THE M&A JOURNAL

THE INDEPENDENT REPORT ON DEALS AND DEALMAKERS

VOLUME 23 NUMBER 10

AUGUST/SEPTEMBER 2024

The Election

How each candidate is likely to affect the future of M&A

*The M&A Journal is published approximately every six weeks, with ten issues per volume. The sequence of issues is therefore tracked by volume and issue number, rather than by month.

Five Norton Rose Fulbright partners held a panel discussion on September 24 to address what dealmakers can expect from each presidential candidate in the new administration.

The Summary

Robin Adelstein
Global Head of Antitrust and Competition and US Co-Head of Commercial Litigation

The Biden administration has taken an aggressive approach to antitrust enforcement, shifting from the traditional consumer welfare standard to a more populist, public welfare perspective. This shift includes reviving long-dormant statutes like the Robinson-Patman Act and focusing on issues such as labor markets, non-compete agreements, and challenges to major technology companies. While the Federal Trade Commission (FTC), under Lina Khan, has pursued bold antitrust reforms, the future of these initiatives under a new administration is uncertain. A potential Trump presidency might continue the focus on tech giants, though other aspects of Biden's agenda could be rolled back. Conversely, Kamala Harris, while sharing some of Biden's goals, may adopt a more nuanced approach, particularly given her ties to the tech industry. Ultimately, the direction of future antitrust enforcement will depend on the political landscape and leadership shifts.

Rebecca Abou-Chedid
Partner, Project Finance

The U.S. has become the top global exporter of liquefied natural gas (LNG), with facilities requiring key permits from the Federal Energy Regulatory Commission (FERC) and the Department of Energy (DOE) for export. The Biden administration paused approvals for non-free trade agreement (FTA) countries, citing the need for updated economic analysis, though this was later challenged in court. Trump, in a potential second term, would likely reverse this pause. The issue of LNG and energy policy, including fracking, remains a focal point in key states like Pennsylvania and could influence the 2024 election.

Susan Feigin Harris
Co-Head of Healthcare

The healthcare industry is facing significant challenges, with rising operational costs, workforce shortages, and declining reimbursements from Medicare, Medicaid, and commercial payers. Voter concerns this election cycle are primarily focused on inflation and the rising costs of healthcare, particularly insurance premiums. Both presidential candidates are expected to influence healthcare policy, with former President Trump likely to expand Medicaid work requirements, prevent the expansion of Medicaid in states that have not expanded it following the ACA and will allow ACA subsidies to expire, while Vice President Harris would likely expand coverage and maintain Affordable Care Act (ACA) subsidies. Bipartisan efforts on price transparency and site-neutral payment reform are gaining momentum, potentially further adversely impacting hospital payments and their investment in physician and other outpatient services. Regulatory changes, including the impact of the Loper Bright decision, are also expected to shape future healthcare policy under either administration.

David Burton
Partner, Tax

The Election →

The Election

continued

Robin Adelstein
Norton Rose Fulbright

Rebecca Abou-Chedid
Norton Rose Fulbright

Susan Feigin Harris
Norton Rose Fulbright

The Republicans winning the White House is unlikely to result in a full repeal of the Inflation Reduction Act (IRA), as a repeal would require Republicans to control both the House and Senate, a statistically unlikely outcome. Further 18 Republicans in the House and Speaker Johnson have stated they would not support a full repeal of the IRA's tax credit provisions. Also, grassroots support for clean energy tax credits remains strong, even among Trump voters. Trump himself has shown a nuanced stance on solar energy, possibly influenced by family ties to the industry. Additionally, administrative and legal barriers, such as the Supreme Court's recent Chevron Doctrine repeal, would make it difficult for a new administration to roll back existing IRA regulations. If Vice President Harris wins, legislative gridlock is also expected, but her administration would likely continue supporting the IRA through regulatory guidance.

Annmarie Giblin
Partner, Cybersecurity

If a Republican candidate wins the 2024 election, significant changes in privacy, cybersecurity, and artificial intelligence (AI) policies are expected. Republican leadership may halt progress in privacy protections, including state and federal laws safeguarding consumer information, and roll back efforts to strengthen reproductive, sexual, and travel rights in the wake of the Dobbs decision. In cybersecurity, initiatives established by the current administration, such as cyber regulations and the protection of critical infrastructure, could be weakened, and agencies like Cybersecurity and Infrastructure Security Agency (CISA) might be scaled back. Additionally, Republican policies may ease regulations on cryptocurrency and relax current safeguards against cyber threats. AI development will likely remain a priority, but concerns about how AI could be used to monitor the public may intensify under Republican leadership.

The Panel

Robin Adelstein: Good morning everyone. I'm Robin Adelstein, Norton Rose Fulbright's Global Head of Antitrust and Competition, and US Co-head of Commercial Litigation. I'm pleased to be here this morning to speak with you about how antitrust enforcement might change with the change in administration. For more than 50 years, US antitrust has been guided by a consumer welfare standard rooted in concerns about pricing, output and quality. Under President Biden, who's made aggressive antitrust a hallmark of his presidency, the consumer welfare standard has given way to more of a public welfare standard with focus on kitchen table type issues. That is, the Biden administration has been focused on antitrust issues that impact everyday life, things you might discuss with a spouse or a partner over the kitchen table. They're asking the questions of how the public writ large and not just consumers are impacted by competitive behaviors, bringing a more populist perspective.

The Biden administration has attempted to revive statutes that have been dormant for years and use a whole-of-government approach to antitrust. One example is the Robinson-Patman Act, a depression error statute, which looks to protect small businesses and has gone virtually unused for decades. The Biden administration has opened Robinson-Patman Act investigations, and I suspect we'll see the FTC bring an enforcement action soon. The Biden administration has also focused on labor markets and has tried to make changes through aggressive FTC rulemaking. Although the FTC has since been enjoined and the cases are winding their way through the courts, the FTC attempted to ban as an unfair method of competition, employers from entering into non-compete agreements with their workers. And the Biden administration has brought more challenges to mergers than we have seen in any previous administration. But perhaps the biggest hallmark of the Biden administration's antitrust focus is its many highly publicized antitrust cases, challenging the country's largest technology companies.

In sum, the Biden administration's FTC has created, or at the very least, attempted to create a revolutionary sea change in antitrust enforcement. The big question is whether these transformational changes will stick. Trump's prior administration was more aggressive on antitrust than most Republican presidencies. Trump might agree with some of the aggressive stances taken by the Biden administration, although so far he's largely remained silent on antitrust throughout this election cycle. Trump's previous FTC and DOJ applied aggressive theories to mergers focused on vertical challenges in nascent competitors. His administration also sued Google in a suit that the DOJ recently won, and Trump's FTC sued Facebook. As president, Trump also was willing to challenge traditional Republican notions by taking action to lower the prices Medicare pays for drugs and Trump issued a

rule setting up a path to import drugs from Canada and other countries. Many Republicans believe Biden's FTC and DOJ have gone too far on antitrust.

The two Republican FTC commissioners have opposed aggressive rulemaking. If either were appointed FTC chair, it might mean a retreat from the current administration's aggressive enforcement. And while Trump has largely remained silent on antitrust during this election cycle, interestingly, JD Vance who's spent some time practicing antitrust law, has seemingly broken ranks with his party in praising the Biden administration's aggressive antitrust enforcement agenda under FTC chair Lina Khan. Noting that Khan is one of the few people in the Biden administration that Vance thinks is doing a pretty good job. Vance himself has espoused a more populist approach to antitrust and claims to be one of the few Republican supporters of antitrust reform. According to Vance, the large technology companies are too big, and he's called for the breakup of Google over its monopolistic control of information, which sounds remarkably similar to the current administration's rhetoric. So it very well may be that a Trump administration may continue Biden's focus on large technology companies.

Although it's not clear that the remainder of the Biden administration's aggressive enforcement agenda would remain intact. A lot may depend on how much of a say Vance will have in setting a Trump administration antitrust agenda. So in contrast, it's not a given that a Harris presidency would mirror the Biden administration's aggressive approach to antitrust, particularly when it comes to the technology sector, although it may not deviate too, too far. Harris has indicated repeatedly that she'll crack down on price gouging, including calling for aggressive government intervention to curtail grocery costs and promising support for smaller businesses such as grocery stores, meat processors, farmers, and ranchers. This is consistent with the FTC's recent statements that it may investigate high grocery prices caused by a lack of competition. It's also consistent with the current administration's attention to the Robinson-Patman Act. Harris also has focused on what she has indicated are unfair rent increases, again, consistent with the current FTC and DOJ's focus on what it claims to be algorithmic price fixing leading to higher rents.

