily use their mobile devices to answer questions by using a search engine like Google, but also access data related specifically to themselves. As apps become more interoperable, a cell phone can provide real-time info pertaining to an individual's health and daily physical activity, for example.

And at the enterprise level, traders are increasingly expecting that the same kind of functionality embedded into the tools they use every day are available in their professional tools. wt

Symphony to Make KYC Play as Part of Ongoing Rebrand

The chat and collaboration platform will tap into the trade and client lifecycle management spaces, beginning with an identity management service. By Rebecca Natale

In line with its decision last fall to rebrand as an end-to-end workflow platform for capital markets, Symphony Communications Services is making a play in the know-your-customer (KYC) space. The move is part of its plan to make client and trade lifecycle management services a core of its business.

In what the company is calling Directory 2.0—named similarly to Symphony 2.0, unveiled at Symphony Innovate last year, and Meetings 2.0, the enterprise-grade version of its video-conferencing-in-the-cloud service, the first version of which was released this spring—the company will create an identity management service, building on its existing database of basic corporate information, says Brad Levy, Symphony's newly-appointed president and chief commercial officer.

Levy previously led the MarkitSERV and Loan Platform businesses at IHS Markit, and currently sits on the US Commodity Futures Trading Commission's Technology Advisory Committee. In both roles, Levy has focused on digital identity and KYC solutions.

Richer Profiles

He says Directory, as it stands today, includes basic information such as name, phone number, email address, and maybe what someone's very high-level role is. The next version, which will likely go live next year, aims to create rich personal profiles that describe who each party is and alerts counterparties to changes in a relevant profile's state as they happen.

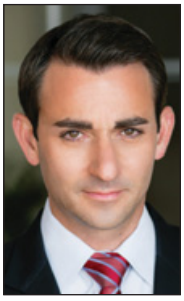
"What I'm trying to do is bring client lifecycle management (CLM) and trade lifecycle management (TLM) to a sounder footing and have them relate to each other more, specifically in someone's daily work or in a firm's relationship back to an account," Levy says.

For example, say a big bank has just established a new relationship and has to onboard that client. After that, the two perform a trade, but the next day, that client changes, such as they launched a new fund, someone's title changed, or are now connected to a new (potentially sketchy) entity. The bank then does another trade based on its idea of who the client is. But, the client has changed its relationship with the bank, even though its file still hasn't caught up.

As Levy puts it, if BlackRock or Pimco set up a new fund, part of Symphony's job will be communicating that and how that changes their identities to the rest of the Street.

He adds that another use-case for Directory is to help clients meet regulatory requirements, such as in the event a bank, as a counterparty in a swap, needs to repaper itself with its dealer in its Isda Agreements. That's a client lifecycle management moment where Symphony wants to help, Levy says. The other side of that is trade lifecycle management, to account for what someone has traded, what they want to trade next, and what the margin is.

"We're trying to solve for all these interactions, largely between the buy and sell sides, but really between any market participants, which could be virtually any combination including providers interacting with the buy or the sell side," he says.



Brad Levy
Symphony

Buy-Side Buy-In?

While Symphony has been most successful attracting banks and vendors as clients, the buy side has proved a more challenging demographic to capture for the six-year-old company. Though chat and collaboration tools remain Symphony's flagship products, an extension to CLM and TLM, as well as building tools for the front, middle, and back offices, could create a different value proposition for asset managers and hedge funds.

Building solutions for banks is a bit easier than building those for the buy side, Levy says, as banks are larger, comparatively more homogenous than the gamut of buy-side institutions, and have adopted and built their own technologies on a larger scale.

"Ultimately, it really comes down to: Do we understand the buy side's needs, their use-cases, and their problems, and are we building solutions to solve for them?" he says. "And while it could be similar and rhyme with the sell side, it could be completely different, or it may just be different in terms of the timing of when they have those issues. So I think making a version of what we do and applying it is fine; I think coming up with newer, different solutions that really cater to them [is better]."

Symphony will also look to create easier ways for the buy side to join its community, such as lowering the barrier to entry onto the platform. That could mean anything from the way they get onto a Symphony service, to the product that entry happens on, or even the commercial model around how the company thinks of the buy side today. wt

UBS Evidence Lab Uses Hospital Data to Profile Regional Recoveries

The unit is combining foot-traffic data and proprietary datasets derived from hospitals to develop a better understanding of outbreaks and predict a timeline for recovery. By Josephine Gallagher

At the beginning of the pandemic, geolocation data played a key role in measuring the outbreak of the Covid-19 disease, and provided something of a warning system for firms as to where the next series of lockdowns were most likely to unfold.

While geolocation data is still being used to monitor for second- and third-wave outbreaks, it is also being used to highlight a return of business for regional hospitals, says Jeremy Brunelli, global head of frameworks at UBS Evidence Lab, the independent research unit separate from UBS Research.

The team is monitoring hospital admittance by measuring the foot traffic entering and leaving hospitals, looking at factors such as inpatient and outpatient volumes, emergency room numbers, total surgeries, and elective procedures. It is partnering with an undisclosed data vendor that cleanses and anonymizes the hospital traffic dataset.

"This is an exclusive dataset that we have, and we get about two reads every month. We have an initial read, which is not the full sample, but it gives us an early indication, and then we get a final read at the end of the month. This is a dataset where we can see a dramatic decline in the volumes [of elective procedures and surgeries] driven by Covid-19," he says.

So, for example, in Washington State, which was the first epicenter of the coronavirus in the US, hospital admittance data showed a significant drop in the number of non-emergency procedures back at the beginning of the pandemic, but those numbers are now improving. In April, there was a 70% year-on-year decline in non-emergency medical procedures, May saw a 50% decline compared to the previous May, June saw a still robust 22% decline, but July saw only a 7% decline, according to Brunelli.

The Evidence Lab uses the Bayesian inference approach to combine multiple datasets to see if they support or disprove a probable investment hypothesis. This is where alternative datasets on health care can be valuable, says Brunelli, as they can more accurately reflect world events than traditional market data.

"We would create this big mosaic of datasets and try to present it in a very digestible way for investors, so that they can look across this mosaic and start to increase or decrease their confidence around some hypothesis they have," he says.

To supplement the hospital admittance data, UBS also conducts a proprietary survey, called a pulse check. The survey puts questions to 40 different C-level hospital executives in the US to learn about the current conditions, in terms of surgery procedures and capital expenditure plans, including funding spent on technologies and beds. Brunelli says that the two data products—the foot traffic and the survey—provide complimentary views on the events unfolding in hospitals

"There are still a significant amount of delays, but they've also improved as things have reopened and recovered, especially with orthopedic surgeries—we've seen 43% of hospitals are reporting delays versus 58% in May, and plastic surgeries and endoscopies have also seen a decrease in delays," he adds.

Yet, these various healthcare insights are not used in isolation. Brunelli says they are most effective when used to compliment other foot traffic or mobility datasets that look at activity around retail shopping, public transit usage, and car traffic congestion, to help understand the pace of recovery in different locations.

For example, mobile device application publishers use Google's software development kit and tie it to Google Maps, and embed it into their own technology frameworks. The location data of the person using the app is then pulled, aggregated, anonymized, and then sold to users like UBS, and they can more accurately see spikes in traffic or activity around retail centers. The Evidence Lab also takes in satellite data from location, navigation, and map technology provider TomTom to monitor auto congestion, and combines that with metrics on app usage from Sensor Tower, which provides data around mobile app usage.

"We use hundreds of vendors and also have, what we call, an internal harvest team," Brunelli says, "where we web-mine thousands of different types of data from the internet, which we curate and create metrics with." wt

BNY Mellon, Deutsche Bank to Extend FX API for Indonesia, India

The two are working out the necessary regulatory, tax, and documentation needed to provide custody services for foreign exchange transactions in the two countries. By Wei-Shen Wong

Investing in foreign stocks and bonds can be more cumbersome than it first appears. Often, many of the workflows and processes go on behind the scenes between firms' back-office operations, with multiple back-and-forth communications between counterparties' custody teams.

The complexity of this process is exacerbated when dealing with investments in countries with restricted currencies—currencies subject to currency controls imposed by their governments.

Some governments impose capital controls limiting the flow of funds into and out of a country to provide stability to the value of their currency. Examples of restricted currency countries include South Korea, China, Russia, Brazil, Malaysia, India, Indonesia, Thailand, Taiwan, and the Philippines. Investing in stocks and bonds in restricted currency countries requires investors to convert into the local currency linked to the assets.

Speaking separately to *WatersTechnology*, both BNY Mellon and Deutsche Bank explain that securities processing in restricted currency countries is mainly manual, and often managed using spreadsheets. The banks are aiming to bring a touch of automation to the process.

Gordon Alexander, head of client access and flow execution for Asia-Pacific at Deutsche Bank, says helping international investors conduct FX conversions to buy a security can sometimes take as long as 36 hours to complete, as it involves satisfying various rules and approvals. Throw in the additional back-and-forth communication between operations, global custodians, and sub-custodians, and different time zones, and you have the perfect recipe for a long and drawn-out process.

To ease this process, BNY Mellon and Deutsche Bank developed an API-enabled FX workflow that eliminates several manual processes. In July, they applied the solution to custody of FX transactions in Korean won, successfully reducing the pre-trade lifecycle from hours to seconds.

Now that the solution is live in South Korea, the banks are working towards introducing it in Indonesia and India by early next year.

Darren Boulos, head of FX for Asia-Pacific at BNY Mellon, says South Korea was the proof-of-concept market for the joint solution, as it is probably one of the more straightforward currency markets the bank operates in. "For Indonesia and India, there are other nuances such as withholding and other taxes that have to be added to the procedure, which complicates the process," he says. "They're the next markets that we're tackling. They are very large markets for our clients, and it's important for us to try to achieve the same result of bringing the approval process down to seconds."

To replicate the solution for Indonesia and India, BNY and Deutsche Bank are working to ensure that the currency leg of a transaction can be executed with the required tax calculations, regulations, and documentation.

Alexander says that because of the different nuances of each market, the workflow around a trade can prove more complicated than the FX conversion itself. "For different security markets, there are different types of rules that the custodian is required to follow in order for the FX to be executed. So the main work involved is not actually extending the APIs with new currencies—it's really creating the rules and the scenarios for each market," he says.

Starting Point

For BNY, the challenge of dealing in restricted currency markets comes from the manual processes used to perform the necessary validations and approvals before executing a trade. "Prior to entering into a foreign exchange transaction in those markets, you have to communicate account balances, make sure trade details are correct, and that any income and corporate action components are approved and have settled," Boulos says.

The manual process of dealing with sub-custodians in restricted markets—where managing approvals for restricted currencies are predominantly spreadsheet-based—was a heavy operational burden. "There are a number of spreadsheets in any given currency, and it takes a significant amount of time to get an approval—as much as 12 to 18 hours to run the process from end to end," he says.

While it doesn't take long to execute the FX trade itself, getting the rate information back to the end investor can take longer due to the friction caused by various steps in the process, whereas this new process now has an API response time of between 10 and 15 seconds, Deutsche Bank's Alexander says. wt

Aquis Exchange Progresses with NEX's Tech Migration

The exchange initiated the tech overhaul after realizing some of the NEX platforms were "out of date" and "terrible". By Hamad Ali

In 2019, London-based Aquis Exchange announced it had purchased NEX Exchange from CME Group. At the time, Aquis CEO Alasdair Haynes told *WatersTechnology* that "we will not be taking their technology; we will be implementing our own technology solution."

Now, 13 months later, that migration is nearing completion.

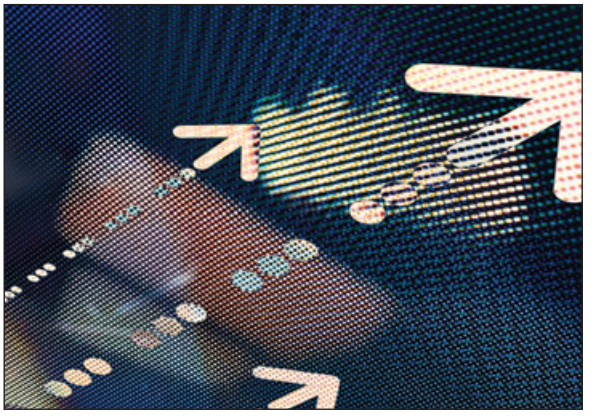
The NEX market is now known as the Aquis Stock Exchange, or AQSE. Since the acquisition was finalized in March, AQSE has migrated to the matching engine, surveillance platform, and data distribution technologies all developed by the Aquis Technologies team.

Haynes says that some of the platforms acquired in the deal were "out of date" and even "sort of terrible," so Aquis officials knew from the get-go that they would move everything over to the Aquis tech stack. While there are still "a combination of proprietary systems" from NEX running in parallel with the Aquis technology deployed on AQSE, those legacy systems will be phased out completely in the coming months.

"We will run on one platform; I do not want to run on two different platforms," Haynes says. "That would be a massive mistake."

Like the large-cap Aquis Exchange equities trading venue, AQSE—which is geared toward small-cap stocks—will start multicasting data to clients in the future. Currently, AQSE relies on FIX messaging over TCP/IP, rather than the one-to-many data distribution model that multicast offers.

As for future upgrades, Haynes says Aquis will examine connectivity



tools and APIs that will allow AQSE to better interact with the major trading platforms in the small-cap space.

"The market makers tend to use two systems: They either have their proprietary system, as in the case of [brokerage] Winterflood Securities, or they use Ion, which is the old Fidessa system," Haynes says. "We have to be able to connect to those so that these market makers can continue to trade the way that they have always traded, and that is quite a lot of technology change. All this is down to getting better connectivity."