And Harris has indicated she wants to see pharmaceutical price caps. As a Senator, Harris co-sponsored bills designed to tackle drug price gouging, also an issue for the Biden administration, and she cast the tie-breaking vote in the Senate in 2022, allowing Medicare to negotiate drug prices. During her tenure as California's attorney general, Harris led several high-profile antitrust matters, including in the area of reverse payment settlements with pharmaceutical companies.

During Harris's term as attorney general, California also brought suit for unlawful no-poach agreements, again, a labor market issue, and challenged an insurance industry merger. But Harris, who's from northern California, reportedly has close ties to many in the technology sector who have called for FTC Chair Khan to be removed from the role. One big question is whether Harris would alter the ongoing tech antitrust cases at FTC and DOJ, and whether Harris would remove FTC Chair Khan or Jonathan Kanter at DOJ. And while Harris likely would come under pressure from her party if she pulled support for the aggressive antitrust efforts of the Biden administration, the way we may see this play out in practice if Harris wins is more of a nuanced shift in focus rather than a radical change in direction. Thank you. And over to you, Susan.

Susan Feigin Harris: Good morning. Thanks so much, Robin. I'm Susan Feigin Harris. I'm Co-Head of Norton Rose Fulbright's National Healthcare Team. And I've been asked to speak about the healthcare industry, healthcare policy trends with respect to both of the candidates. And I think the way to sum most of this up is it really is about the economy. In fact, this election cycle, it's been really hard to hear anyone talk at any great length about healthcare issues in contrast to past elections. And I think it can be summed up with the age-old saying "It's the economy, stupid." Individual healthcare issues really rank behind other key topics for voters this fall.

Most voters want to hear about the cost of healthcare and insurance premiums, and that tends to be what is most reported. The primary concerns for voters continue to be inflation and the rising costs of health insurance premiums. In a recent AHA, American Hospital Association report, hospitals and health systems, in fact continue to face escalating operational costs. And for our practice, in particular, my practice, which focuses on hospitals around the United States, the significant layoffs, worker shortages, closures and declining reimbursement from Medicare and Medicaid and other governmental programs as well as commercial payers is really the primary

The Election ➔

David Burton
Norton Rose Fulbright

Annmarie Giblin
Norton Rose Fulbright

The Election

continued

issue I think that confronts our healthcare system and that we see on the front page of many of our papers.

The federal government spent more than 38% than it collected in revenue. So with the large increases in the Medicare and Medicare program and in increasing Medicaid expenditures, this will continue to drive healthcare policy in the legislature and in government. With respect to healthcare reform, it's hard to believe it's been 24 years since the Affordable Care Act passed. And what's very interesting is a majority of voters hold a favorable view of the Affordable Care Act after all this time, including almost half, like 23% of Republicans want the next president and Congress to expand it. So we're likely to see continued tweaks if we have a Trump administration and pretty significant moves under a Harris administration. The Affordable Care Act benefited health systems and hospitals by increasing the number of insured patients, reducing uncompensated care and promoting value-based care models. Hospitals, again, benefit by this because it's better to have an insured patient than an uninsured patient. Same for physicians.

And former President Trump has stated that he's not planning to get rid of the Affordable Care Act. He has concepts. So we can expect that there may be more flexibility given to states and how they manage perhaps their Medicaid programs, but no wholesale elimination of the Affordable Care Act. In contrast, Vice President Harris will continue to support the current administration's policies and we can expect expanded subsidies to exchange plans, increasing coverage options and continuing to crack at the number of uninsured. Research has indicated that the uninsured rate could decrease by 25% if remaining 10 states expanded Medicaid.

We'll move on to the Inflation Reduction Act, which as many people today will talk about. But with respect to healthcare, it's really the Affordable Care Act's enhanced premium tax credits are expected to expire in 2025. We can expect that the Harris administration would move forward to try to maintain those subsidies going forward. If those subsidies go away, we can expect a large number of individuals to have their healthcare insurance premiums go up. And I think we can look at a rise again in what I'll call the underinsured, those individuals who cannot afford even their co-pay and insurance deductible. So what are areas of likely bipartisan agreement? Well, the continued focus on price transparency, the Lower Costs, More Transparency Act, which passed the House in an unusual bipartisan vote of 320 to 71, will codify and expand price transparency rules. In my own practice, with respect to hospitals, we can see complaints are coming in and hospitals are dealing with responses to complaints about failure to provide appropriate and comply with the transparency requirements.

We can also expect more site-neutral payment reform. What is that? That's the payment reform that aims to reduce Medicare costs for services that are provided in more expensive settings like provider-based departments, and to reduce incentives for hospitals to acquire physician practices. This would have a significant impact on our existing hospital system and how hospitals and physicians and outpatient services are delivered. However, CBO has anticipated that making the change, creating site-neutral payment reform, could lead to a $3.7 billion reduction in Medicare spending over the next 10 years.

And finally, with respect to healthcare in general, we know the safe, equitable, and efficient operation of the US health care system and public health depend largely on federal and state regulatory agencies. They regulate safety, the credentialing, use of healthcare products. The change that occurred during this last spring with respect to the administrative review under the Loper Bright decision has got to have some kind of impact on the disputes that exist within the regulatory environment between hospitals, physicians, and those agencies that regulate them. How much really is yet to be determined, but there will be a significant change in direction. We know the executive branch is under scrutiny and we know Congress has developed various task forces focused on what the agencies will do to respond to the Loper Bright change in agency review. And with that, I'm going to turn it over to David.

David Burton: Thank you, Susan. That was very interesting. So I am David Burton. I'm a tax partner in the New York office of Norton Rose Fulbright, and I'm going to discuss the Inflation Reduction Act and the tax credits it provides for normal energy. So a question we are getting a lot is what would a Republican victory in the White House mean for the Inflation Reduction Act? And a repeal is more difficult than it may appear. So just because Trump wins the White House, one should not assume that the Inflation Reduction Act would be fully repealed or even partially repealed. He would also, Republicans would also need to keep control of the House

and then they would need to have at least 50 votes in the Senate with the vice president casting the tiebreaker vote. And if they had all that, it could be, they could pass tax legislation and alter the Inflation Reduction Act using the budget reconciliation process, which is how President Biden pushed the IRA through in 2022.

But winning all three of those aspects of government seems statistically unlikely, but I've been wrong about possible outcomes before. So anything can happen, but getting a majority of the votes in the House is even less likely than just Republicans winning the House or keeping the House because in August, 18 members of the House wrote a letter to Speaker Mike Johnson saying it would not support a full repeal of the IRA because it was creating jobs and economic opportunities in their districts. The key word being a full repeal, the key phrase being a full repeal because that implies that possibly they would entertain partial repeal or selective changes.

Speaker Johnson recently responded to that letter by making comments saying that changes to the IRA would be made with a scalpel, not a sledgehammer. So that shows that even the speaker is recognizing that there is some support within his coalition for the tax credits and Inflation Reduction Act. Earlier this month, the Solar Energy Industry Association SIA published a poll in which 78% of the respondents that described themselves as Trump voters, said they favored the incentives for clean energy in the IRA. So we're even seeing grassroots support amongst Republican voters for the IRA clean energy incentives.

During Trump's debate with Vice President Harris, he said he liked solar but had concerns about how much land it required, and that seems to be a small nod to his voters that support clean energy. He may have been showing a preference for rooftop solar, that is solar that's not mounted on land and rather is mounted on rooftops so it doesn't take land because his son-in-law, Jared Kushner's Affinity Partners made a large investment in a rooftop solar financing company in the summer of 2022. That company is called Mosaic Solar. It's one of the leaders in rooftop solar financing. So that could be why he was suggesting that he might have a more critical view of land mounted solar wersus ground mounted solar. That family connection could also suggest that solar might not be in Trump's gun sights at all. So maybe if he does win the White House, his desire to curtail the IRA tax credits for clean energy would exclude solar.

Even without the passage of legislation, with a stroke of the pen, the president could revoke notices that have been critical to the renewable energy industry, such notices define things like beginning of construction, which tells you whether or not you qualify for tax credits but have sunset dates. However, in President Trump's first administration, those notices were also in effect and he generally approached them with benign neglect. He wasn't really helpful, but he also did not go out of his way to revoke them, to not revoke any of them, didn't even talk about revoking them. So we may see in a possible Trump administration further benign neglect, that he just kind of ignores administrative guidance on clean energy. The Biden administration has proposed many tax regulations to implement the IRA. The Biden administration is doing the best it can to expedite those being finalized. Once they're final, it requires notice and comment under the Administrative Procedure Act, the APA, to change them.

As Susan referred to in her comments, the Supreme Court's repeal of the Chevron Doctrine, taking away the deference to agencies for administrative action, would make it hard for the Trump Treasury Department to just nearly reverse all the favorable final regulations under the Inflation Reduction Act because it would suggest that they will not get the benefit of a presumption of validity with respect to administrative action anymore. And if it was consistent with statutory language in the Biden administration, why isn't it consistent with statutory language in a potential Trump administration? So it's going to be more challenging than it would've been before the Chevron Doctrine was reversed by the Supreme Court, for the Trump administration to change the final regulations that have been issued under the Inflation Reduction Act. So that changes the landscape and the possibilities. Finally, if Vice President Harris wins the White House, her administration as well is likely to face gridlock in Congress.

So really, whoever's in the White House is probably going to be in a gridlock situation. Therefore, legislative expansion of the tax credits in a Harris administration would probably be a difficult road as well. So we should not assume that if Harris wins, that it's just anything can be enacted that the clean energy industry wants. However, under a Harris administration, I would expect to see continued friendly supportive guidance around Inflation Reduction Act credits and clarifications and making those more user-friendly, which can be important and have significant ramifications. So that is a mate-

The Election ➔

The Election

continued

rial benefit to the renewable energy industry if Harris wins the White House, although legislative change in either scenario of control of the White House is really pretty challenging. So those are my thoughts on that. I'm going to hand it off to my partner, Rebecca, who's going to talk about project financing clean energy more broadly than tax credits.

Rebecca Abou-Chedid: Hi everyone. Thank you, David. So first I'm going to cosign everything David said in terms of the IRA, but I'm actually going to focus a little bit about liquefied natural gas and some of the Biden administration's movements on that area and how a possible second Trump term would address those. So liquefied natural gas, the United States has recently surpassed both Qatar and Australia to be the top global exporter of LNG, and there are three key permits that any LNG exporter needs in order to build their facility and export LNG. The first is an authorization from the Federal Energy Regulatory Commission or FERC. That deals with siting and construction of LNG import and export facilities. The second is in order to actually export LNG once natural gas has been liquefied, and there are two separate authorizations you need that come from the Department of Energy. One is to free trade agreement countries, the other is to non-free trade agreement countries.

And in order to issue those export authorizations, the Department of Energy needs to determine that the export would be in the public interest. For countries with a free trade agreement, those exports are deemed in the public interest kind of by default. For non-free trade agreement countries, it goes through a separate analysis. And on January 26 of this year, the Biden administration put a pause on approving additional non-free trade agreement export authorizations. So there was no grandfathering, it didn't apply to any existing non-FTA authorizations, but it did pause those that were pending or anything that would come after January 26. This was obviously a surprise to the industry, especially existing facilities that are trying to expand. The Biden administration's response is that since 2018, which was the last time that the Department of Energy updated their economic analysis, we have tripled our LNG export capacity. And so in their view, an update was needed and that's still underway.

Now on July 1st, a US district court in Louisiana issued an injunction against the pause. And so since then the Department of Energy has confirmed that they're complying with that injunction. Over Labor Day, they issued one permit to export to non-FTA countries for the first time since the pause, which was for a project called the Altamira Project, which started production in July. However, this was a short-term approval. It was about a five-year approval. And projects are typically, when they're fully contracted, those are long-term contracts to export natural gas, usually about 20 years. And so projects are looking for much longer term approvals in order to finance those projects. So LNG is something that I think can be, so we've already seen that in the debate. LNG actually came up in the form of questions about fracking. Vice President Harris had said when she ran for president in 2020 that she would ban fracking.

She has since come to a different conclusion and says that she would not ban fracking. With respect to the pause, former President Trump has said that on day one he would reverse that pause. So there's clearly a difference in opinion between the two candidates when it comes to LNG exporting. And there's also, even within the Democratic Party, there can be differences in the views here, particularly in states like Pennsylvania where the energy industry and specifically fracking and natural gas is a large part of that industry. So in January when the Biden administration issued their pause, you did see the two Democratic senators from Pennsylvania issue a statement together saying that they were concerned about it. So it's definitely not as easy as a Democrat versus Republican issue, but it's one that I think you'll continue to see unfold. In any case, the Department of Energy says that they should be finished by March with their review.

So there isn't an indication that this pause in any case would be a long-term issue. And whether LNG specifically and energy is going to affect the election, I think it really is going to be determined on a state by state basis. So in an election that's going to be won at the margins, for a state like Pennsylvania, that is going to be important. And so I do think you'll hear, not necessarily when they're speaking to national audiences, but when the two candidates are speaking specifically at rallies and everything, to state-based voters that they have to appeal to, you will probably hear questions about energy, renewable energy and LNG and the IRA come up based on what they think those voters in those specific states are interested and want to hear. So I will now turn it to my colleague, Annmarie.

Annmarie Giblin: Thank you Rebecca. Hi everyone. I'm a partner in the Global Privacy and Cybersecurity Group for Norton Rose and also in the Artificial Intelligence Group. So I'm going to direct my comments at those three areas today. The key areas that would be impacted by a change in policy should a Republican candidate win this November, the first one would be privacy. The first would be the direction and momentum of laws and regulations concerning the privacy rights of US citizens. Currently, laws of the United States regulate data by its type, so we have medical and financial information which have enjoyed both federal and state law protections for decades. And what we're seeing today is a revolution in what's considered consumer information, which is a catchall for all other types of information that have been collected and are being collected about Americans as they go through their daily lives. Currently, they're protected by several state laws.

We have 19 enacted. They're not all fully live yet, but they will be within the next two years. And we have certain federal agencies such as the FTC that have made privacy protections a really strong focus and have used things like the FTC Act to protect privacy rights. The current administration has bolstered these efforts with a series of executive orders and empowerment of the FTC to fully regulate this area, which has been effective, giving Americans more visibility and control into how their information is collected and used. And should the Republican candidate win, these efforts might be stalled or stopped. The Dobbs decision not only took away a woman's rights for reproductive choice, but it also challenged decades of legal precedent holding that US citizens have a fundamental constitutional right to privacy. Republicans have made it clear that not only will they not enact federal legislation to provide back those privacy rights that Dobbs has challenged, but they also will probably expand restrictions on such rights as well too.

There are Republican proposals for a federal abortion ban, rights restricting the right to trial from state to state, seemingly aimed at stopping travel to other states to get an abortion. Rights related to the availability and obtaining of reproductive medicine such as contraception and medicine and care related to IVF and in vitro fertilization, of also challenging these procedures as well. They also have proposals aimed at rights related to sexual freedom, the right to marry and the rights for parents to control the upbringing of their children. We've seen several versions of this agenda already playing out in different states, and if similar bills are passed by a Republican-controlled Congress, they would likely be signed by a Republican president. Going back to my colleague's statements before, that is not fully guaranteed as there is a lot of gridlock currently in Congress. However, should all of the tea leaves align, that is possible.

By the same token, it is unlikely that a comprehensive federal consumer privacy law would be passed if a Republican candidate is in office. And actually if one were to get passed by some miracle as well too, it would likely not be as comprehensive as some of the state laws that we currently have. For example, the protections against collecting and using a person's health information, which is now considered personal health information, not protected health information under HIPAA and is an expanding data category currently, could be removed from such bills as it would stress the other Republican restrictions that have been proposed, such as protecting certain elements under state privacy laws and tracking those elements. It's also likely, as we have said before too, that the FTC could be redirected to stand down from its current focus on protecting both the cybersecurity and privacy rights of Americans, while potentially freedom of information laws could be repealed or amended to protect certain government records from review and public scrutiny.

The second area of cybersecurity concerns, which are not only becoming more serious, but also a bigger part of everyday lives for Americans. If the Republican candidate wins, there are several areas of cybersecurity that could be stressed. The current administration has put several new laws in place to better heat map the cyber risks around the United States, specifically referring to new CISA cyber reporting regulations and the enhanced role of CISA generally. They've also put in place protections for Americans' personal information, the transfer of which not only to data brokers, but to countries of concern. They've also put in new regulations and requirements about American companies becoming more cybersecure, specifically the White House National Cybersecurity Strategy, new FTC regulation, new high-tech regulations, the use of the FTC Act and updates to the NIST standards and frameworks, including CISA's continuing cybersecurity public-private partnership with many of the largest companies.