Shaking up the Exchange Model

AQSE is one of only four equities-focused Recognized Investment Exchanges (RIEs) in the UK—a license that confers certain regulatory exemptions. NEX's RIE status was a key factor in Aquis' decision to buy the exchange.

AQSE has taken the approach of segmenting the exchange into its Main market and its Growth markets. The Growth market—which will look to compete with LSEG's AIM growth market—is divided into two segments: Access and Apex. Access is for companies with less than £10 million market cap and a free-float market cap greater than 10%. Apex is for companies with a market cap of between £30 million and £60 million, and will have its own set of listing and trading requirements. Haynes describes this market as AQSE's "sweet spot".

The Main market is for larger companies with a track record of three years or longer, as well as other issuers who are able to comply with the more demanding requirements of UK regulatory requirements. Like Aquis Exchange, AQSE will operate on a subscription model, charging users per their messaging traffic, rather than by a percentage of the value of the stock they trade.

"One of the things we are going to focus on is making quite certain that execution-only brokers in retail, as well as wholesale investors, will have easy access through technology to make certain that they have the data, they have the information, and they have the capability of trading on these stocks," he says.

Aquis is also considering automating the documentation processes for new companies listing on AQSE, creating templates for the admissions documents and growth prospectuses that are required for listing.

"That should make things cheaper, more efficient, and faster for companies that are looking for capital," Haynes says, adding that automating these processes would allow companies to sidestep middlemen like nominated advisors and their fees. He says the exchange will be working with lawyers to have an automated method ready for the end of the year. wt

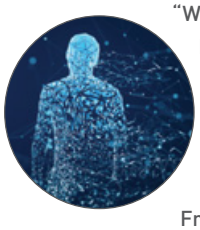
OPEN OUTCRY

"At its core, ZTA is essentially saying that there is no longer implied trust between systems just because they exist on the same network. It's extremely useful and powerful, but also can be disruptive to how employees are used to working. It will be a huge shift in the way firms operate." **Phil Vachon, a security architect at Bloomberg**

» *see page 12 for full feature…*

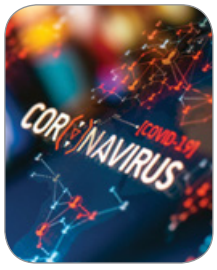
"The deployment felt like a 'mission impossible' task, particularly in Manhattan, which was being decimated by Covid. People were unable to come into the office, and we needed to very rapidly figure out [how] to handle voice trading in a way that nobody had ever planned for." **Christopher Purves, co-head of execution and platform and co-head of digital at UBS**

» *see page 32 for full feature…*



"When we are trying to transmit data, if the protection is not high enough, people can still collect your data today, waiting to crack it tomorrow. People used to think it is stupid, this will not happen. But I can tell you even in the last few years, there have been a number of very strange activities. From time to time we can see the entire internet traffic being diverted to some servers in Russia or in Eastern Europe." **Andersen Cheng, CEO at Post-Quantum**

» *see page 20 for full feature…*



"There are still a significant amount of delays, but they've also improved as things have reopened and recovered, especially with orthopedic surgeries—we've seen 43% of hospitals are reporting delays versus 58% in May, and plastic surgeries and endoscopies have also seen a decrease in delays." **Jeremy Brunelli, global head of frameworks at UBS Evidence Lab**

» *see page 8 for full feature…*

"The odd lots problem is a problem that is worth tackling. I just don't think the SEC has tackled it the right way." **Phil Mackintosh, chief economist at Nasdaq**

» *see page 26 for full feature…*

"There's a phrase in software engineering—'there's no such thing as free lunches.' Since it was invented, everyone has tried to find shortcuts to try to make it a faster process, make it a more deterministic process. And then every attempt when you do it at scale, and you do it over a long period of time, the corners that you cut to get to something quickly, usually you end up paying for in the end." **Jon Butler, CEO of Velox Financial Technology**

» *see page 16 for full feature…*

"It's been up to firms to self-regulate. It's been up to firms to say, 'Okay, it's a pain to have all this mobile surveillance functionality, and roll out all these devices, and it costs money.' But also, if we don't monitor any of these mobile devices that employees are definitely using for work, then they're basically just whistling past the graveyard until someone does something really, really bad." **Danielle Tierney, a senior advisor on market structure and technology at Greenwich Associates**

» *see page 4 for full feature…*

"It's a way of removing from the process the number of interactions or touchpoints you have between global custodian operations, sub-custodian operations, sub-custodian operations to [the] sub-custodian trader to confirm rates to global custodian operations, and trading for them to basically do the execution then come back to the end investor. That's a lot of handshakes in that process." **Gordon Alexander, head of client access and flow execution for Asia-Pacific at Deutsche Bank**

» *see page 9 for full feature…*

Trust Issues

The Covid-19 outbreak heightened the need for IT and data security, exposing areas for potential improvement. One option is to lock down sensitive areas using a practice called Zero-Trust Architecture, which offers a host of benefits, but brings with it some practical challenges that firms need to get used to. By Max Bowie

After the Covid-19 pandemic took hold globally, financial firms not only grappled with technology and connectivity issues associated with enabling traders, investment bankers, and others to work remotely, but these institutions have also needed to address security concerns around how employees access sensitive systems and data outside highly secure offices and trading floors.

These concerns range from whether a connection between a server in a datacenter and a device registered to an employee is secure and encrypted, to verifying the identity of the employee using that device, and whether they are exposing their secure access to the risk of data breaches.

One lasting impact of the coronavirus may be to drive adoption of more stringent security protocols, such as Zero-Trust Architecture (ZTA), which works exactly the way it sounds: Everything on a network assumes it cannot trust anything else on the network as default, and requires authentication and verification of each person, device, or application attempting to access it.

Phil Vachon, a security architect at Bloomberg, says that a decade ago, employees had access to sensitive applications simply because they were using a corporate desktop that was connected to the same network as the application. ZTA upsets that model, as it adds layers of authentication to ensure people can only access the specific applications they need to do their job.

"At its core, ZTA is essentially saying that there is no longer implied trust between systems just because they exist on the same network," says Phil Vachon, a security architect at Bloomberg. "It's extremely useful and powerful, but also can be disruptive to how employees are used to working. It will be a huge shift in the way firms operate."

Interest in ZTA has risen in the past couple of years, but are firms acting fast enough? While that might have been the case, Dr. Chase Cunningham, principal analyst covering security and risk at Forrester Research, says the Covid-19 pandemic is actually accelerating security projects.

"Our original projection was that banks would be done with ZTA by 2025. But with Covid, we think that anyone not done with ZTA by 2022 will be behind the curve, and will be left open to breaches, and the regulatory fines that such breaches incur," Cunningham says.

Firms have implemented security measures for years to govern who can access what systems, and the principles of ZTA have been around for a decade or longer, depending on who you ask. Charles Porter, CTO of distributed ledger-based digital-rights startup TradeX, describes how, previously in his career while working on a major investment bank's architecture and engineering team, he was not able to access production systems without first scheduling a specific time to access a system, then being assigned a temporary support login to access only that system at the allotted time.

Scott Rose
NIST

Zero-Trust takes this a step further, requiring these kinds of authentication for even those who need to routinely access systems.

Scott Rose, a computer scientist at the National Institute of Standards and Technology (NIST), adds that some ZTA models track behavior and understand if any access is out of line with someone's profile. "For example, if they are trying to access something they don't need, or if the number of access attempts by someone or a device goes up dramatically," they will be locked out.

The bulk of any ZTA program should take place behind the scenes. But for those responsible for underlying technology architectures and market data infrastructures, the impact is more visible and disruptive.

> "I've never seen a ZTA project go flawlessly. You have to weigh productivity against the risk of downtime during implementation, and maybe focus on low-risk areas to deploy to first, before looking at non-critical systems, and doing it in phases that allow people to get used to—and benefit from—any changes. For the end user, if it's done right, it should be a seamless experience."
> **Phil Vachon, Bloomberg**

Phil Vachon
Bloomberg

A market data technology executive at a major US bank says their firm's ZTA program forces staff to obtain multiple levels of permission each time they need to access servers running data systems—even if their job is maintaining those systems on a daily basis—which can result in routine tasks taking up to 20 times longer than previously.

However, Grigoriy Milis, CTO of RFA, a provider of IT services to buy-side firms, says that while the ZTA process can be frustrating at times, the foundational technology elements of the architecture have matured and are more widely adopted, making for a "significantly more pleasant" experience.

He says that "ZTA is having a renaissance" right now for two key reasons. First, banks and asset managers are

> "ZTA is heavily dependent on a service-based architecture. When you break down applications into their components, the services and microservices need to understand each other and who is accessing them. It's like, instead of locking your house, you lock down everything inside it."
> **Guy Warren, ITRS**

increasingly running significant portions of their architecture in the cloud. Second, the technology that runs ZTA has evolved. Multifactor authentication is now a standard; granular permissioning has improved; segmentation has matured; and companies largely already have a device management structure in place. As a result, it's now easier to build dynamic policies into ZTAs by observing a user's behavior, Milis contends.

"For example, if I'm based in New York and, after logging out in New York, I'm seen logging in from Hong Kong, that would be identified as risky," he says.

'Growing Pains'

To help with ZTA adoption, Forrester Research created the Forrester Certification Program to familiarize market participants with the main principles of ZTA, create standards, and unite the industry around a harmonized approach. The on-demand program includes about 20 modules of videos, written materials, and assessments. The whole program can be completed part time over two weeks, or full-time in two working days.

"All the challenges of ZTA are understandable growing pains facing IT organizations today," Vachon says. "Workforces are increasingly mobile; people are using their own devices, and bring your own device (BYOD) is a big motivator. But this is how people expect to work now—or have to, for example, under Covid-19. … It's a natural evolution for the industry to think this way about security."

Certainly the ongoing pandemic has forced the industry to reevaluate security procedures for people and computers accessing core corporate systems from their kitchen table rather than the boardroom table, but many measures so far have focused on securing those new endpoints, rather than tackling large-scale, enterprise-wide security protocols.

Guy Warren
ITRS

For example, Porter says TradeX's platform can be an enabler in firms' drive toward implementing ZTA, leveraging their existing permissioning systems and monitoring the flow of data internally to ensure that only those who need access to a system actually have access to that system.

"For any file transfer protocol (FTP) site where you log in with a password, you're always going to get people trying to access that," Porter says. "With us, you have to be a registered user with a login and password, and be on a registered end-point with a piece of software that securely communicates back to the server … and you can't generate a key to access any data unless you have that software."

Though ZTA restricts internal access to sensitive data or applications, it aims to hinder external attacks—ransomware or data exfiltration attacks, among others—that conceal their origins using the labyrinthine layers of complexity that comprise modern enterprise architectures, and use their point-of-entry to impersonate a device or user with existing authorization to access important data systems, says NIST's Rose.

Sometimes the easiest point of entry for an attacker is an on-network device whose function may be so mundane that it is simply overlooked, such as printers and copiers, adds Bloomberg's Vachon.

"Printers are terrifying. They have a lot of privileges, such as the ability to scan-to-email or scan-to-folder, and therefore represent a large risk because they can access a lot of assets," he says. "So you'll have to put in place a lot of extra security controls around printers; you have to say that a corporate laptop can't print directly to any printer—instead, it has to go through another system first. So a device in one trusted zone can't interact with a device in a less trusted zone."

The risk associated with Covid is that an attacker could breach a home worker's technology and use their remote access to infiltrate corporate networks. Hence, the work-from-home Covid economy presents the perfect justification for enacting a ZTA strategy—to ensure that each remote access is who or what it claims to be.

But depending on firms' existing systems, the very rules set up in the past to minimize the risk of attack may make it harder for firms to implement changes to prevent future attacks—for example, whether they allow major changes to be implemented remotely, such as under current circumstances. Indeed, the more lightweight a firm's technology is, the easier it may be to move, says Guy Warren, CEO of real-time systems monitoring technology vendor ITRS.

"ZTA is heavily dependent on a service-based architecture. When you break down applications into their components, the services and microservices need to understand each other and who is accessing them. It's like, instead of locking your house, you lock down everything inside it," he says, which has built-in monitoring capabilities for microservices, such as Red Hat OpenShift and Kubernetes. "Because the microservice doesn't know who the user is, they are likely to take the ZTA approach."

But not all firms are yet that advanced. Forrester Research found that progress spans the full spectrum, from early stages to advanced deployments.

"We're in the early stages, and are certainly hampered by legacy infrastructure," says an enterprise security executive at one large North American bank. "We are finding that the more we abstract from the physical technology layer, the more things we can do around ZTA. It's easier to make changes when you are dealing with the software layer."

Therefore, any ZTA strategy needs to be developed alongside adoption of a modern architecture. And while a firm's security function may not be able to singlehandedly drive IT modernization, it needs a seat at the table of those tasked with setting the agenda, the executive adds.

Casting a Wide Net

But ZTA needs to extend beyond that table and the primary offices where firms' users, devices, and corporate networks reside, to encompass off-site locations that constitute important kernels of infrastructure and house huge swathes of sensitive data about a firm, its activities, and its customers, says Vachon.

"The crown jewel of any financial services business is probably its datacenter. It houses customer data, trade data, and systems that give a firm its critical advantages. So, to me, the whole concept of ZTA naturally must extend to datacenters," Vachon says.

Under legacy infrastructure rules, on-site applications could access off-site servers. But since any on-net datacenter is vulnerable to attempted cyberattacks, firms must apply the same controls to their datacenter that they would to assets housed within their own four walls. "You can't stop attackers in their tracks if you don't have resources and assets ring-fenced by controls with depth of authorization," he adds.

'Fertile Ground for Shadow IT'

However, a natural response to change is that people will try to minimize their day-to-day work.