Even though many of these initiatives were started by the previous administration, they do not seem to be a policy goal of the current candidate. It is not clear how efforts that going

The Election ➔

The Election

continued

after threat actors internationally would also be stressed, as in some cases they're suspected to be backed by foreign governments. And the current administration has been balancing the need to secure our critical infrastructure and Americans generally from these threats, while also not directly engaging the governments suspected of supporting and enabling these threat actors. If the Republican candidate wins, this could be changed in a number of unpredictable ways, including the potential for the candidate's positions on the war in Ukraine and NATO generally, stressing the cooperation that the US utilizes and relies on from our allies when trying to address these risks internationally and prosecuting cyber threat actors abroad, but also possibly to a softening of the new proposed and considered regulations which are meant to further protect our critical infrastructure.

Additionally, as mentioned by my colleagues, without Chevron, agencies no longer have the deference to interpret broad regulations as a matter of course in certain court cases that would actually challenge them. This is particularly concerning in the cyber security field where the technology protections and threats are constantly changing and require experience and practical interpretation. Currently, there are also pending CISA regulations that will change and create new obligations for most companies, but the ability for CISA to enforce them as needed may be challenged by the lack of Chevron and potentially by the lack or gutting of these regulations. On the White House National Cybersecurity Strategy enacted by the current administration, this calls for new regulations aimed at software and hardware developers to make their products more cyber secure. It includes increased liabilities for them as well. And it's possible that we may not see these regulations come to fruition or they may become softer if the Republican candidate wins.

It's also not clear if the Cybersecurity and Infrastructure Security Agency, CISA will be disbanded or greatly reduced under a Republican president. Several other federal agencies like the Department of Education have been targeted for potential destruction. So it's not clear how far that would go, and if that would impact CISA as well. And finally, on that space, considering the Republican candidate has just launched his own cryptocurrency, it's unlikely that any new regulations would be created for the crypto industry and possibly it could stress the development of a central bank digital currency or a digital dollar, as that could be seen as a threat to other types of coins of this nature. It's also likely the anti-money laundering laws that currently apply to crypto wallets and exchanges may be softened or repealed as that stresses these types of coins as well too.

And it could lead to an increase in ransomware as cryptocurrency remains the preferred payment method of choice for threat actors. And then finally, in artificial intelligence, regardless of who wins, it is expected that the federal government will continue to prioritize artificial intelligence. There is a concern regardless of who wins over how the government will use AI to monitor and control the US public generally. These concerns are slightly increased with the Republican candidate winning as he has discussed, using tools of the government for personal vendettas and for other methods to, as we mentioned before, restrict privacy rights that have been taken away by the Dobbs decision. It is unlikely that a Republican administration would continue the sanctions and export controls that have put in place to secure American technology and the foundations of AI. Additionally, the Republican candidate might seek to repeal or limit the CHIPS and Science Act, which has also sought to strengthen the underlying technology for artificial intelligence for the United States as well too.

It is very likely as well, going back to the FTC, that the FTC will not be as aggressive in its privacy and cybersecurity pursuits, but also the work it's doing to protect Americans from the bad effects of AI like deepfakes and other concerns related to cybersecurity, but also could challenge their year-long effort of addressing the problems that AI creates for current encryption methods and standards and the work they're doing to prepare for new types of encryption, especially on the eve of quantum computing.

Question time

To Ms. Adelstein: How might the private litigation community view a potential change in administration?

Ms. Adelstein: So it's really interesting that you have a very active FTC and DOJ, and they've really changed the way antitrust is being interpreted. As I said, you had this consumer welfare standard for decades, and now they're taking a different approach to antitrust. The problem they have is that the law has been established based on the old standard for how antitrust should be looked at with a focus on pricing and output and

quality.

And so what the FTC and DOJ need to happen is for the law to change. And the only way that the law can change is if there are challenges to the rule of law, and you have new precedent and new case law being made. So they've been aggressive in trying to change the way the law is being interpreted. We also see then the private plaintiffs' bar following on, and where you see aggressive antitrust enforcement, you see plaintiffs' class action lawyers trying to mirror that. And the more aggressive the government is, the more you see an active plaintiffs' class action bar. And so the aggressive stance by the current administration has been mirrored in the private litigation bar as well. Assuming that aggressive litigation continues by the government under a Harris administration, I think we'll continue to see a very active private litigation bar. And that may continue as well as I spoke about earlier under a Trump administration.

To Ms. Feigin Harris: The Medicaid program financing appears to be a source of increased congressional and agency oversight. Can you explain why? And then also, what do you foresee with states and their various Medicaid program expansion plans or non-plans?

Ms. Feigin Harris: Yes. Well, Medicaid, I don't know how many people know this, but Medicaid is one of the major insurers for children in the United States. And because every state enacts a slightly different Medicaid program in conjunction with Medicare, excuse me, in conjunction with the federal government, because of the way the funding works, every state's Medicaid program is different because the funding mechanisms all have altered. Each of the states, specifically states that have not expanded their Medicaid programs, have looked at, I'll call it unique ways to draw down federal funding. Some of those mechanisms have pushed the envelope with respect to what the current administration believes is appropriate under the federal law. And so what we've seen is some regulations that were issued last year that really challenge some very specific funding mechanisms in the states. And ultimately, the entities that come that are in the middle of this are the hospitals and the providers who are just seeking the more wholesome payment under the Medicaid program.

Medicaid in particular is well known for underfunding and underpaying. So for every patient that walks in a door, you do not receive the costs of the care that you're expending. So there are all these supplemental payments that have grown up over time to try to help sustain hospitals. And as I said at the outset, the issues of the sustenance of hospitals in the United States and trying to ensure that rural hospitals and others don't close is a very important component of what we foresee in the future as of great concern. This issue is one of the key issues that will come up over the next four to five years in terms of how we continue to sustain our hospital systems. In particular, those in the rural areas of the country, those who treat large number of Medicaid program and uninsured patients. Those tend to be freestanding children's hospitals, but not exclusively.

They also tend to be public safety net hospitals. And so that is why there's been such scrutiny. I would say that most of the work that is currently being done in the United States by lawyers is work to try to figure out how to appropriately draw down those federal funds in a legal way and create those funding mechanisms in a sustainable way. And the law is consistently changing and the regulations are changing rapidly. So this happens to be an issue of litigation. We'll see how it plays out, but it is currently a hot topic, certainly in my area. So hopefully that answers the question.

To Mr. Burton: Given your experience with structuring tax-efficient transactions for renewable energy, what tax initiatives or reforms should policymakers prioritize to encourage further investment in sustainable energy post-election?

Mr. Burton: That's an interesting question. The first thing is that we shift the tech-neutral credits next year for projects that start construction under the tax definition of starting construction next year or later. They're subject to the tech-neutral credits, and those credits are not available if you have any emissions, and that means fuel cells and biogas will not qualify for tax credits if the project starts construction after this year. Fuel cells and biogas have other valuable environmental attributes. For instance, with biogas, you're often taking manure from a dairy farm and turning that into renewable natural gas rather than just having it decompose and have the methane released anyway.

But those credits seem to be extended for fuel cells and biogas and other effectively clean energy technologies, but nonetheless have some amount of emissions, so they won't qualify. So that would be an important thing. Again,

The Election ➔

The Election

continued

unlikely to happen due to gridlock, but that would be a very good policy to pursue. The other thing is that the Department of Energy has concluded that geothermal heat pumps are the cleanest, most efficient way to provide heating and air conditioning services. So geothermal heat pumps use the difference between the temperature of the ground and the temperature of the air to either heat or cool buildings, from homes to skyscrapers. The technology qualifies for tax credits even after next year, but faces three obstacles, one of which is the proposed investment tax credit regulations to prohibit what we refer to as split ownership. So in other words, the same taxpayer needs to own the geothermal loop out in the backyard as owns the heat pump in the basement.

And there are regulatory restrictions on that happening. In some instances, utilities are not, in some jurisdictions are not allowed to own the equipment in the house. There's also economic considerations, but it just makes it very impractical. The same company has to own the big heat loop out in the backyard and own the heat pump and piping in the house. The second issue is that there's a concern that those geothermal heat pumps could be subject to what's called the limited use property doctrine, which would make tax equity transactions difficult on them. And tax equity is really the most efficient way to monetize tax credits and depreciation. And the Geothermal Exchange Association, the trade associaion for this industry has asked Treasury to address that, Treasury declined, and said it required a legislative fix. So that too would require legislation. That probably should not be that controversial.