"It's inevitable that people will get creative and find workarounds, so you have to be innovative," says Bloomberg's Vachon. "You need to facilitate the business operating while you are making these changes. And you have to understand your business inside and out, and talk to the business users, and involve them in these technology decisions—all with the understanding that if what you're doing is creating too much inconvenience for end users, you're creating fertile ground for 'shadow IT.'"

For example, if a firm restricts employee access to an internal chat program, they may simply set up their own Slack group outside the auspices of corporate networks or a firm's ability to monitor it.

"It's about having a good plan for how you get people used to the concept of ZTA, and how you not only will disrupt but also enhance how users do their work, and actually simplify the way people use systems," Vachon says. "I've never seen a ZTA project go flawlessly. You have to weigh productivity against the risk of downtime during implementation, and maybe focus on low-risk areas to deploy to first, before looking at non-critical systems, and doing it in phases that allow people to get used to—and benefit from—any changes. For the end user, if it's done right, it should be a seamless experience."

ZTA also can't be done in a "big bang" approach. While it must have a single purpose, the complexity of firms' infrastructures, and legacy technology challenges, mean that a phased approach is inevitable, says the bank enterprise security executive.

"If it's too much to tackle across the enterprise as a whole, we look at the criticality of each business line, and ask what systems would benefit most from increased security or better operations," they say. "Even if we do risk stratification, we look at it across the organization. If something is high risk in the capital markets, it is probably also high risk in retail, too. So we work with all teams and hopefully build a cohesive model or patterns that can be used across the bank."

Dr. Chase Cunningham, Forrester Research

Good Housekeeping

ZTA offers secondary benefits beyond its core security aspects. The bank exec admits that the challenges of working under ZTA have forced staff to be more conscious and critical of every time they request access to a system, but they're also cognizant of fixing issues the first time around so that they don't waste time repeating the authorization process to fix follow-up errors.

"It did make us realize that we were being somewhat liberal with our accesses before," and as a result tightened up internal processes, the data executive says.

And in the event of a "break-the-glass" emergency where someone may need root control immediately to restart a system after a malfunction, an engineer or administrator must still log the cause and time taken for access to a system. IT may then question how they plan to reduce that number. That, plus the fact that logging each instance makes accessing systems far more onerous, should encourage firms to also work more efficiently under ZTA, says ITRS' Warren.

"To reduce the number of instances, you need good housekeeping routines. So you need to move anything you do routinely into your weekly 'housekeeping,' so that you only have to dive in to fix something unexpected," Warren says.

He and Forrester's Cunningham agree that harnessing ZTA to make banks' most critical data and systems bulletproof will automatically deter external threats because they represent more effort and less chance of success to would-be hackers, while NIST's Rose says firms should view ZTA as an "opportunity" to refine and improve their existing workflows. "It forces you to reevaluate and improve your business processes," he says.

> "I tell people that security is about enabling the business—it's business enablement through security strategy. If there is a silver lining to the Covid crisis, it's that it proves that ZTA is the correct approach to security, and that there is no perimeter anymore—we're all outside of it."
> Dr. Chase Cunningham, Forrester Research

And therein lies the key to success: Though ZTA is a technology architecture issue, it is important to treat it not purely as an IT problem, but to involve the business side of an organization, and assess and articulate the benefits and risks in terms of business objectives.

"I tell people that security is about enabling the business—it's business enablement through security strategy," Cunningham says. "If there is a silver lining to the Covid crisis, it's that it proves that ZTA is the correct approach to security, and that there is no perimeter anymore—we're all outside of it." wt

How Low Can Your Code Go?

What if you could create your ideal, fully functional application without writing a single line of code? With low-code and no-code platforms, you can—with a catch … or two, or three, or four. By Rebecca Natale

There's no such thing as a free lunch, or so it is said. Low-code technology providers are looking to challenge that axiom.

With the low-code application market set to reach nearly $50 billion by 2026, its place in the upper echelons of financial services, among other industries, is cementing. Low-code platforms, and their sibling no-code platforms, proposition something almost too good to be true: that anyone can quickly build their own applications with minimal to no coding expertise. The premise is contradictory to the contest between Big Tech and High Finance to hire the best and brightest engineers

To be sure, low-code and no-code software contains code. It's just that the user side need not bother with it, as apps are built visually, or "Lego-style," by custom dragging and dropping pre-configured components and widgets onto a blank slate.

Proponents of low-code and no-code "engineering" assert that it circumvents legacy vendor technology, solves the buy-vs-build dilemma, and fosters an army of citizen developers, each of whom double as business experts and technologists. They also posit that as Covid-19 pandemic-induced remote working further takes root, leaving on-premises hardware solutions and tech departments often miles away from users, the practice will quickly go from accessory to necessity.

Across the aisle, skeptics say good software takes no shortcuts, and that there's a trade-off between ease and error, especially at the enterprise level, making a project more time-consuming and expensive to maintain in the long run.

"There's a phrase in software engineering—'there's no such thing as free lunches,'" says Jon Butler, CEO of Velox Financial Technology. "Since it was invented, everyone has tried to find shortcuts to try to make it a faster process, make it a more deterministic process. And then every attempt when you do it at scale, and you do it over a long period of time, the corners that you cut to get to something quickly, usually you end up paying for in the end."

Despite mounting buzz, those same skeptics argue the best use-cases for low-code and no-code remain simple, manual tasks and workflows like approval chains, useful in the way that robotic process automation (RPA) is useful.

However, the tech is relatively young—though that, too, is up for debate—and

sources say that as adoption grows, so will its propensity toward more complex systems, such as trading technology and data delivery. The central question, then, is how much disruption, if any, do the low-code and no-code styles of development pose to finance—and indeed, to software development as a field?

Lay of the Land

Before low-code and no-code were what they are, they had a different name. Emerging in the 1980s, they were once known as CASE technologies—a tidy acronym for computer-aided software engineering—or expert systems, which are logic-based computer systems that solve problems through "if-then" rules. They garnered hype and praise in their own right, before peaking in the 1990s, with businesses citing frustration over rigid adherence to design conventions and restrictiveness in developing complex, custom applications.

Now seemingly back from the dead—perhaps not a surprise for 2020—several vendors in the space are starting to make some noise. Five-year-old Genesis launched its low-code application platform specifically designed for capital markets in October of last year, following a $3 million Series A funding round led by Illuminate Financial and Tribeca Early Stage Partners. This past May, it joined the Fintech Open Source Foundation (Finos).

A rival company, three-year-old Unqork, which raised over $50 million in February to expand its platform, boasts an enterprise-grade no-code platform used in a bouquet of industries, including financial services, healthcare, education, real estate, and government. It recently teamed up with consulting giant Deloitte on a number of initiatives, including small business lending and broader financial business challenges, and counts Goldman Sachs among its investors.

> "Software is a time-consuming, expensive, error-prone kind of skill that people, especially in the enterprise, struggle to do efficiently, so you end up with big banks spending billions of dollars on it. And so, there's always been this kind of thinking—is there a shortcut? Is there a way we can just simplify this?"
> **Jon Butler, Velox**

Jon Butler
Velox

And of course, Big Tech is also starting to take notice. In June, Amazon Web Services (AWS) jumped aboard, rolling out its own tool—though not specifically aimed at finance—called Amazon Honeycode, which allows users to build web and mobile apps without writing any code. Two weeks later, New York-based alternative data analytics provider Apteo released Predictive Insights, its own no-code predictive analytics platform, a move which Apteo's CEO, Shanif Dhanani, hopes will expand the company's client base beyond financial services.

A Case for CASE 2.0

Gary Hoberman, founder and CEO of Unqork, began programming in the fifth grade. Somewhere between then and now, he cultivated an ambitious goal: to see his company capture its entire addressable market—$500 billion per year—which, he says, accounts for every dollar's worth of custom code written across industries. He adds that in his view, the role of a software developer is obsolete.

"I would say the word 'developer' should be eliminated because the word itself actually has no meaning," Hoberman says. "Developer means someone who writes code; it doesn't mean they actually solve the problem."

He says this is evidenced by the percentage of enterprise tech projects that fail. A 2015 publication by Boston Consulting Group found that 93% of large IT projects with budgets greater than $10 million failed to deliver value to their organizations. A more recent paper published by market research group Forrester Consulting found that out of 315 US, UK, and German firms—financial firms made up 16% of that figure, the largest demographic—35% of projects failed to meet their original business intent, 38% failed to meet initial timelines, and 34% failed to finish within budget.

As a second premise, Unqork's platform doesn't allow any users to override any of its own functionality unless it's programmed with the ability to be turned on or off—a stipulation that, in a certain light, seems to run contrary to no-code's draw of customization and vendor freedom, though it does ensure the service stays as close to its code-free promise as possible.

Unqork's first clients were in the paper-intensive insurance sector, building no-code user interfaces—wizards, which typically require thousands of lines of code be built—for companies like Liberty Mutual, Principal, and the Hanover Insurance Group. Then, the company entered banking and capital markets, with Goldman Sachs as its first client.

Before making its first $22 million investment into the startup, the bank rolled out its first tool powered by Unqork, reported *American Banker* last year. The tool collected applications and data from employees at the bank wanting to apply for an in-house incubator called GS Accelerate, which in 2018, received 1,000 applications.

"We became a system of record there, not just a workflow system," Hoberman says. "We not only could be a front-end to your trading platform, your execution management system (EMS), your order management system (OMS), your clearing, your reconciliation, but in addition, we will be the core system; we will be the EMS and OMS. We will be the actual high-speed transaction to the Street."

Gary Hoberman
Unqork

Genesis co-founder and CEO Stephen Murphy has similar thoughts. Genesis can be used for simple business process management (BPM) use-cases—and indeed, this has been a large focus for customers, Murphy says—but there is a budding interest from firms that want to use low-code to automate more complex financial processes.

Stephen Murphy
Genesis

In February, institutional brokerage XP Investments partnered with Genesis to develop a treasury product to automate workflow management between the trading desk, institutional clients, and wealth managers, which was developed and deployed within weeks. Now, Murphy says, Genesis handles all of XP's fixed-income trading workflows and event processing.

The low-code movement has been enabled and empowered by the rises of microservices and application programming interfaces (APIs). While a monolithic enterprise application might be made up of a database, a user interface, and a server-side application, and available through one web app, a microservices architecture connects the capabilities of a business to users via open APIs.

Because these are built in standardized formats like REST, they provide a means for software systems to "talk" to each other and facilitate integrated apps. APIs can be bundled into architectural frameworks like API gateways, which act as a single point of entry for multiple APIs.

Microservices also serve as the foundation for Murphy's Genesis. Beginning as a microservices infrastructure stack for capital markets, the company began positioning itself as a low-code application platform only about two years ago. It launched its full-fledged low-code application platform, LCAP, in October of 2019, prior to which it had released low-code and no-code web-based tools.

But there's a striking difference between the likes of Unqork and Genesis, one perhaps rooted in practicality versus purity.

With Genesis, users can write their own code. Genesis will continue to take care of the innermost pipes—like how low-latency messaging will work between microservices, for instance, or complex real-time event monitoring—while users can enhance and customize their front-ends with additional code. The platform is also equipped with code libraries containing Python, Java, Angular, React, and other languages and libraries, for programmers to utilize.

In the next month, Genesis will announce the completion of a complete new trading platform built on its service, combining business-process-management workflows, new trading technologies, and a lot of legacy integration using both in-house and third-party apps, Murphy says. It will be the first of its kind for the platform, but it signals a certain maturation.

'Everything, Squared'

A CTO at a US investment bank says people have been talking about these solutions for years, over which time he has formed the opinion that they're a good choice for workgroup applications, but no one would seriously consider using them for any enterprise application.

"For instance, DealCloud was originally built on Sharepoint, which could be thought of as a low-code platform. But eventually, they had to migrate to a real platform. Also WordPress is another low- or no-code platform for websites, and it is terrifically popular, but at some point if an application has legs it will outgrow these platforms, and then they will need to be migrated to a more performant platform," the executive says.

Four years ago, Jon Butler left Goldman Sachs, where he was a managing director for 15 years. He went on to spend a little more than a year as the head of capital markets technology at Deloitte, before co-founding Velox in 2017. Though he left the bank before it formed its relationship with Unqork, he says Goldman had been considering low-code and no-code solutions for years prior with little success.

As it relates to trading functions, he is still skeptical of the technology. As a software engineer by trade, he understands why others might call him a "dinosaur" in his thinking, and he understands why those same people would want to move away from traditional programming—but he doesn't think low-code and no-code are completely viable alternatives, at least not on a big scale, just as each new programming language written doesn't replace those of yore.

"Even 50 years ago, software was everything. And obviously now, software is everything, squared. Software is a

> "It's a good enabler for an industry that is still heavily reliant on huge-scale deployed software with huge-scale on-prem data storage, that has spoken a good game about cloud migration, big data, AI and all these other things, but in reality is still in the very, very early stages of its adoption of those."
> **Mark Beeston, Illuminate Financial**

time-consuming, expensive, error-prone kind of skill that people, especially in the enterprise, struggle to do efficiently, so you end up with big banks spending billions of dollars on it," he says. "And so, there's always been this kind of thinking—is there a shortcut? Is there a way we can just simplify this?"

All the different programming languages are more or less built on top of one another. In programming's humble beginnings, there was machine code (binary 1's and 0's) and assembly code (a low-level, plain-text version of machine code). These are most easily digested by a processor. On the other hand, a high-level code—say, Java—will get compiled down to machine code in order to run on a processor. No-code and low-code are extensions of this, Butler says, which creates an additional level of abstraction that makes software building easier, faster, and more accessible to those with non-programming backgrounds.

When banks are spending millions, or billions, on a tool or platform, they won't settle for something that "just about works," Butler says. At Goldman, end-users of the bank's low-code and no-code early experiments, often wrote and re-wrote around the edges of the tools, what Butler calls the movement's "back door" problem.

Back doors, or custom configurations—a capability Genesis offers, but Unqork does not—is where trouble often started. On one hand, it allows the creator to tailor the tool to their specific wants. But on the other, it opened it up to security and control issues, and the organization takes on risk.

Mark Beeston
Illuminate Financial

Dan Schleifer
Cosaic

"You create a bit of a monster [this way]," Butler says. "In the old world, the technology department builds the technology. They have controls around it, they have processes around figuring out where the code is, version control, and security, and all this stuff. With low-code [and] no-code, anybody can write anything, so what you end up with is thousands of these apps that become critical to processing, but aren't really fully controlled."

At Odds

Interestingly, the low-code and no-code movement is adjacent to, and in some respects, directly opposes another trend in capital markets, one that arguably has an even stronger footing—the desktop app interoperability movement.

If low-code and no-code aim to give users the freedom to build their own user interfaces, the method of the three interop kingpins—OpenFin; Glue42; and Cosaic, formerly known as ChartIQ—is to keep the complex interfaces of users' third-party apps, and make those user interfaces (UIs) talk to one another.

Dan Schleifer, co-founder and CEO of Cosaic, says low-code and no-code have a promising pitch, but even as users build their own interfaces, they can't totally get away from those of their third parties, and the ongoing maintenance cost of a low-code system grows over time.

"Usually folks only build out a tiny fraction of the user interface for a given app—say, a few bits of Salesforce—and then the user still needs to go back to the main vendor UI for anything but the most basic of functions, such as advanced search, long-tail features, etcetera," Schleifer says. "Not to mention, as the vendors innovate and deliver new functionality, you then have to go in and replicate it in your own bespoke low code UI."

He says, however, that the use-case around order and execution management systems (OEMSs)—Unqork says it can serve as an OEMS—is interesting. Firms often end up with a mishmash of OEMSs and they want to pull them together into a single interface (this problem also is giving way to the rise of server-side interoperability). But, Schleifer says, it's unclear how well it works to accomplish this in reality, and whether it simply further entrenches what the OEMS users have and don't like.

It's possible then, that the question isn't whether low-code and no-code are good or bad, or whether they work or not. It might become: How compatible are they with finance?

Mark Beeston, founder and partner at venture capital firm Illuminate Financial—a leading investor in Genesis—says finance has very particular needs, which makes many, if not all, of the low-code and no-code solutions available in the broader software-as-a-service (SaaS) world non-contenders in the space. There are standards for resilience, latency, and security—all of which are filtered through the oversight of an up-close regulatory eyeball. It's an industry that, by design, has no silver bullets.

It's easy, then, to recall a very different craze that received a lot of hype but very little production: "the 2016 blockchain gold rush, where it was like, 'Hey! We've got a technology!' Great. Now show me [an actual] problem," says Beeston.

That said, Beeston takes the view that low-code and no-code have their part to play in the evolution of financial technology, marking a distinction between evolution and revolution.

The bank CTO says something similar, which is that any software development platform will provide code that users don't have to write in the form of libraries to use, and low- and no-code can be thought of as just being further along this spectrum.

"It's a good enabler for an industry that is still heavily reliant on huge-scale deployed software with huge-scale on-prem data storage, that has spoken a good game about cloud migration, big data, artificial intelligence and all these other things, but in reality is still in the very, very early stages of its adoption of those," Beeston says. "The Lego-block approach to microservices infrastructure, and the low-code product generation that can sit on top of that framework, is a big enabler of successfully going through that journey."

No silver bullets. No free lunches. Maybe that's no problem. Bankers will order the steak, anyway. wt

Cryptography's Quantum Threat

Executives from Barclays, IBM and Post-Quantum discuss why financial firms have to start preparing today for the future of hacking and quantum computing. By Hamad Ali

In early April this year, a curious incident took place. Internet traffic from over 200 of the world's largest content delivery networks (CDNs) was redirected through Rostelecom, Russia's state-owned telecoms provider.

The occurrence only lasted for about an hour, but it affected many large online providers such as Google, Facebook, Amazon, CloudFlare, and GoDaddy.

This was not the first such incident.

In April 2017, traffic from over a dozen financial services firms, including MasterCard, Visa and HSBC, was also redirected through Rostelecom. Occasionally, countries including China, Belarus and Iceland, have also been involved in similar incidents of internet traffic re-routing for short periods of time.

These kinds of occurrences are known as Border Gateway Protocol (BGP) hijackings. BGP is the routing protocol that maps out the connections for internet traffic. BGP hijacking is often the result of an innocent misconfiguration. But security experts worry that some of these re-routing occurrences have a more sinister motive lurking behind them.

"When we are trying to transmit data, if the protection is not high enough, people can still collect your data today, waiting to crack it tomorrow," says Andersen Cheng, CEO at Post-Quantum, a firm focused on post-quantum security. "People used to think it is stupid, this will not happen. But I can tell you even in the last few years, there have been a number of very strange activities. From time to time we can see the entire internet traffic being diverted to some servers in Russia or in Eastern Europe."

1994

Shor's algorithm was invented in 1994 by Peter Shor at Bell Labs. His computational method for integer factorization showed, theoretically, how to use a quantum computer to break schemes for public key cryptography

Cheng says certain countries are probably carrying out experiments or trials through such traffic rerouting, and are waiting for a time when the computing power arrives to be able to access the stored data. One way in which a malicious actor could decrypt this data in the future is with the help of quantum computers.

Recent advancements in quantum computing, including Google's claim of achieving quantum supremacy last year, have drawn attention to

> "At that point, they could potentially be able to run Shor's algorithm to factorize large numbers, which would be the tipping point for bad actors being able to crack existing classical cryptography."
> Lee Braine, Barclays

Lee Braine
Barclays

the threat these machines could pose to current encryption schemes.

Lee Braine, director of research and engineering at Barclays, says there is a steady, incremental increase in power in quantum computing, so people are able to extrapolate and look forward to a point in the future when quantum computers would be scalable, and able to run complex algorithms on much greater numbers of reliable qubits.

"At that point, they could potentially be able to run Shor's algorithm to factorize large numbers, which would be the tipping point for bad actors being able to crack existing classical cryptography," he says.

Shor's algorithm was invented in 1994 by Peter Shor at Bell Labs. His computational method for integer factorization showed, theoretically, how to use a quantum computer to break schemes for public key cryptography, which are widely used in many applications today.

Which Data Needs Protection?

There are certain types of data, such as government communications or private medical records, that organizations must take extra care to prevent falling into the wrong hands.

However, Cheng, who was formerly European head of credit risk management at JP Morgan, says for a financial services firm, not all types of data are top secret—for example, information related to the buying and selling of securities, which often can end up in the public domain.

Rather, he says, for a bank, it is customer or reference data that needs to be protected. Any leakage of this information could be very costly. Cheng says people who hold this data will treat even investors' existence as a secret, including their relative holdings, transactions, how they conduct their business, and signature blocks.

"A hacker can go in, they know how it is done, and they can copy the signature and they can forge it," he says.

Other types of data that need long-term protection include email communications, which regulators require to be kept for a certain number of years, and information related to mergers and acquisitions. As such, firms need to carefully examine the data they hold, and suss out any that needs long-term protection.

Getting outside help could be one way to do this. This year, IBM introduced a quantum-safe cryptography service on its public cloud, which includes a risk assessment service to help firms understand what types of data need to be protected from quantum computers in the future.

"Our consultants go into a bank or to a government," says an IBM spokesperson. "Some organizations have dozens and maybe even hundreds of different types of cryptography. You need to understand and assess what cryptography is at risk."

After making its assessment, IBM informs the client which systems are holding data that needs to be protected for the longer term, say for 10 or 20 years.

"Then you look at those systems and then you look to migrate them

> "There are some deep engineering challenges that need to be solved in terms of scalability during that time, hence some researchers emphasizing that there will need to be some significant breakthroughs in the coming years in order to reach the scale that would be necessary to run Shor's algorithm on large numbers."
> **Vikram Bakshi, Barclays**

potentially to something that is quantum-safe," the spokesperson says.

The Encryption Landscape

Not all cryptography is broken by quantum computers, however, says Vadim Lyubashevsky, a cryptographer at IBM. There are two main types of cryptography currently used by classical computers: symmetric and asymmetric.

In symmetric encryption, the same key is used to encrypt and decrypt data, while in asymmetric encryption, different keys are used: a public key to encrypt the data without compromising on the security process, and a private key to decrypt it. Asymmetric encryption is also more commonly referred to as public key encryption.

Symmetric key cryptography such as the Advanced Encryption Standard (AES), which is used by the US government, is not broken by quantum computers.

"The only problem was the public key encryption, so that is what we are dealing with," Lyubashevsky says.

Building an algorithm is only part of the journey to becoming quantum-safe. Lyubashevsky says it will be interesting to see at which point people completely trust a new scheme from IBM. "Very similar things happened with RSA and elliptic curves," he says.

Rivest–Shamir–Adleman (RSA) is the public key encryption scheme that is currently widely used. It was introduced in the late 1970s, and has since become a global standard. In the 1980s, a new approach known as elliptic curve cryptography was introduced. Lyubashevsky says there was hesitation in adopting the new system due to the wider use of RSA by that stage.

Vadim Lyubashevsky
IBM

"Now, 20 years have gone by since then and people completely trust elliptic curves, so RSA is being almost phased out," Lyubashevsky says. "Maybe similar things will happen [with quantum-safe cryptography]; there will be some standards three years from now, and then we'll see what actually gets used."

The Road to Standardization

Moving over to a new encryption scheme will be a slow process. The National Institute of Standards and Technology (NIST) in the US is currently running a project to standardize post-quantum cryptography. IBM is among the candidates to have submitted their algorithm to NIST for consideration.

"The most important thing about cryptography is you want a lot of eyes to look at the implementation, look at the hard problems just to sort of be somewhat sure that it really is secure," Lyubashevsky says.

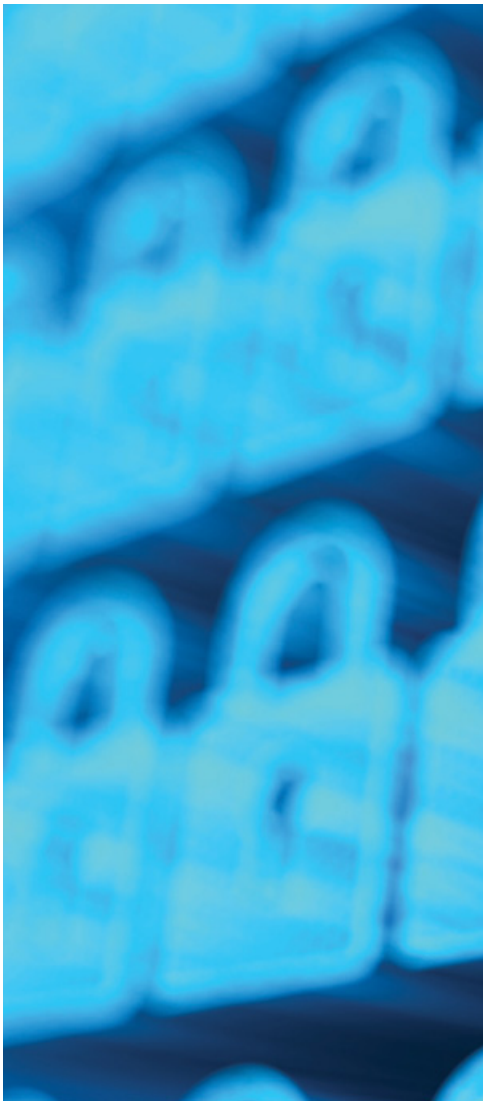
There are a number of categories within the project for candidates to submit their algorithms. These include lattice, code-based, hash-based, multivariate and supersingular elliptic curve isogeny.

IBM has developed a lattice-based method for cryptography, which hides data inside complex math problems called lattices. Lyubashevsky says the encryption they have developed is fast and flexible.

Many banks and asset managers are waiting for standards to emerge before they can more fully explore these types of encryption.

"Once this becomes closer to the standard, we will see probably a lot more interest," says a source from IBM. "A lot of clients are waiting for the NIST decision."

The spokesperson at IBM says the banking industry can "begin to look at this technology and look at potentially doing some pilot projects with it. They don't necessarily need to wait for it to become a standard, they can already begin to do some more pilots to understand how this is going to change their encryption schemes. Also, it helps them understand how agile they are in terms of their cryptography as well."



Still, there's a concern about fragmentation when it comes to this type of security. Braine from Barclays says although firms could explore candidate solutions, and maybe even promote them to live environments, there is a risk that these would not become an industry standard, which will come in later and potentially replace those candidate solutions.

"What you do not want is different parties using different approaches and algorithms because we really need

to encrypt and decrypt using the same techniques across the industry. So encryption standards are incredibly important. Many parties are highlighting the NIST initiative that is working through candidate algorithms and producing recommendations and draft standards—this will provide useful input for financial institutions considering which specific algorithms should actually be deployed," Braine says.

Post-Quantum also submitted its algorithm for consideration to NIST. Cheng says the submission is one of seven currently left in the code-based category.

"We are in the code-based category, which is the most important and we know for sure that they are going to pick one candidate from here for standardization," Cheng says.

Quantum Ready, Quantum Safe

For the past three years, Cheng has been promoting the concept of hybridization, also known as crypto-agility.

Cheng says if he went to the chief information officer of a bank and offered his product, he would likely get a "no." However, if he instead offered RSA encryption wrapped around a quantum-safe adapter, it would be easier for the bank to embrace the new technology.

Cheng says there is a difference between being quantum-ready and quantum-safe. He says being quantum-ready is somewhere between the current protocol, which is not future-proof, and being quantum-safe.

"We are offering quantum-ready solutions, because some of our customers just want the elliptic curve for the time being, but then be switchable to become quantum-safe later," Cheng says.