But nonetheless, the Treasury says it doesn't want to do it and it doesn't have the authority to do it, and it must be done legislatively. Finally, geothermal heat pumps do not have a domestic content that takes the tax credit from 30 to 40%. That's an additional 10% on it. Equipment has to be, or a project has to be 40% domestic to qualify for that. And wind, solar and batteries have safe harbors and make it very clear as to how to calculate whether or not something is foreign or domestic and meets that 40% threshold. But geothermal heat pumps do not, and that's hampering the implementation of the technology on a broad basis around the country.

To Ms. Giblin: How might the key agencies such as the DHS, TSA, etc, be impacted by either Harris or Trump regarding cyber security policy on critical infrastructure?

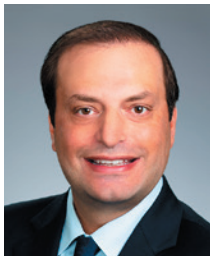
Ms. Giblin: That's a great question. If Vice President Harris wins, it would most likely remain the same. This administration has been really focused on shoring up cyber security, not only for the federal government and then from a national security perspective, but also helping a lot of companies in the small to the small, to the large to the large, get their cyber house in order, which has been a great effort that really was started actually in the previous administration, but greatly continued and expanded during this one.

So I would largely expect that to continue if Vice President Harris were to win, if former President Trump were to win, I'm not sure, because the proposals have been kind of all over the place. We haven't seen anything specific on cyber security come out that would seem to stress it, or it should remain a goal of any administration. But the proposals regarding less regulation and decreasing the size of the federal government could stress these agencies depending on how they impacted them. So overall, cyber security remains a huge concern, but we're not, I can't really read the tea leaves fully on that to see how it would be different.

~~MA~~

Private Equity

Why did transactions fade away and what will bring them back?



Alain Dermarkar
US Co-head of Private Equity and Private Equity Sector Lead
A&O Shearman

Christopher Zochowski
US Co-head of Private Equity and Private Equity Sector Lead
A&O Shearman

To discuss the plight of private equity, both its frail condition and the rising hopes for its revival, we turn to two renowned leaders of the industry: Alain Dermarkar and Christopher Zochowski, co-leaders of the practice at A&O Shearman.

Private equity has been quiet for some time, sinking to record levels. At one point in 2023, for example, the value of sponsor activity dropped from a high in the number of deals of 9,667 worth $1.85 billion to 7,346 transactions worth $645 million, the second lowest number in the past six years. The lowest, below that of 2020 came during Covid. Take-privates were below 2022 levels. Some experts point to the fact that there were more failed processes and more withdrawn transactions in the last eight years.

But something is stirring under the permafrost. On September 18, the Federal Reserve cut the interest rate by a full 0.5 percent. "A cut was widely expected and had already been largely factored in," says Mr. Dermarkar, "so if it hadn't happened I think you would have seen negative implications for the PE industry. Overall, this cut does help to reassure the industry that rates have peaked for the foreseeable future and helps to lower the cost of capital for transactions."

Mr. Zochowski agrees: "I may add that the current rate cut and potential additional rates cuts to come should help to unlock sell-side opportunities by private equity firms in 2025 as such firms seek to achieve improved realizations more in line with the investment thesis applicable to their portfolio companies."

We turn now to what each of the two lawyers sees as the causes and effects of the hibernation. First up is Mr. Zochowski.

What happened to private equity?

Mr. Zochowski: The dramatic increase in interest rates put a damper on the market. It caused a contraction because the market had been modeled on very low interest rates for a very long time, and all of a sudden we had a very different dynamic, very different modeling for an investment thesis. The rate increase occurred so quickly that it caused everybody, both those in the process of a transaction and those exploring new deals, to reconsider the way that they were evaluating the economics of these transactions. The result is that transactions simply cost more from a buy side perspective, which put downward pressure on purchase price discussions with sellers; in essence, it created a gap between buyers and sellers on valuation. In order to bridge that valuation gap, the market needed to get more comfortable with some more unconventional economic structures. We've seen an increase in earn outs and other alternative financing strategies, such as bridge financings among funds, in order to close that gap.

But all that took quite a while to work its way into the system to normalize the approach. I think in 2024, we've seen an increase in activity, but personally I feel like it hasn't been a robust return at this point for several reasons. For one, sponsors are also sellers with portfolio companies that they need to monetize to return money to LPs and develop their track record. But the market dynamics I discussed have caused the

Private Equity ➔

Private Equity

continued

carrying value for many portfolio companies to exceed current valuation expectations for a sell-side opportunity. Rather than sell prematurely, the goal has been to hold onto companies until valuations improve on the sell-side. But this extended hold period has also caused the pace of returning capital to LPs to slow, thereby causing negative pressure on the fund raising market for new funds. This, in turn, causes a slow down of new funds to hit the market on the buy-side. This cycle has dampened activity in the market generally. That said, I think you see quality assets being sold, but there's still a lot of sell side opportunities waiting to come to market.

Mr. Dermarkar: I echo what Chris said. I think there was a lot more impact in 2023 and early 2024. Now, I think people are coming to the realization rates are not going to go any higher, which has helped stabilize the market. In fact, the market has priced in a 92 percent chance of a rate cut even before the election. So I think the impact of it has largely subsided at this point. It is what it is, and people have started to get on with it. [Note: The market was right. The Federal Reserve cut interest rates by half a percent on September 18.]

You hear a great deal about dry powder and how dealmakers are always under deadlines to deploy it. This adds to private equity's special difficulties when it's just not an advantageous time to do so. Is that an accurate characterization of today's private equity market?

Mr. Dermarkar: Yes. It is difficult. I mean, I think we're in a period of historic lows on the sell side from PE. Holding periods are so high and as more funds go into fundraising mode and what they're telling us they're hearing more and more from their LPs is "We'd love to invest, but you've got to return some of our money so we can recycle it." That is a lot of pressure to start to do some divestitures and to realize some gains both to demonstrate the track record, but also to provide money that can then be recycled into the next fund.

Mr. Zochowski: The market is dynamic; it's a series of interrelated elements. You're a fund, you've raised $5 billion, you've deployed that capital, you have a portfolio. But because of market dynamics, you probably have your portfolio marked in a way that you need to get some more value out of it before you sell in order to achieve your investment thesis goals.

So you hold onto the companies longer than anticipated while, at the same time, you need to raise your next fund. So you go to your own LPs as well as LPs of other funds and they all say: "But we haven't been returned enough capital." This creates a tension. A similar tension exists on the fund raising and deployment side. If you raised a $5 billion fund but don't deploy it, then it makes it harder to justify raising the next fund of similar or larger size. But to raise that next fund, you need LPs to be flush with cash on the returns you provide from your existing portfolio. The idea is to always be growing. So there's a pressure to fully deploy capital and to return capital on a relatively consistent time frame. All these elements are interrelated. One element dominoes into other elements. It's a cycle.

Is this reminiscent of other cycles that have come and gone? Are there special characteristics of this one that make it more or less difficult?

Mr. Dermarkar: All cycles have basically a similar feel. They vary more in length than in the kind of driver or impetus for each. Fundamentally, at its crux, it's a valuation disconnect. So if you look at the financial crisis, there was certainly a disconnect. I'd say the difference here is probably for virtually my entire career and probably in the entire career of many private equity folks, rates have always been lower than this. And so this may be the first time that a lot of people in PE have seen rates at such a high level.

Mr. Zochowski: Looking back on the cycles I've been through, this isn't like the financial crisis in 2008 where there was an absence of financing to do anything. Period. It was a crisis in confidence about many things. That's not this. And you can't compare this to capital market cycles, which are just different for many reasons. This is a cycle that, all things being equal, should not have occurred. It was artificially created. Since the financial crisis, we had this dip in rates, which is really contrary to the way rates have always been set throughout history. Rates have naturally and historically been considerably higher. The persistence of low interest rates is what makes this somewhat artificial. However, confidence is high and the appetite for activity is high and, because of that, I would say that this cycle will be less difficult to resolve. It requires

shedding some artificial supports and a return to normalcy in deal evaluation and execution. In this regard, I don't think there is a bubble to burst; rather, I think the market is just digesting elements of a new normal.

Is all this similar to the valuation issues that strategic buyers and sellers have been facing or is private equity its own world?

Mr. Zochowski: I think strategic buyers are just fundamentally different. They buy for different reasons so I don't think you can necessarily compare the two. They also have different economic strategies and timelines at play, as well as the ways that they finance their transactions. Their investor base is different and the goals and objectives of a transaction are different. Overall, while the M&A process elements may be similar, the buy/sell/hold dynamics of strategics are fundamentally different than those of private equity sponsors.

Mr. Dermarkar: I agree. They have also experienced, most of them anyway, an increase in the value of the currency they can use, their stock. And they're not typically doing some type of leveraged acquisition. So I don't think it affects them as much because, as Chris said, theirs is a totally different dynamic. I mean, it affects the models as to add-ons and how they can consolidate in the industry, who they can potentially sell to in further transactions. Plus the FTC and the regulators pressing to get more disclosure out of private equity shops, including a push to limit board interlock.

Mr. Zochowski: I'd like to add to what Alain just said on antitrust regulators. In certain segments of the market, it's more relevant than others, with one caveat. Private equity is I think notoriously focused on roll up or consolidation efforts as part of their overall strategy. And so you might do a lot of small deals, but I think there's probably a little more scrutiny being put on even small deals below filing thresholds where consolidation may be occurring. And certainly the position of the FTC and DOJ is to make antitrust elements more a point of discussion, whereas I think 5 years ago or 10 years ago, it was really just a question of, are we filing or are we not filing? I think today there's a little bit more discussion about some of the substantive issues that come along with deal execution.

Mr. Dermarkar: Yeah, that's right. Indeed, I think the new HSR rules and the new filing requirements require a lot more disclosure on your roll-up strategy. I don't think they're doing anything with it imminently but you can see where it's going, where they might try to argue a preemptive issue based on your future strategy.

Mr. Zochowski: The policy direction is anti-transactional and anti-private equity. I'm not sure it's necessarily having the impact in terms of slowing the market, but it's definitely creating situations where you have to have more conversations.

How do you see the election and how it might affect private equity and dealmaking in general?

Mr. Dermarkar: Normally any election can have a major effect on the deal market, particularly when you have elections with big tax changes, which this one potentially could. We hear a lot about it, but candidly, I haven't heard anybody talk about the election this time around.

Mr. Zochowski: I haven't either. Taxes could play a role, but in general I haven't heard too much talk about the election having an important impact. Unlike prior election cycles, nobody has been saying, "Okay, we need to get this done before the next administration comes in." I haven't heard any of that type of discussion.

Turning to your own merger with Allen & Overy, you are now basically partners in a different firm.

Mr. Dermarkar: It's more fun advising on mergers than going through a merger. However, there is a lot of excitement and optimism about the possibilities this combination provides. The combined platform is really the first fully integrated law firm with unparalleled geographic reach and global scale, with depth and quality of experience in all key global markets.

Mr. Zochowski: That's true. At first, you don't quite comprehend how much focus is required because everything changes. Your website changes, your pitch materials change, your capabilities change, etc. All to the better, of course. But, you're trying to pull from all different parts of previously two separate organizations. Plus, it's a people business. We're not selling a product. We're selling the services of individuals with expertise. Trying to reorganize 4000 lawyers is a daunting task. It is a lot of work and, as Alain

Private Equity ➔

Private Equity

continued

said, it's better to be an advisor to a merger.

That said, we're really excited. It's been a great cultural fit and I think that we are really well positioned globally to be very competitive and offer great capability to our clients in a lot of regions and countries. We're really eager to push forward.

~~MA~~

Cybersecurity

The Berkeley Spring Forum

The Panel

An introduction by Ethan Klingsberg, Forum co-host and co-head of U.S. corporate M&A at Freshfields

Freshfields partner Beth George (former acting General Counsel of the Department of Defense) moderated a panel with Spencer Fisher (Department of Homeland Security, Cybersecurity and Infrastructure Security Agency), Sean Newell (DOJ, Chief of the National Security and Cybersecurity Section), and Jorge Tenreiro (SEC's Crypto Asset and Cyber Unit).

The conversation kicked off with a discussion about cybersecurity risks facing the United States. Sean explained the entirely new level of sophistication that cyberattackers have developed and potential risks posed to US companies that are unable to maintain sufficient levels of preparedness to effectively anticipate and respond to such attack.

The panel discussed how M&A can make companies vulnerable to cyberattacks as a result of weaknesses at the target company and the pressure for systems to be decrypted and otherwise compromised to facilitate integration. Cyberattackers take advantage of the transition period that M&A integration presents.

The panelists then discussed the fact that the threat of cyberattack comes from not only individual criminal actors, but also nation-states. Cybercriminals have developed a synthesized ecosystem of "ransomeware-as-a-service," in which they pool diverse expertise to launch attacks against U.S. companies. Nation-states find cyberattacks can be a low-cost way to advance their regime goals. Partly as a result of this phenomenon, preventing cyberattacks is not only essential to protect U.S. information systems, but key to maintaining the physical security of U.S. critical infrastructure. Cyberattacks have also posed threats to U.S. democracy in more abstract ways; for example, in 2020, Iran attempted to disrupt the presidential election through cybersecurity breaches. Partly because both individual cybercriminals and nation-state cyberattackers usually operate from safe havens that U.S. justice systems can't reach, the traditional law enforcement model does not translate well to cybersecurity. Instead, rather than building a case over a long time that eventually goes to court and/ortrial, the DOJ has pivoted to attempting to "disrupt" cyberattacks by anticipating them and buying time to dismantle the hackers' operations, a more preemptive model than traditional prosecution.

Finally, the panel addressed the intersection of cybersecurity and public company disclosure requirements relating to cyber risk, through a case study of a hack of a company called

Solarwinds. Beth described Solarwinds as an "exquisite hack" because of how Russia managed to target the U.S. government through a cyberattack on a cybersecurity company, manipulating source code in a software update in order to target the users of the software, including several government agencies. Spencer discussed the steps the DOJ has taken in light of Solarwinds to improve its ability to protect critical infrastructure from cyberattacks on U.S. companies with access to government infrastructure.

As a result of the attack, the SEC charged not only the company itself but also its Chief Information Security Officer with fraud and internal controls failure. The panel discussed how the SEC's case against and the SEC's new rule requiring public companies to disclose cybersecurity breaches within a matter of days significantly increases exposure for public companies for disclosure violations on top of any liability that results from the underlying security breach. Jorge highlighted that the new rule reflects the view that information about cyber risks is material to investors.

The panel closed with a very helpful discussion of practical steps that CISOs can take to avoid liability for cybersecurity breaches and related disclosure obligations. These takeaways included steps relating to internal education and engagement within one's company, as well as monitoring and internal implementation of proper systems and disciplinary actions for nono-compliance.

The Discussion

Moderator: Beth George, Partner and head of Strategic Risk and Crisis Management, Freshfields; former General Counsel of the U.S. Department of Defense:

Beth George: Cyber ecurity has been a really hot topic over the last couple of years. Then, AI came on the scene and now everyone seems to have forgotten that cyber security is an issue, but everyone's still after your data. I can't tell you the number of M&A deals that I have been brought into because in the middle of the deal, a hack has happened normally in the target and we're trying to assess what's the risk for the acquiring company.

We're very lucky today to be joined by three of the leading—I know you guys don't want to be called regulators—government officials tackling at cyber security issues. You have a great range of folks to hear from today.

First, to my immediate left is Spencer Fisher, he's the Chief Counsel of the Cybersecurity and Infrastructure Security Agency, otherwise known as CISA at DHS. CISA is probably the crown jewel that the government thinks of as its attempt to address cybersecurity issues.

Next to him, is Sean Newell, Chief of the National Security Cybersecurity section at DOJ. Thinking of the DOJ, he has one very specific area that he focuses on, and that's nation-state actors, which tend to be the most pernicious areas of attacks in the areas where we see actual material devastating impacts to companies. He'll describe a little bit about that.

Then, on the phone, hopefully we have, by video, Jorge Tenreiro, who's the Deputy Chief at the SEC on enforcement, who's going to talk a little bit about the pain points that I think probably most people in this room are very familiar with, the new cybersecurity rules around the SEC and the SEC's enforcement actions around this.

Really excited to have all of you here. I want to start by just introducing this audience to your areas of expertise. This is of course, only three of the pillars, there's probably another 20 at the United States Government, that are trying to tackle cybersecurity.

Sean, I wanted to start with you. It's been well over a decade now that DOJ has been very strong in playing this area of national security-meets-cybersecurity. Since then, we've seen, I think about 10 to 12 years ago, the United States Government first started talking publicly about Chinese hacking of U.S. companies. At the time, I think the FBI director called it the greatest transfer of wealth in history, if that's totally accurate, but that was the lens through which it-

Sean Newell: It was the NSA director, yes. Keith Alexander.