He says when the time comes to switch to being quantum-safe, his firm knows exactly what to swap out and what to swap in.

"For us to go from being quantum-ready to quantum-safe, it will just be a matter of a few hours," Cheng says. "Then, two [to] three days to do testing, and then the entire thing will become quantum-safe. I do believe this has to be way forward for anyone who has data to worry about,

> "When we are trying to transmit data, if the protection is not high enough, people can still collect your data today, waiting to crack it tomorrow. People used to think it is stupid, this will not happen. But I can tell you even in the last few years, there have been a number of very strange activities."
> **Andersen Cheng, Post-Quantum**

especially in the asset management business where a lot of the systems are very outdated now."

Lyubashevsky from IBM also talks about taking a hybrid approach. "As long as you're not becoming weaker, you can, for example, always combine whatever is used now, [such as] RSA; you could use it together with anything you want and it would still be standardized because RSA is secure," he says. "You can sort of put it together with whatever you want, and hopefully it achieves even more security, but it's definitely not less secure than something standard."

Andersen Cheng
Post-Quantum

Timeline to Quantum Threat

The timeline of the threat from quantum computers is open to debate. Braine says that while some feel it could be as soon as five years from now, the consensus tends to be around 10 to 15 years. Some even say that it may take as long as 30 years.

"My observation has been that the estimates tend to depend on the background of the people, including how closely they're engaged in not only the theory of constructing the algorithms but also the practicality of actually building the hardware," Braine says.

Vikram Bakshi, developer in the research and engineering team at Barclays, says that to be able to construct a quantum computer capable of running Shor's algorithm on a larger scale, many logical qubits are needed. For example, a few thousand logical qubits with long coherence times and extremely low error rates would be needed. In order to construct each logical qubit, probably around 1,000 physical qubits are needed to implement the necessary error correction. A quantum computer would likely need a total of a few million physical qubits.

"At the moment, if you look at general purpose quantum computing, some of the latest systems have about 50 to 70 qubits, and perhaps upcoming systems will have double that number in another nine months, and so on. At that rate, it's going to take a long time to reach over a million physical qubits," Bakshi says.

"There are some deep engineering challenges that need to be solved in terms of scalability during that time, hence some researchers emphasizing that there will need to be some significant breakthroughs in the coming years in order to reach the scale that would be necessary to run Shor's algorithm on large numbers," Bakshi says.

For the time being, Barclays is busy getting quantum-ready. This has involved the bank connecting with multiple vendors to get their opinions, installing and running some software packages, and performing architectural reviews of third-party initiatives. The bank also produced internal session papers to increase awareness of the potential future threat.

One of the firms that has gone through the Barclays Accelerator program is Post-Quantum, with the bank's CTO performing a deep dive review of the vendor's technology.

It's not just that the algorithms need to be good. Bakshi says the implementations of those algorithms must be bulletproof too.

"We have not yet explored one of the topics that NIST has been discussing, which is combining algorithms from different categories in order to construct more resilient solutions such that, if one of those algorithms or categories gets cracked in the future, you could potentially rely on the other algorithm," Bakshi says. "That is a promising avenue that we intend to research in future."

Bursting the Blockchain Bubble

Another area of concern is investment from financial institutions in blockchain technology, with the fear it has exposed them to the risk of being hacked with quantum computers in the future.

Barclays has explored, partly via the R3 consortium, the benefits of a blockchain solution that couldn't someday be cracked by a quantum computer. Braine says that could mean the security of assets stored on a distributed ledger could be potentially guaranteed for a much longer period. He says R3 has already published a post-quantum signature algorithm tailored to blockchains.

"One of the things we have come to appreciate in the blockchain space is that, the more you decouple the messaging and storage functionality from the cryptography, the easier it should become to 'plug and play' different cryptographic algorithms, making it simpler to be able to upgrade in the future," Braine says. "This is important because if we hypothesize that one of the quantum resistant algorithms recommended as a standard could subsequently be cracked in future, you could more easily switch to an alternative algorithm at that time."

Braine says blockchain technology is no more at risk than existing classical solutions of being cracked by bad actors using quantum computers. "The key point is that, at some point in future, it will be necessary for both existing centralized solutions and distributed blockchain solutions to upgrade," he says.

Although standards are still some years away, financial institutions need to start examining their data now and make sure it is not being compromised by occurrences such as BGP hijacking, to be stored by bad actors in order to crack later. They should adopt good data practices, and perhaps also start exploring the algorithms that are being developed and testing hybrid-encryption products. After all, just because a hacker can't do something malicious with stolen information today, doesn't mean that will always be the case. wt

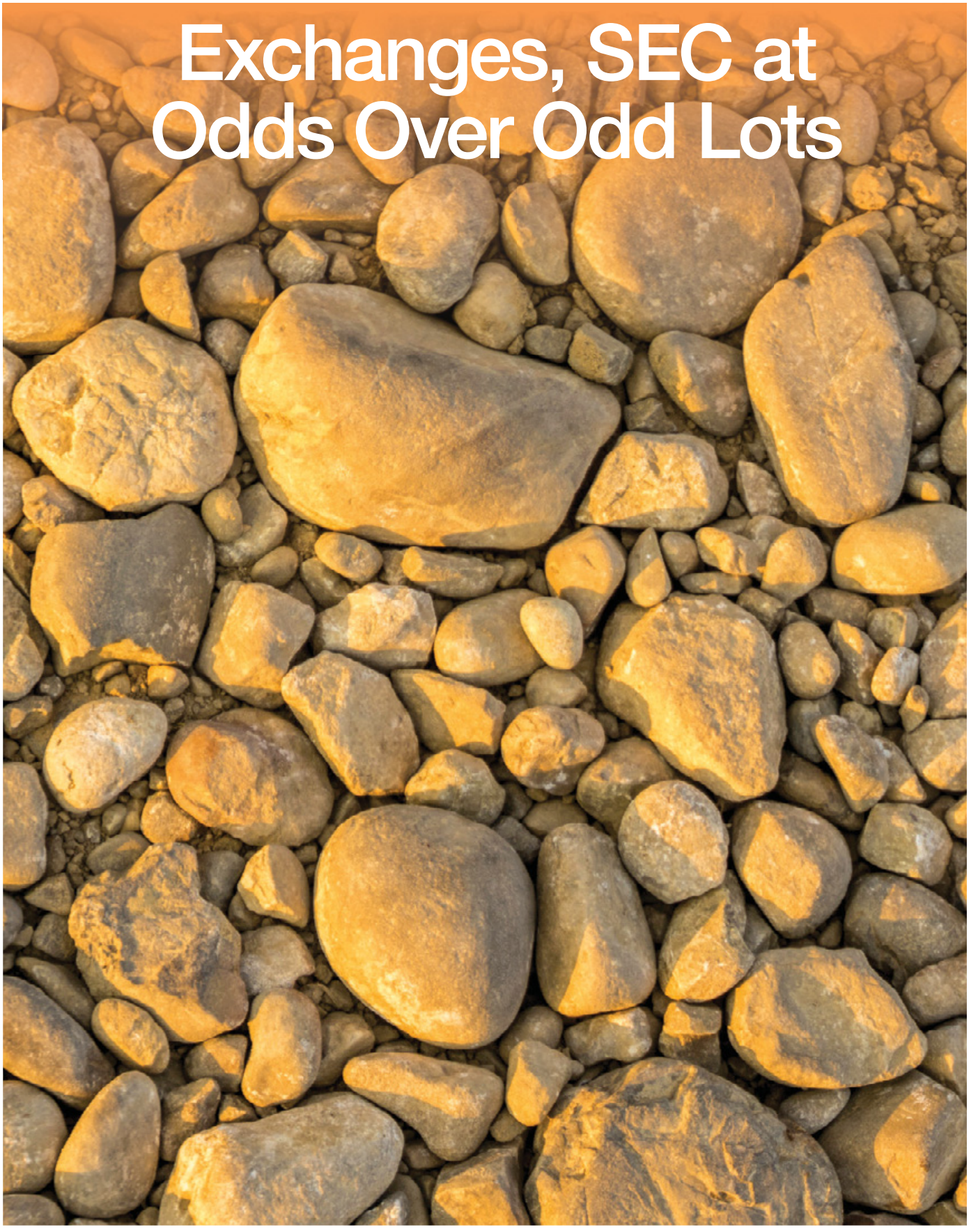
waterstechnology | Follow Topics

Build your own email alerts

Follow our coverage on individual organisations like ESMA or ISDA. Or pick specific topics such as Mifid II, blockchain, or artificial intelligence. Plus many more. Select your topics and you'll receive everything you are interested in, all in one email.

Visit waterstechnology.com/follow

Exchanges, SEC at Odds Over Odd Lots



Industry insiders warn that the SEC's attempts to modernize equities data by redefining trading lots will fall short of the mark if odd lot orders remain unprotected. By Jo Wright

Almost by definition, financial regulators have a thankless job. Industry participants rail against overly burdensome requirements; consumers say their interests aren't being considered enough. To make matters more challenging, regulators need to be able to see into the future even as technology increasingly changes the market in unforeseen ways—but everyone has an opinion on exactly how the rules will have consequences in the future.

Regulation National Market System (Reg NMS) was established in 2005 and provides the fundamental principles of fairness in price execution and access to market data in US securities trading. The Securities and Exchange Commission (SEC) says that technological change and evolving market practices are making aspects of Reg NMS outdated.

Take, for example, odd lots. US equities trading is based on round lots—the standard unit of 100 shares of a stock that a dealer or broker uses to trade. In 2005, odd lots—orders of less than 100 shares of a stock—made up a small percentage of the market. And a decade later, odd lots still accounted for only 20% of market activity.

But then the market started to shift significantly.

According to research done by SEC staff using data from its analytics platform Midas, the number of exchange odd-lot trades as a proportion of the number of all exchange trades for all corporate stocks ranged from about 29% to 42% of trades in 2018; in 2019, the rate exceeded 50% several times. The SEC has also found that on average, the measure of bid–ask spread widens significantly when calculated using only round lots relative to the odd-lot quotations displayed on proprietary feeds.

The problem is that because the NMS is so centered on round lots, all this odd lots liquidity does not appear on the feeds of real-time, consolidated data distributed to the market.

Earlier this year, the SEC rolled out a controversial rule proposal to expand and reform the content and distribution of public US equities market data. The rule has divided market participants, but US exchanges and trading firms seem mostly united on at least one aspect of the update: that the currently proposed solutions around odd lots would create more complexity for market participants and threaten the ability of brokers to provide best execution.

The controversy is not around the inclusion of odd lots quotations on the public feed, which market participants more or less agree should be the case, and which is what the SEC is proposing. Where the opinions start to fly is the manner in which the SEC wants to achieve that goal.

The SEC's plan would attach the definition of a round lot to its share price, as opposed to the current definition of the standard 100 shares of a stock. There are several sticking points in this shift, but the most important one, say trading firms, is around the Order Protection Rule (OPR). Odd lots are not protected from trade-throughs under Reg NMS, and still would not be under the new proposal, which, exchanges say, undermines the transparency and price discovery benefits of including odd lots on the public data feeds in the first place, for both retail and institutional investors.

"The odd lots problem is a problem that is worth tackling. I just don't think the SEC has tackled it the right way," says Phil Mackintosh, chief economist at Nasdaq.

> "The odd lots problem is a problem that is worth tackling. I just don't think the SEC has tackled it the right way." Phil Mackintosh, Nasdaq

There are a number of reasons for the rise in odd-lot volume, especially in high-priced securities. One is algorithmic trading, which splits up large orders into smaller ones to avoid creating large price changes. Another is that over the years, corporations have stopped splitting stocks, and some prestige stocks have attained high prices. Retail investors don't trade in round lots of those stocks. For example, if Amazon is trading at around $3,000 per share, a round lot of that stock would be $300,000. To put that into perspective, $200,000 qualifies as a block-sized trade, Mackintosh says. The average retail trade is $10,000.

"Most of the rest of the developed world has done away with the concept of round lots because computers don't really care, and they moved back to integers. So if you trade one share, or you trade 97 shares, or 122 shares, it doesn't matter. And now in the US, retail brokers are doing fractional shares. So realistically, in modernizing the market, we don't need round lots at all," Mackintosh says.

As the SEC looks to enact market reforms, the rise of odd lots has major implications for best execution.

For one, odd lots are not reported to—and thus do not appear on—the real-time consolidated feeds of market data distributed to the public by the Securities Information Processors (SIPs), unless they are of sufficient size to be aggregated into round lots.

There are two SIPs—one for Nasdaq-listed securities, and one for NYSE-listed securities. They calculate and disseminate basic, top-of-book

market data, notably the national best bid and offer (NBBO). The NBBO is the best available bid and ask prices at which brokers must trade when buying or selling securities for their clients. It was created to level the playing field for investors, ensuring best execution for all. If more sophisticated users want depth-of-book information, including odd lot quotes, at lower latency, they need to buy enriched datafeeds sold by exchanges or have the rights to the underlying data and receive it from aggregators like Bloomberg.

However, if odd lots now make up a significant portion of trading volume, and they don't appear on the SIP feeds, then not only is a growing segment of the market lacking transparency, but brokers who only see the SIP might think they are getting best execution for their clients, while there may be small buyers and sellers at slightly better prices in the market.

Jonathan Kellner
MEMX

"Because the content of current core data does not reflect these important market developments, many market participants say they cannot rely solely on SIP data to trade competitively and provide best execution to customers in today's markets," the SEC stated in its February consultation paper.

The SEC published the market infrastructure proposal on February 14 this year, following a related proposal published in January, which sought comment on governance provisions for the structure of exchanges' NMS plans. The public had until May 18 to comment on the Valentine's Day proposal, and the SEC is now considering the consultation responses from exchanges, buy-side firms, dealers, data vendors, and others.