Ms. George: Yes, the NSA director. There's been North Korea's attack on Sony, there's been Russia's exquisite attack on Solarwinds, which we'll talk about a little bit, there was Colonial Pipeline. Right now, we're in the middle of Change Healthcare, which has a ransomware attack that may or may not be nation-state based. Microsoft most recently released, not one, but two 8-Ks about a nation-state hack on their systems, and the second 8-K noting that it had happenedand the second 8-K noting that it was actually ongoing. Can you give us a little bit more background on how National Security Division at DOJ sees the world, the threat picture right now? What's keeping you guys awake and how you guys are getting involved in some of

Cybersecurity ➔

Cybersecurity

continued

these attacks on U.S. companies?

Mr. Newell: Thank you Beth. First of all, I do want to thank Jorge for wearing a tie today. Spencer abandoned me by getting rid of his tie. It's not a very good representation of Washington D.C.

Nonetheless, as far as the threat picture, what we are seeing, unfortunately is I think both in the nation-state context and the transnational criminal organization context, just the actors continuing to evolve, continuing to increase the sophistication and scale of their activities. There's a large number of factors to that. I think on the nation-state side of the house, you now see these countries seeing cyber-enabled activities, whether it's theft or destructive or disruptive cyber-attacks, theft of crypto or fiat currency in the case of North Korea. They see these as all low cost ways to advance their regime goals.

Then on the criminal side of the House, you're definitely seeing the development of an ecosystem with specialization of cyber criminals where you have one cyber criminal who is really good at coding malware and you have another one who's really good at obtaining initial access to companies. And they're just developing this ecosystem where they're all coming together in what we call, in the ransomware context, ransomware as a service, and just really upping their game in the scale of their attacks.

I think on the government side, as set forth in the administration's National Cybersecurity Strategy, which came out last year, we have really been called upon and we called upon ourselves to up our own game in countering these activities. For the National Security Division of the Department of Justice, one of the things that we have done to help implement that strategy is we have stood up the National Security Cyber section, which I now lead, which has prosecutors who are entirely devoted to disrupting nation state hackers. We have colleagues in our criminal division in the computer crime and intellectual property section who are entirely devoted towards disrupting the criminal threat. And we have AUSAs all around the country, including here in San Francisco and Oakland and San Jose, who are also working in these types of cases.

One thing I want to point out there before I talk about what keeps me up at night, you'll hear me say, "disrupting," because that is something that I think is being emphasized right now by the Department of Justice and our leadership in the context of our own strategy to disrupt cyber threats and in the National Cybesecurity Strategy, which is we're all prosecutors at heart, we work with the FBI, we have their law enforcement agents, they have handcuffs, they like going and arresting people, but in the cyber context, that law enforcement model of building a case over a long period of time, keeping a secret, busting down the door, arresting the guy and taking him to the courtroom and having a trial and eventually convicting them. It's just not perfectly applicable in the cyber context because a lot of our adversaries, whether they're transnational cyber criminals or nation states, are obviously hacking from safe havens. They're in places where we can't get to them with our law enforcement tools. While arresting them is the ultimate disruption, we think we have to think of other ways to raise their costs, to prevent them from doing what they want to do and from buying network defenders time and space to defend their companies. We really are focusing on that, even though we're prosecutors and law enforcement nation as a heart, we see our mission much more through a cybersecurity lens and enhancing cybersecurity.

What keeps me up at night. Personally, for me, looking ahead, we're talking about the People's Republic of China actors targeting critical infrastructure. You've probably heard about a lot of discussion from the US government about that since November of last year. Something that we are seeing, we're disrupting it as much as we can. DOJ launched a core authorized operation back in December and January to really disrupt some of the infrastructure the Chinese hackers are using to target our critical infrastructure, to lie low and gain persistent access to eventually maybe take an action to disrupt that critical infrastructure if there were ever a crisis between the United States and China.

That definitely is something that's high on our radar. Iran is doing a little bit of activity targeting industrial control systems, a similar type. And then, I'm also right now thinking a lot about formula line influence, cyber-enabled formula line influence in the context of the forthcoming election in November, 2024. For here, trying to figure out how the actors are going to try to sow division, create misinformation, things along those lines in the context of our election. We've seen that happen in 2020. I don't know if folks are familiar with that. We saw the Iranian government, the IRGC, in particular, conducting a campaign to sow discord by pretending they're the Proud Boys and threatening democratic voters,

and then they compromised a media company and they were going to put out fake news stories after the election. Luckily, we caught onto it and headed that off at the pass. But those are the two things that keep me up.

From the business community, I might actually tweak that a little bit and say PRC is still, but maybe the theft of intellectual property, of sense-of-business data that continues. We're fighting it, but they continue to do that and they're continuing to look out there for companies in the West that have technologies, have data that would advance their own objectives, which are pretty much laid out in their five-year plans.

And then ransomware, the ransomware actors are out there looking for opportunities. Beth, you mentioned the context of M&A, companies getting hit, and I think we are seeing them, and the FBI actually put an alert about this out in November, 2021. We're seeing these actors recognizing that certain business events, and M&A transactions being one of them, where they have maximum leverage over the victims, they have maximum opportunity to gain that initial access to the system and that's because there's unclear reporting lines in the context of the merger or the acquisition, there's legacy systems, they're being left over after an acquisition, there's the cybersecurity folks are more focused on the transition as opposed to cybersecurity at that point in time. And then, there's a lot of pressure to actually get your systems decrypted, so they have maximum leverage on actually extorting that payment from them.

I think from a government perspective, I'm focused on a critical infrastructure, formula line influence, but I think from a business community perspective, I would almost say the big things are PRC theft of data and then the ransomware threat.

Ms. George: That makes a lot of sense to me. I think even on the outside in the private sector, I've been struck by the number of times that my clients have had a ransomware incident that seems to be exquisitely timed around 10K, 10Q reporting at some point where that 72-hour deadline is buttressed by something else and it's trying to prevent you from trying to negotiate that out. It's definitely something I think we see in the private sector.

Spencer, Sean talked a little bit about critical infrastructure, but that's really your bread and butter over at CISA. When we talk about critical infrastructure, I think it's really easy for people to think about water facilities, energy plants, but it's broader. How does the government think about critical infrastructure?

Spencer Fisher: Thank you for having me today. . I really appreciate it. The weather here is awful. It's just terrible. I can't believe I came, but gorgeous day. Thank you.

The nation's critical infrastructure, it's organized into 16 different sectors, those comprise assets, systems, and networks, whether physical or virtual that are considered so vital to the United States that destruction and incapacitation would have a debilitating effect on security, national, economic security, or public health and safety. That is, as you mentioned, the bread and butter of CISA's mission. But within that mission set, we have to prioritize, just like every agency has to prioritize what it focuses on. So I'll just run through a few of the things that we're prioritizing in that space and that might be helpful for folks to hear.

At the end of last year, we launched a shields-ready campaign making resilience during incidents a reality by encouraging organizations and individuals to take action before an incident actually occurs. In the government or in the military, we would talk about this as left of boom, and that is part of CISA's guidance at this time and we're going to continue to promote that in 2024.

I'll be the first to say AI, so yep, gotcha, gotcha, and awesome, you know I wanted to do this, I'm going to slightly take a detour here and mention that I visited a very awesome gentleman down the road here that shines shoes and has been doing so for 40 years, right down the road from here. He had something interesting to say. He told me that in the buildings surrounding where he works, again, just a few blocks down the road here, everyone now is working on AI. And he said, "You know what I've found is that every 12 years, that changes." Twelve years ago it was social media, 12 years before that it was dotcom. He said, "12 years from now, that'll be something else." And I thought, "That's pretty awesome. That actually sounds perfectly true."

Right now, AI though is top of mind for everyone and we need to make sure that we're prepared for the adoption of that technology across critical infrastructure. CISA has a number of initiatives and products as well as standalone products on AI that we've co-sealed with other agencies as well as other governments that promote the safe and responsible design of AI products.

Third, we're looking to support, if folks have not heard about Secure by Design, a Secure by Design revolution, there's no other way to put it.

Cybersecurity ➔

Cybersecurity

continued

And this movement really looks to shift cybersecurity burdens to product vendors and away from end users and create a culture of security within innovation. This is discussed in the Cyber Security Strategy that Sean mentioned and ancillary or parallel to that is a conversation and an ongoing dialogue about software liability standards. My team at the CISA Chief Counsel's office has been deeply involved in those discussions.