The round lots redefinition is just one aspect of the changes represented in the proposal, which some buy-siders and exchanges are calling Reg NMS II, in reference to what they say is a fundamental overhaul of the NMS that touches on every rule in the regulation.

Apart from new data definitions, the proposal seeks to establish a decentralized consolidation model: the two SIPs disseminating the NBBO would be replaced with around 12 vendors, called competing consolidators, supplemented by self-aggregators (broker-dealers that would generate market data for their own use but would not distribute it externally). These competing consolidators would develop their own consolidated market data feeds, but could also sell data products. The NBBO would become multiple BBOs localized in these entities.

The decentralized competing consolidator model would reduce geographic latency for subscribers by facilitating the delivery of market data more directly, as it would not have to be sent to a separate location to be consolidated by the exclusive SIPs, the SEC says.

At the same time, more data would go onto the SIP feed. "Core data" would be defined so as to include what the SIPs already disseminate, plus the odd lots data, certain depth-of-book data, auction data, and some regulatory data. To include the quotation data for smaller-sized orders round lots would be redefined: Instead of being 100 shares, they would be based on a dollar value, with five tiers of round lots based on a stock's average closing price on an exchange for the prior calendar month, ranging from $50 or less per share to $1,000 per share.

By setting these levels, the SEC hopes to capture more odd lots as round lots, which would therefore appear on the SIP feeds. The Commission notes that "of the odd-lot transactions executing at a price better than the NBBO during all of the trading days in September 2019, approximately 38% of such transactions and 61% of the odd-lot volume were in sizes that would be round lots under [the proposed rule]."

However, order display would be required without protection: That is, odd lots would still not be protected under OPR, also known as the trade-through rule. The OPR is a lynchpin of Reg NMS's fairness principles, and makes trade-throughs—trades that are filled even though a better price was available on another exchange—illegal. But the rule was written in a time when round lots represented most of the market, and odd lots are not protected from trade-throughs.

The proposal keeps trade-through protection pinned to 100 shares, creating an NBBO based on the new tiered round lots, and a protected best bid and offer (PBBO)—applicable only to quotes of 100 shares or more.

> "It makes sense to start displaying odd lots because there is a lot of volume, meaningful dollar amounts that are traded that people are willing to buy or sell at prices that are better than the best bid and offer. So why aren't we displaying that?"
> **Jonathan Kellner, MEMX**

"Given the amount of volume in odd lots, it makes sense to make it a part of the data that is published to the SIP, and to make it broadly available," says Jonathan Kellner, CEO of dealer-backed startup exchange Members Exchange (MEMX)."It makes sense to start displaying those because there is a lot of volume, meaningful dollar amounts that are traded that people are willing to buy or sell at prices that are better than the best bid and offer. So why aren't we displaying that?"

Reg NMS II?

This is one reason why the SEC is looking to modernize the data disseminated to the market via these SIPs, saying that the SIP feeds are no longer fulfilling their goal of leveling the playing field for all investors.

Protection Racket?

A diverse array of exchanges—including NYSE, Nasdaq and Cboe, as well as newer, disruptive entrants to the market IEX and MEMX, which were founded in part as a response to industry frustrations with the NMS status quo—responded to the SEC's consultation. Though their responses vary according to their commercial interests and points

of view, all broadly agree that they are in favor of improving the data on the SIP and reforming round lots. But they differ from the SEC's proposals on how best to achieve this.

The exchanges agree, however, that order protection must be extended to odd lots. "In proposing to exclude from protection smaller-sized quotations in higher-priced stocks, the Commission

The SEC notes that "of the odd-lot transactions executing at a price better than the NBBO during all of the trading days in September 2019, approximately 38% of such transactions and 61% of the odd-lot volume were in sizes that would be round lots under the proposed rule."

NYSE, for example, agrees with the Commission's approach up to a point, recommending that it expand SIP content with depth-of-book data and an NBBO-only version for retail customers, and mandate round lot reform.

Elizabeth King, chief regulatory officer at NYSE, said in her consultation response, however, that the exchange believes the best way to address the lack of odd lot data on the SIP would be to include the best-priced odd lot quotation from each exchange in the definition of core data.

"Absent that, NYSE agrees that a market-wide graduated 'round-lot' definition based on each security's share price could be a low-effort technical solution to ensure investors can access liquidity currently inside the SIP's NBBO—provided the relationship between round lot and protected quote status is preserved," King said.

Nasdaq's global chief legal and regulatory officer, John Zecca, on the other hand, gives a more aggressive critique, kicking off the exchange's 63-page consultation response by saying the proposal "is too risky to adopt."

"The Commission fails to recognize, and thus insufficiently analyzes, how the proposed rule would essentially rewire the equity markets," Zecca said, adding that the proposal violates not only the Administrative Procedures Act (by failing to engage in a sufficiently robust qualitative or quantitative analysis), but the US Constitution itself, in that it "takes from exchanges their market data without adequate compensation."

suggests (but does not outright state) that it shares the views of some market participants that Rule 611 (the OPR) has negatively impacted equity market structure, and that it should be repealed," Zecca said in his response, adding that extending order protection to the proposed new round lots is necessary to ensure best execution.

MEMX's Kellner agrees that this is a concern. "The OPR says the displayed best bid or offer needs to be protected. For both institutional and retail—but especially retail—if you see a price on the screen, you expect to be able to get that price," he tells *WatersTechnology*. "And we have all, ever since the OPR was introduced, been really focused on our ability to get the best bid or offer."

The proposed method would create confusion in the market over what is available and what is protected, he says, placing the onus on brokers and the exchanges that route the orders to make decisions about what is best for the client. "Let's say you start displaying the odd lots, but they're not protected," he says. "You might have something that is offered at $900 per share for a round lot. The odd lot could be $850, but because that $850 quote isn't protected, a broker might say, 'In order to ensure that I get 100 shares filled, I am going to pay $900.'"

Kellner says MEMX isn't against re-evaluating the OPR, but says it should be done completely separately from this infrastructure proposal. "The Commission needs to do effective analysis, modeling, maybe even a pilot to determine if eliminating the OPR makes sense. But to just put it in this proposal, create all this confusion, and then potentially impact the current market structure is not the right approach," he says.

Jay Clayton
SEC

Buy-side firms that responded to the proposal seem to agree with the exchanges on these issues.

BlackRock's Hubert de Jesus, global head of market structure and electronic trading, and Samantha deZur, director of global public policy, wrote that the asset management giant "strongly opposes" the proposed changes to the OPR.

They note that the proposal says that best execution obligations apply to odd-lot orders, which the SEC believes would be enough incentive for market participants to engage with meaningfully sized orders as they already have visibility into odd-lot quotations. However, they add, academic research has shown that trade-throughs of non-protected odd lot orders are frequent, resulting in hidden costs for equity traders.

"Applying OPR to the new round lot definition at the outset is essential for promoting fairness in trading outcomes and achieving best execution for investors. Further, the introduction of an NBBO that deviates from the PBBO would increase complexity and sow confusion," they wrote. Apart from the confusion for market participants having to apply disparate odd-lot aggregation methodologies and conflicting reference prices between the NBBO and the PBBO, they would be required to update their systems and routers.

"The substantial implementation effort associated with this revision to the OPR are an added and unnecessary cost, as no adjustments would be required if the newly proposed round lots were protected," they add.

Charles Schwab's letter, likewise, said the investment firm believes that the OPR "should be extended to any new round lot sizes established by the proposal. With Reg NMS, the SEC found that price protection encourages limit orders as it increases the likelihood an investor will receive execution—which will foster confidence in the market."

> "The Commission fails to recognize, and thus insufficiently analyzes, how the proposed rule would essentially rewire the equity markets."
> **John Zecca, Nasdaq**

In the first quarter of 2020, some 23% of Schwab customers' limit orders for stocks priced higher than $100 are for fewer than 100 shares, and so would remain unprotected, the firm's letter adds.

T. Rowe Price, however, doesn't see the SEC's approach to the NBBO and PBBO as eliminating restrictions on trade-throughs. "Rather, we agree with the SEC that the OPR would be applied under the proposal similarly to how it is handled today," the asset manager wrote in its letter, which is signed by Mehmat Kinak, global head of systematic trading market structure, and Jonathan Siegel, senior legal counsel of legislative and regulatory affairs.

Kinak and Siegel say they are not convinced that the proposal would alter asset managers' best execution obligations as a result of potentially different reference prices between the NBBO and the PBBO, or that it was a burden for asset managers to ensure that broker-dealers achieved best execution. The buy-side should as a matter of course be evaluating broker-dealers' best execution capabilities with nuanced assessments of multiple factors, they said.

"Having the knowledge and understanding of how one's broker-dealer utilizes an NBBO versus PBBO in their routing or mid/peg-pricing should already be part of asset managers' best execution due diligence. Simply looking at whether a broker-dealer satisfied the OPR should not, in our view, be a mechanical barometer for determining best execution," they wrote.

Broker-dealers themselves have visibility into odd lots anyway—they just have to subscribe to the richer proprietary feeds, the letter states.

Extending the OPR to odd lot quotations would have significant trading implications, forcing market participants to display quotes in very small sizes. "This would not be a good outcome, as asset managers with large transactions would increasingly have to further 'slice' their trading activity into smaller increments to avoid signaling their full trading interest to the market," they said.

A source at a smaller asset management firm tells *Waters Technology* they were surprised to see what the proposal did with the PBBO. "That makes a lot of complexity around the NBBO and PBBO, where the PBBO is only quotes of over 100 shares, but the NBBO is based on new round lot quotes. So if there is one share of Amazon, it's not protected, but if there are 100 shares of Amazon, they are protected," the source says.

However, they add that this won't have much of an effect "on the way we trade, or our best execution, but it would be confusing for retail."

Changing of the Guard

With the consultation now closed, the SEC is considering the responses and meeting with various stakeholders.

While some had hoped for an extension to the consultation process, sources on the buy side and at exchanges say they don't expect to be given more time to consider the 595-page infrastructure proposal, Covid-19 disruptions notwithstanding.

The forces behind the Reg NMS update are two vocal individuals: SEC chairman Jay Clayton and Brett Redfearn, the director of the SEC's Division of Trading and Markets. Clayton's five-year term ends next year, and several sources said they believe that Redfearn, who has been at the Commission since October 2017, is unlikely to stay in his role much longer than Clayton in his.

With the clock ticking on Clayton's tenure, he is going to want to put his stamp on the Commission, and in Redfearn, he has an ally. While the changing definition of odd lots might be left for another administration to rule on, the SEC—as it's constituted today—is clearly interested in reforming the content and distribution of public US equities market data.

Despite the contentious fight that is shaping up between regulators, exchanges and market participants on the modernization of the markets—on odd lots and on broader issues—the regulators will find support in their efforts to level the playing field between the SIP and the direct feeds. The industry just wants to be heard on its concerns.

As MEMX's Kellner says: "We appreciate what the regulators are doing in terms of trying to make changes to the SIP and to market data in general. ... But there are some specifics that we think the Commission should understand from a market data perspective what the goal is." wt

MOONSHOTS SHELVED:

Banks Spend on Home-Working Tech

Senior technologists from UBS, Deutsche Bank, Nomura, SocGen and others discuss where their tech spend is being directed. By Luke Clancy

In late 2019, UBS asked 20 of its traders to experiment with a so-called soft turret system, developed by fintech vendor Cloud9 Technologies. Lee Fulmer, the bank's global head of innovation, expected the idea of replacing traders' heavy-duty phone consoles with a software application to meet resistance.

"But at the end of the first month, all 20 of them asked to have another month to keep playing with it," says Fulmer. The only complaint: some sales traders missed having physical buttons to quickly turn the volume down.

As it transpired, this localized experiment presaged what would become a fundamental shift in banks' philosophy of trading technology. When the Covid-19 pandemic forced them into working remotely, their tactical response set the scene for a more strategic reassessment of home-working technology across the industry.

"[The deployment] felt like a 'mission impossible' task, particularly in Manhattan, which was being decimated by Covid," says Christopher Purves, co-head of execution and platform and co-head of digital at UBS. "People were unable to come into the office, and we needed to very rapidly figure out [how] to handle voice trading in a way that nobody had ever planned for."

"Within three weeks," adds Fulmer, "we were able to engineer a solution where we deployed Cloud9 onto Surface tablets, locked them down so they were UBS devices and we had control over them, and sent them home to people. We patched the devices into our private wires so people could talk to clients and their colleagues still in the office."

And, in many ways, the soft turret solution has been better than the real thing.

The metadata farmed from the high-quality call recordings is rich, and enables the firm to detect the flow and sentiment of conversations, says Fulmer, who is also chief data officer at the investment bank.

The ability for traders to quickly replay something a client said on a call gave the firm comfort around its risk appetite in challenging market conditions. And, from a supervision perspective, the bank was able to prove that staff who were voice-trading at home were operating under the same governance policies and procedures that apply in the office.

Purves points to its portability as further evidence of its suitability for the post-Covid workplace.

UBS is getting behind the solution: it led a $17.5 million funding round in Cloud9, which is also backed by JP Morgan and Barclays.

"People were unable to come into the office, and we needed to very rapidly figure out [how] to handle voice trading in a way that nobody had ever planned for."
Christopher Purves, UBS

Moving to Higher Ground

Other banks tell similar stories. The rapid deployment of new technologies has meant that traders working from home have, in some cases, been more productive than at the office. As commute time has been replaced by working time, productivity has been sustained—and, in some cases, even increased—and sickness rates have dropped. Dealers have handled a massive jump in trading volumes and second-quarter trading revenues are up double digits year-on-year.

The transition has met with such approval that many firms have talked of downsizing their physical real estate as they prepare to have more of their staff working remotely on a continuing basis.

Generally, working from home because of Covid-19 has been "seamless," says Deutsche Bank chief information officer Scott Marcar. Around 80% of the bank's desktops globally were already virtual, although concurrency—the volume of people simultaneously logged in—became the main issue to solve.

Christopher Purves
UBS

He acknowledges "a bit of tweaking" was required to provide those on the trading floor with virtual desktops. They achieved this via Citrix, a digital workplace platform, combined with a soft turret solution from IPC. Used remotely, the combined solution is piped into the channels that physically sit inside the bank's primary campuses or datacenters.

In Nomura's immediate response to Covid, the bank facilitated staff working from home with API-driven digital toolkits that foster cross-regional communication—for example, by employing visualizations to illustrate fixed income trade flows across products and regions, says Jezri Mohideen, global chief digital officer for Nomura's wholesale business.

"When markets are calmer, traders will ring and have a chat with other regions," he says. "But, with each individual trader working from home, it's a lot easier to deliver that electronically through visuals showing all the trade flows going through the platforms. Half the battle with any of these toolkits is getting widespread adoption—but now they see the benefit of them."

A fourth bank, Societe Generale, also says its traders have been "fully equipped" to work from home. The bank was in the process of assessing a phalanx of innovation projects—both internal and external—for incubation as the crisis evolved.

This exercise followed one in 2017 that moved 30 internal start-up ideas into development, among them the digital asset platform Forge, according to Albert Loo, its deputy head of sales for global markets with responsibility for innovation and digital transformation.

He explains that the bank had already begun rationalizing the second cohort of fintech firms based on its learnings from the first—in particular, homing in on ideas that could be packaged for an external audience. But inevitably, Loo says, the crisis reconfirmed its view that funding should go to projects that maximize value for both its clients as well as its trading and sales desks.

Moonshots in the Long Grass?

In the short term, at least, the pandemic is likely to change the way in which banks allocate their technology budgets. This could mean banks turning their attention to nuts-and-bolts solutions necessary to ensure successful home working—as funding is cut for ambitious "moonshot" projects or those with longer-term payoffs. Some sources cite quantum computing and even artificial intelligence projects as examples of efforts that may be consigned to the long grass for now.

Rupert Bull, co-founder of The Disruption House, a benchmarking and data-analytics business for early-stage fintech firms, says innovation and change budgets, particularly at larger banks, are getting shaved as they focus on solving challenges to their immediate resilience. This means less investment in strategic, or even compliance, projects that are seen to be a long way from generating alpha or saving money.

"People are trying to solve problems closer to home. In that sort of world, it's all hands to the pump, just to keep the lights on," he says. "Many large organizations are caught up in the optics of restructuring and survival.

Jezri Mohideen
Nomura

They're just too busy dealing with the consequences of Covid."

A second fintech consultant, Oliver Bussmann, founder of Bussmann Advisory and the former chief information officer at UBS, agrees. He says big multi-year transformation projects are being put on hold at tier-one banks "because that has an immediate effect on capital expenditure and cashflow. There is much more focus on short-term impact and cost-efficiency. The investment priorities have changed significantly since the beginning of the year."

Fintech adviser Stuart McClymont, managing director of consulting services at JDX, thinks many big banks "are, in fact, realizing they may already have the necessary tools in their stable. Either they're invested in them, or they're in incubation. ... So, they may stop any new investment and just double down on optimizing existing digital transformations."

Maintaining Integrity

In practice, the new technology priorities are more fundamental than experimental.

"What you discover with Covid-19 is that you need to make sure you focus not on things that are ancillary for the trading or sales desk, but on those most important for us and our clients," says SocGen's Loo. "In a situation like Covid, you immediately see what is useful and what is not. And actually, we had already started on this path of rationalization."

The bank is not alone in prioritizing technological integrity.

At Nomura, in addition to accelerating the electronification of workflows, Covid-19 has increased the bank's focus on the operational robustness of its platforms, says Mohideen. "With the explosion of the 'data universe,' it is critical to have a unified data lake which allows artificial intelligence (AI)-driven, in-depth analysis to run seamlessly in real time. Having a unified data framework is essential to avoid operational inefficiencies, such as poor data quality, data duplication across departments, lack of data ownership in business, as well as the inability to run large-scale analysis across businesses and regions," he says.

"We're trying to fast-track that now," he adds, explaining that this includes putting more data into the cloud and using it for AI. "We've been continuously trying to experiment with the usage of data for AI in the trading and

sales businesses, as well as within the corporate function. Can we optimize capital, derive valuable insights, fight financial crime, or do trade surveillance better? How can we detect best-execution behaviors? Can we also extract alpha using market data?"

To do that effectively, he concludes, would mean building further on Nomura's efforts to establish a unified data framework across its organization.

Deutsche Bank is also of the view that a unified data framework will be a key element in making its systems robust enough to cope with future crises.

The technology strategy in Deutsche's investment banking operations has so far largely been a "simplification and electronification play," according to Marcar. But, as the bank exits its equities business to focus on fixed income and currencies, it is, like many banks, working on "getting the data right" to enable full straight-through processing.

"If anything," he says, "Covid just reaffirmed the need to remove people from the process and take errors out, which does lead into making sure your banking controls are based on good data."

Marcar says the firm solved its concurrency squeeze by upgrading the capacity of remote access servers in all locations and creating a dedicated trader environment to ensure no latency issues. It also increased the network bandwidth for all remote access circuits.

Home Remedies

But as banks face potentially difficult choices in tech spending, savings might equally be found in other areas, such as reviews of property portfolios. With large swathes of their workforces at home, and that experiment now seen as a huge success, banks may not fully return to their offices until Covid-19 fully subside—or perhaps never again in pre-pandemic mode. Given that remote working may persist for some time, banks are reconsidering the size of existing offices and the utility of disaster recovery buildings.

Marcar confirms that Deutsche Bank is asking itself some serious questions: "Do we need to be in so many buildings? Do we need to have so many physical disaster recovery sites? Or can disaster recovery be more remote?"

Another fintech expert, Mark Beeston, founder of venture capital firm Illuminate Financial, sums up the position: "In the UK, business continuity planning is no longer a large redundant building in Croydon, Reading, or Staines. It is planning for everybody catching the same cold and a fully distributed workforce."

> "What you discover with Covid-19 is that you need to make sure you focus not on things that are ancillary for the trading or sales desk, but on those most important for us and our clients."
> **Albert Loo, Societe Generale**

Albert Loo
Societe Generale

In Switzerland, too, Bussmann believes many offices in its financial centers will primarily be transformed into meeting spaces: "I think over the next 12 to 18 months minimum, the working-from-home infrastructure will continue to be utilized. I hear banks are considering reducing their office space by 20% to 30%. In the Swiss environment, certain banks are going back to not more than 40% to 50% staffing in offices. You just can't with the social distances required at one or two meters."

The focus of banking technology, for the time being, it would seem, is locked down on the home. wt

Max Bowie

Does Your Board Have Zero Trust?

Financial firms' boards are increasingly taking a more hands-on role in IT security—thus, Max says, driving adoption of important new security measures for their firms and the industry as a whole.

As financial firms continue to grapple with security concerns relating to their staff working from home during the Covid-19 pandemic, an approach called Zero-Trust Architecture (ZTA)—which was already gaining traction prior to the outbreak—is emerging as a potential solution to some enterprise-wide security challenges.

ZTA essentially locks down sensitive systems and data, removing any notion of inherent trust in a user or device trying to access them simply by virtue of being on a company's network. (*See page 12.*) But while the Covid-19 outbreak is a perfect proving ground for ZTA, its adoption is being driven by other factors—and increasingly, this is coming from the top, rather than being driven by business lines clamoring for management sponsorship.

Some believe the impetus for a sudden focus on tighter controls at banks is board members concerned about personal liability for any data breaches that occur on their watch. And while perhaps cynical, that's not necessarily a bad thing if it motivates senior management to look closely at the issue and drive greater security across the business.

"There is definitely a bigger push from the top these days, driven by regulations, but also by boards recognizing that security is a central business component," says Grigoriy Milis, CTO of RFA, a provider of IT services to hedge funds and asset managers. "Once they realized that, it became easier for IT to push it up the agenda. IT departments have been trying, but because it's seen as a cost … it was not met with board approval in the way that IT wanted."

In other cases, banks—as they start to describe themselves in the language of fintechs—have begun appointing seasoned technology executives to their boards, who bring knowledge of issues such as IT security that board members from a purely business background may be unaware of.

"I think a lot of people have probably heard the ZTA buzzword, but may not fully understand what it means," says an enterprise security executive at one large North American bank. "For example, management wants to know that their firm has security in place, but may not think they need to know the exact details."

> ZTA isn't a technology issue; it's a business issue that requires senior executives to understand technology to solve it.

Scott Rose, a computer scientist at the National Institute of Standards and Technology (NIST), says ZTA is currently gaining ground because of a confluence of supply and demand: namely that technology is now sufficient to handle its requirements, while Covid and high-profile data breaches have focused executives' minds on IT security more than in the past. "The complexity of enterprises has also changed. Whereas everything used to be internal, using firms' own datacenters, with managed software and cloud providers, a lot of that has changed where your perimeter is, and how you protect that," Rose says.

Because of the urgency to adopt ZTA, and the fact that many firms are still questioning where they should start, Forrester Research created the Forrester Certification Program to familiarize market participants with the main principles of ZTA, create standards, and unite the industry around a harmonized approach.

"We've had CEOs, board members, network engineers, and technology professionals take the certification. The aim is to be at the executive level, to get their thinking standardized," says Dr. Chase Cunningham, principal analyst for security and risk at Forrester. The on-demand program comprises about 20 modules made up of videos and written materials, and can be completed in two days, or over a couple of weeks.

At the end of the day, ZTA isn't a technology issue; it's a business issue that requires senior executives to understand technology to solve it. So, says Milis, IT departments need to articulate the solution in terms of its business impact.

"IT has been explaining this in terms of what it is trying to accomplish, such as ZTA and greater security," he says. "But IT staff need to explain it in terms of the business outcome: it's not about securing data; it's about minimizing liability, and avoiding fines. The board doesn't care what technology you use—they care about what you are trying to accomplish." wt

EU's AI Regulations Could Implicate CTOs

Jo wonders whether the bloc's approach to regulating AI will adapt existing liability laws—with implications for individuals.

In ancient Mesopotamia, King Hammurabi turned Babylon into a city-state to be reckoned with. His famous code is one of the earliest legal frameworks that modern humans know of. Its 282 laws include some regulation of the construction industry: if a house collapsed upon its owner and killed him, the builder could be put to death. If it killed the owner's son, the builder's son could be killed in restitution.

Fortunately, the EU's modern legal system doesn't put anyone to death for faulty products or services. But the idea of protecting consumers and holding producers liable for harm or loss persists, 4,000-odd years after Hammurabi.

The European Commission (EC) is currently considering how to apply these principles to the regulation of artificial intelligence (AI), technology that by its nature makes it difficult to apportion blame along a production chain.

It seems the commission intends to publish proposals for AI regulation, probably early next year, as it put out a consultation in a whitepaper in February that gave an early indication of what its approach to the legislative framework for emerging technologies will look like.

A major aspect involves adapting existing EU liability concepts to AI. In doing this, the whitepaper draws heavily on a 2019 expert group report which said that while the existing liability regime offers protections for AI users, adjustments are required to make it suitable for emerging technologies.

First, "strict liability" must lie with the person who is in control of the risk associated with the operation of the AI. This means the producer of an AI product is liable for harm resulting from its use, even if they were ignorant of the fault in the product.

These operators also have duties of care, including the need to monitor the system, the report says.

So, could a chief technology officer be held responsible for a defective artificial intelligence product, or for ruinous decisions made by an algorithm?

> While AI regulation is desirable, it could come at the cost of innovation

John Ahern, partner in the financial services group at law firm Covington in London, says this is a question that lawmakers and regulated entities have to ponder as the EC's approach to a legal framework solidifies. While AI regulation is desirable, he says, it could come at the cost of innovation, as increased liability would reduce interest in senior tech jobs at financial firms, or make chief technical officers overly cautious.

"What we need to be attentive to is where in the chain of liability are individuals affected. Think, for example, of the CTO: if there is a flaw in the design of a database product, or an algo, or any other form of AI product or service, does that mean, from a liability or a regulatory perspective, that the human being overseeing the process, product design or development now has an increased risk of liability in one form or another?" Ahern says.

The financial services industry already has a regulatory framework for product safety, he says, in the sense that regulators can intervene if a product is detrimental to the market or consumers. The UK's Financial Conduct Authority, for example, recently banned the mass-marketing of speculative securities to retail investors.

But there are no stipulations in law specific to financial services or regulation against the products themselves.

"What is not in the regulatory framework in a really explicit way right now is product design, where a product has an intrinsic flaw and somebody suffers loss having invested in it—that specific issue is not legislated for," Ahern says.

This would be a pivotal decision in the production of AI tools, he adds. Who would get the blame for a proprietary algorithm that causes a software glitch that lost investors' money? There might be liability attached to the firm, and legal consequences for the individuals that oversaw the creation of the algo.

This is food for thought not only in Europe. Whatever the commission's legislative framework for AI ends up looking like, its implications will extend beyond the bloc. While the EU has scrambled to catch up with the US and China in AI development, it has led the world in technology law.

The world took its cue from the General Data Protection Regulation, which has spawned imitators elsewhere, including in the US. It may do so again when it comes to regulating AI. wt

Wei-Shen Wong

HKEx's Data Play Slowly Comes Together

HKEx is currently working on building its enterprise data bus for better internal data management, but Wei-Shen finds that the exchange is still short on long-term answers.

This year marks the midpoint of the Hong Kong Exchange and Clearing's (HKEx's) three-year strategic plan to make it the "global market leader in the Asian time zone."

The strategy focuses on three areas. The first looks to make HKEx—through Stock Connect—the main hub for international entities to invest in China. The second aims to lower internal barriers to allow the exchange to become more interconnected with international outlets. The final piece is all about technology and modernizing HKEx's core trading platforms while exploring new partnerships.

Included in this tech transformation is the rollout of its next-generation post-trade platform, the adoption of an event-driven architecture, and, more generally, instituting a "more data-oriented management culture" throughout the exchange. In particular, by creating a scalable data marketplace platform, HKEx will be better positioned to mobilize and monetize its exhaust data, it contends.

The great killer of great plans is the unexpected. While Asia, and China specifically, has experience in dealing with pandemics, Covid-19 has proven to be a different beast to contain. During an Aug. 19 conference call to discuss its 2020 results, Charles Li, CEO of HKEx, indicated that the exchange's long-term play would be monetizing its budding data endeavors—but that strategy is still forming.

"It's also a strategy that is going to take time for us to bring to the right angle—the right shape—and we are still a good distance away from articulating clearly what our role is going to be in that new universe where data becomes a new asset class," he said.

The exchange declined to clarify its data plans and elaborate on data becoming a new asset class.

In an earlier announcement expressing its intent to buy a minority stake in TsingJiao, HKEx said partnering with the data technology vendor would help build its future data marketplace. The company specializes in multi-party computation (MPC) technologies—a subfield of cryptography—that allows for collaborative data analysis without revealing private data during the analysis process.

> By creating a scalable data marketplace platform, HKEx will be better positioned to mobilize and monetize its exhaust data, it contends.

How quickly this materializes will only be known when HKEx has a clear vision for building that data marketplace, and when the exchange is ready to talk about it openly.

Every organization has different data needs and Li said HKEx's role could be in the organization, development, and implementation of a technology platform that addresses the problem of data privacy and protection.

"We are constantly looking at that particular role that we are very good at, which is connecting the dots and bringing everybody together, building up our alliances so we can start to build out our ecosystem in data, and that's where we put the investment in," he said. "Probably our role is going to be in the organization and development and the regulatory enforcement and implementation of a particular technology platform that allows us to solve one common problem in the data space, which is privacy and data protection. So it's in that angle where we are most likely going to explore—again, this is something that is some distance away from our core business."

Last year, HKEx bought a 51% stake in Shenzhen-based Ronghui Tongjin—now known as BayConnect—which specializes in regulatory and exchange technologies. HKEx also signed a memorandum of understanding with Ping An Insurance Company of China to explore areas of collaboration in fintech, artificial intelligence (AI), and data analytics, to support the mutual connectivity of the mainland Chinese, Hong Kong, and international markets.

Li told *WatersTechnology* during the call that the exchange is still considering how these acquisitions and technologies will fit into its overall data strategy. As he noted previously, this is "a strategy that is going to take time" to complete.

HKEx is an important piece of the Asia-Pacific marketplace, especially as Beijing exerts more authority over Hong Kong. The exchange can serve as a keystone for international players and mainland China to come together, but it seems that right now, the building blocks to reach that point have a long way to go. wt

Human Capital

HKEX Announces Group Head of Technology Risk

Hong Kong Exchanges & Clearing (HKEx) has appointed Brian Lee as group head of technology risk.

In the role, Lee will work across the HKEx risk team, with a focus on improving cybersecurity and technology resilience, enhancing the group's policies and guidelines, and performing risk assessments.

Lee previously worked for 25 years at the Hong Kong Monetary Authority, where he held a number of senior roles, most recently as a division head of the banking policy department.

Brian Lee

TMX Group Taps John McKenzie for CEO

TMX Group has appointed John McKenzie as chief executive officer and made him a member of the group's board of directors. He was previously the group's interim CEO following the retirement of Lou Eccleston in January.

McKenzie has spent 20 years at TMX. He was named chief financial officer in 2016, and was responsible for the company's corporate strategy, corporate development, and investor relations functions, as well as finance. In 2018, McKenzie gained oversight of TMX's trust and capital formation businesses, which includes Toronto Stock Exchange and TSX Venture Exchange.

John McKenzie

Mark McKeon

TP ICAP Announces New Regional Sales Heads

TP ICAP has filled two senior roles in its data and analytics division.

Jeff Missimer joins the company from PolarLake, a Bloomberg subsidiary, as head of sales for the Americas, and will be based in New York. He was previously head of sales for the Americas at PolarLake.

Rhys Spencer has been promoted to head of sales for Asia. He has been with TP ICAP for more than 10 years. Based in Singapore, he will be responsible for building a team to grow revenue from client segments including asset managers and hedge funds.

The appointments support TP ICAP's wider strategy of diversifying and growing its revenue streams and client base.

Jos Dijsselhof

FIF Makes Howard Meyerson MD

The Financial Information Forum, an industry association focused on addressing and resolving open implementation issues that impact the securities industry, has announced the appointment of Howard Meyerson as managing director.

Meyerson was most recently global chief compliance officer at Liquidnet, where he managed legal, regulatory, and compliance for the rollout and operation of the Liquidnet trading system in 46 countries.

Prior to that, Meyerson worked at law firm Morgan Lewis, where he focused on a range of issues.

BNY Mellon Taps Mark McKeon as Global Head of Front-to-Back Solutions

BNY Mellon has hired Mark McKeon as global head of front-to-back solutions for its asset servicing business.

McKeon is based in Dublin and will help deliver BNY Mellon's open architecture strategy by expanding the company's front-to-back solutions platform globally.

McKeon was most recently global head of investment analytics at State Street. He has 20 years' experience of delivering proprietary risk management and analytics solutions for hedge funds, asset managers and institutional investors.

Jos Dijsselhof Takes Non-Exec Chairman Role at BME

The board of directors of Bolsas y Mercados Españoles (BME) has appointed SIX Group chief executive Jos Dijsselhof as non-executive chairman. BME has also named former lead independent director David Jiménez-Blanco as non-executive deputy chairman.

BME was recently acquired by SIX for €2.57 billion ($2.9 billion). The exchange's board made the appointments following an extraordinary general meeting in Madrid.

Dijsselhof has been CEO of SIX since January 2018, prior to which he was group chief operating officer at Euronext. He has also worked at ABN Amro Bank, Royal Bank of Scotland, ANZ Australia, and New Zealand Banking Group.

Jiménez-Blanco has been a director and member of the investment committee at Gawa Capital Management since 2010. He has previously worked at firms including BK Partners, Merrill Lynch and Goldman Sachs.

DELOITTE BOLSTERS FINANCIAL SERVICES INDUSTRY GROUP

Deloitte has named Monica O'Reilly as the new leader of its financial services industry practice, and has announced the appointment of Mark Shilling as banking and capital markets sector leader.

O'Reilly will lead the strategic direction of broad client-facing efforts in the industry. She succeeds Kenny Smith, who retired in May. Shilling will do the same in banking and capital markets, Deloitte's largest sector by revenue.

Shilling, a principal with Deloitte Consulting, previously served as the banking and capital markets sector leader for that business unit. He succeeds Scott Baret, who will be shifting into a strategic client-focused role supporting Deloitte's portfolio of banking and capital markets clients.

Monica O'Reilly

SS&C Algorithmics Hires Sales Exec for Asia-Pacific

SS&C Algorithmics has hired Antoine Burke as sales executive for South-east Asia, based in Singapore. Burke joined the vendor last month from Asset Control, where he spent five-and-a-half years, including as sales director and acting managing director for Asia-Pacific. Before that, he spent six-and-a-half years at SunGard, including as global account manager for the MarketMap terminal product throughout North Asia and South-east Asia, based in Hong Kong, and senior regional account manager for market data products in Geneva, Switzerland.

At SS&C, Burke reports to Elmar Nadschlaeger, senior director of sales and services for Asia-Pacific, who joined the vendor earlier this year from IBM.

Daniel Pellegriti Joins MTS Markets International as Senior Sales Manager

MTS Markets International, part of London Stock Exchange Group, has hired fintech industry veteran Daniel Pellegriti as senior sales manager.

Pellegriti will help drive growth for the company's electronic fixed income all-to-all trading and connectivity platforms in the US.

He has previously held fixed income sales and trading positions at Deutsche Bank, Morgan Stanley, Santander and, most recently, Algomi Corporation.

Qontigo Appoints Courtney Scharff as Global Head of Strategic Partnerships

Courtney Scharff has joined Qontigo as global head of strategic partnerships, focusing on indexes and analytics.

Previously, Scharff worked at Bloomberg, where she was global head of index data management solutions and, most recently, global equity index product manager.

Antoine Burke

Prior to that, she was head of North American client services at FTSE Russell. She has also served in several key client-facing roles at Russell Indexes.

Qontigo has also hired Ping Jiang as head of multi-asset solutions for the Americas in the customer experience group. In the new role, Jiang leads the pre-sales and product specialist team dedicated to Qontigo's risk offerings.

Jiang was previously head of investment consulting at New York Life Investments. Prior to that, he worked at AllianceBernstein, MSCI and Merrill Lynch.

Luminex Taps Ilisa Gruber as Sales and Relationship Manager

Luminex has hired Ilisa Gruber as its new sales and relationship manager.

Based in Chicago, Gruber will oversee Luminex's relationships with buy-side clients, and target growth in the Midwest and other regions.

Gruber is a Liquidnet veteran of 18 years, after becoming the firm's first sales trader. Prior to that, she worked at firms including Thomas Weisel Partners, Schroders & Company and CS First Boston.

Christopher Bok Takes Charge of Compliance at OTC Link

Christopher Bok has been named chief compliance officer at OTC Link.

Bok will be responsible for all aspects of OTC Link's regulatory compliance, and will focus on coordinating the firm's program regarding the SEC's Regulation Systems Compliance and Integrity (Regulation SCI).

The position was previously held by Mike Corrao, who retired in July.

In his previous role as director at Financial Information Forum, Bok was responsible for the management and oversight of operational and content-driven activities.

He reports to OTC Link president Michael Modeski.

Finastra Hires Ian Savage as Chief Financial Officer

London-based Finastra has appointed Ian Savage as chief financial officer.

Savage's recent roles include three years as chief financial officer at CashFlows Europe, a Pollen Street Capital-backed fintech payments business. He has also worked at Sigma Financial and Anacap Financial Partners.

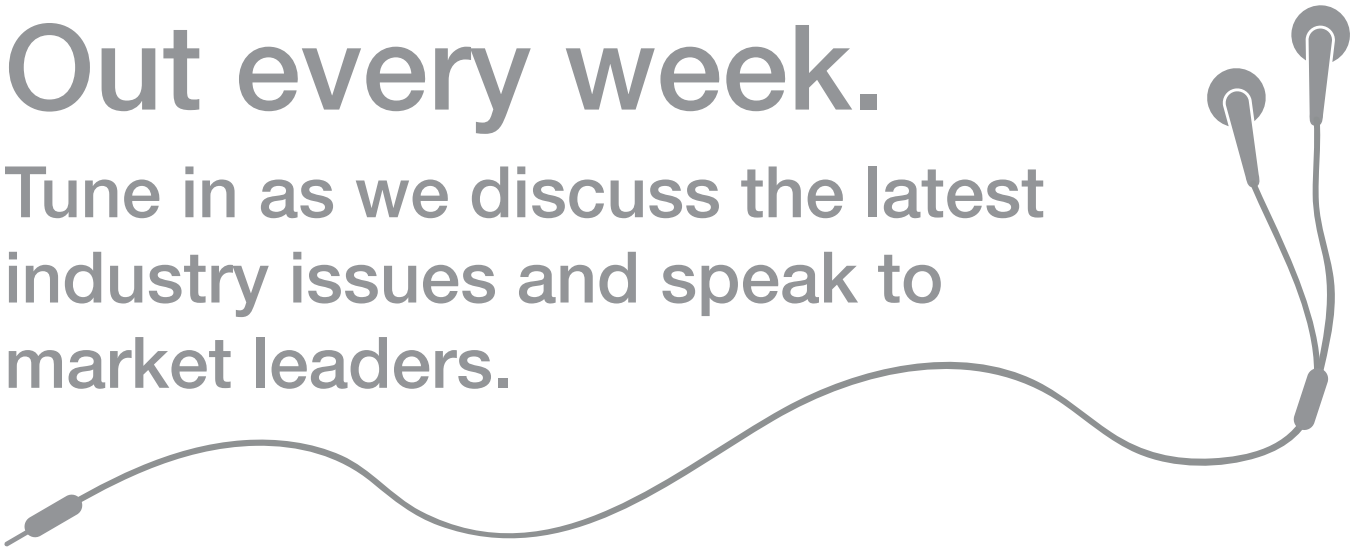
Finastra has also hired Paul Strudley as head of group finance. Strudley joins from Reflexis Systems, where he was finance director for Europe, the Middle East and Africa. He will be responsible for delivery of the company wide Netsuite project and IFRS adoption. wt

waters tech

Waters Wavelength Podcast

Out every week.

Tune in as we discuss the latest industry issues and speak to market leaders.



Subscribe at:
soundcloud.com/waterstechnology
or search the iTunes store for
"WatersTechnology"


SmartStream
The trusted security master built by the financial industry
Today, global institutions are critically dependent on high quality reference data to trade successfully, automate operations, and report accurately to regulators.
The SmartStream Reference Data Utility (RDU) has come up with a simple solution to satisfy these complex reference data needs, by providing a high quality security master built using industry best practices.
Developed in close association with industry leaders, the RDU offers a suite of managed services, including its newly launched Equities Service, all proven to deliver better quality data.
REFERENCE DATA
EQUITIES
LISTED DERIVATIVES
SYSTEMATIC INTERNALISER
REGISTRY
SFTR
MIFID II
info@smartstreamrdu.com
smartstreamrdu.com