Next, as Sean mentioned, is securing the 2024 elections. That extends the protection of individuals actually running elections at the state and local level. This is something that's near and dear to my heart, I've worked on elections in one way or another really my whole career starting out at the Department of Justice. We just released today a product co-sealed with the FBI and ODNI on FMI, Foreign Malign Influence, and we continue to put out products and guidance on securing our elections and protecting 2024.

Finally, and certainly not least, is a campaign that we've started called Secure Our World. I knew I made it, I knew I made it when I was hired at CISA and went grocery shopping at Safeway and heard a jingle for Secure Our World playing over the loudspeaker. And I was like, "That's cool. That's where I work."

Secure Our World's a campaign, it's a call to action really for businesses, states, local governments, schools, hospitals to consider security an essential element of our everyday interactions. Technology is such a fundamental part of our daily lives that we need it to be reliable and secure, it's the job of tech manufacturers to help with that. But we also need to make sure as end users, we're doing the basics to stay safe and responsible. CISA is working to help folks get there.

In addition, I'll just mention a few since you mentioned the critical infrastructure, there are a few focus areas that our director and the agency have identified such as K-to-12 schools, the water sector, it was mentioned earlier, hospitals as you mentioned, the change healthcare. There are pieces of that that we're focused on, but obviously we have to worry about the whole as well.

We're the lead for cyber defense, the national lead for cyber defense, but really we're all on the front lines to borrow some of my military parlance when it comes to defending and creating a safe cyberspace. Over the next year, you can expect CISA as we've done over the past several years, to keep developing and putting out products and guidance in that respect.

Ms. George: Thanks Spencer. Jorge, I think you're probably the regulator that everyone's the most familiar with in this room. The SEC has been active in cybersecurity for over a decade and that most recently culminated in publishing a rule on requiring reporting on material cybersecurity incidents. Can you talk a little bit about how the SEC is structured to tackle cybersecurity and where you guys are thinking about putting priorities for enforcement?

Jorge Tenreiro: Sure, thank you. I will start with the usual SEC disclaimer about my remarks obviously are mine in my capacity and not necessarily reflecting the views of the staff, commissioners or the commission certainly.

I think as you alluded to, the SEC has been active on cyber issues for a while. In 2011, our Division of Corporation Finance issued staff guidance to help public companies on issues to be considered in addressing cyber issues and their disclosures and what cyber-related incidents or issues to disclose in periodic filings including in the event of breaches.

In 2018, the Commission itself issued additional cyber guidance for public companies to provide, I guess from my perspective, further granularity and reiterating the obligation of public companies to share material information about cyber incidents with investors. And then as you just mentioned, in this past July, the commission adopted a new rule for public issuers, public company issuers regarding cyber.

I would say that each level of guidance and then the rule have built on what came before. But in terms of how the SEC is structured, I think it's fair to say there's a number of different parts of groups or offices of the SEC that tackle cybersecurity-related concerns and disclosures. Most prominent in my mind are I think the Division of Corporation Finance, the Division of Exams and, in some instances, also the Division of Enforcement wherever.

To take a step back, I think the SEC has approached cyber through essentially two separate channels, one is what I think about as the registrant community and the other is public companies, which is what you're talking about in the new rule. Just very briefly on registrants such as broker dealers, registered investment advisors, other SEC-registered intermediaries, there's been for a while now a variety of rules that apply to how they maintain, secure, and dispose of customer sensitive information.

The Division of Examinations performs periodic exams and other reviews of these policies and procedures and implementation to ensure compliance with those rules. That's a part of the SEC that deals with those issues.

Now for public companies, I think the SEC is committed to ensuring that investors have access to material information to which they are entitled so they can make informed investment decisions and consider cyber-related risks that may impact their returns. The Division of Corporation Finance reviews public filings and engages with filers. And I think as people in that division have recently stated publicly and have always stated as interpretive questions arise, I think the division does have a long-standing open door policy and they want to encourage you to talk to staff about questions you may have.

Finally, perhaps some people's least favorite division is the Division of Enforcement, the one you least want to hear about. I can't blame you necessarily. Obviously we're authorized to investigate violations by registrants and public companies and with commission authorization, we can bring enforcement actions to re-identify violations.

Slightly different than from what my colleagues have been talking about, our focus there is on disclosure and of course we're mindful of punishing a company that has suffered a breach that has in some ways been a victim in the ways that they've described. But our focus is on public companies and to make sure that the breach doesn't create additional victims essentially because the company failed to provide investors with material information.

In terms of our priorities, I think the new rule is interesting and a priority. It's new, so sometimes it takes a while for that to percolate its way to the enforcement division. But I think it's fair to say that's something that enforcement people are keeping an eye on. We'll talk a little bit more about the rule I think later in the program, but generally speaking, just for the purposes of this question, the rule includes periodic violence, cyber governance and risk and disclosure within four days after materiality determination following the cyber event. A priority for the division, I think remains for that registrant bucket that I talked about, ensuring that they comply with the regulations that apply to them about protecting customer data.

Ms. George: Thank you. I want to talk about my nightmare, which is Solarwinds and it brings all of you guys together. For those of you who are not familiar with Solarwinds, it is a security company that experienced what I describe as the most exquisite hack that I think I'm aware of that's been public, by Russia. The targets were its clients, which included the United States Government. After having gone through what was a disaster of an experience, they are now in a situation where their CISO has been charged with fraud by the SEC and that the company has been charged with failure for issuing property disclosures around its cybersecurity risks. This is from moment of threat vector to end regulatory situation, like the worst scenario I think for a company.

Sean, I want to start with you and talk about how this was not a typical hack that I think people think of where you think, "This group is coming in and they want to steal data so they can sell it or they want a ransomware or something, or they want my data." This was a group that came in and said, "You are my access, my key into possibly 18,000 different customers." Talk a little bit about what happened here from what you can talk about in the unclassed situation, maybe it's all unclassed today. What Russia did, why they targeted Solarwinds and why it was such an effective hack.

Mr. Newell: I probably should have mentioned this type of hack, which we refer to as a supply chain attack in my what-keeps-me-up-at-night message because it does just resonate for many months and many years after the initial hack.

What happened was Solarwinds, a software company based in Texas, they had a piece of software called Orion, which helped cybersecurity network defenders monitor their network. What happened was the members of the Foreign Intelligence Service of the Russian Federation, they're known as SVR, one of the successors to the KGB, figured out, because they're very smart and very sophisticated, they figured out that Solarwinds provides the software to its customers, periodically updates that software for its customers. They are, as you mentioned, the door into many different places we want to go through for our intelligence gathering purposes. They targeted Solarwinds, they gained access to Solarwinds. This was in October. This is all public information that I'm telling you, it's information that's been acknowledged by the company, it's not classified or information the company provided to us during the course of the investigation.

But in October, 2019, they gained access to the network. They laid low, they slowly moved

Cybersecurity ➔

Cybersecurity

continued

laterally through the network to the production environment, they gained access to the production environment for the software and they watched how the company updated the software and pushed out the updates. At a certain point in time, between October 2019 and March 2023, they inserted their own code into that software, which provided them a backdoor to any system in which that software was loaded.

So March 2023 comes around and the company comes to its normal cycle, updates the software, pushes it out, not realizing that at the time of that update the SVR had gotten in and put a backdoor into it. All the customers of Solarwinds that updated their software March 2023 had a backdoor.

Now this is thousands, if not tens of thousands of customers around the world. But what the SVR did after that was they looked at who they then had access to and went in a very targeted manner to U.S. government agencies, foreign governments, and then a lot of private sector entities. They were using this backdoor to get in the systems and go for the data that was of interest to the Russian government.

That was in March. It wasn't until December 2020 when they went after a company called FireEye, which, for those of you who aren't familiar with it, is an incident response company, and a very sophisticated one. I think we're all fortunate that they went after FireEye because who better to discover a network intrusion by a very sophisticated adversary than a company that makes its living by discovering network intrusions by very sophisticated adversaries?

Luckily for us, FireEye noticed something was up, started digging into it and actually discovered that there was this vulnerability and sounded the alarm. From then on, the U.S. government popped into action, we initiated investigations, DHS was very involved in getting out information about the hack and getting out information to federal government, civilian enterprise saying, "Here's where you got to look for, here's the patches," things along those lines.

It was very devastating. DOJ in particular, and yours truly, we had our emails stolen. A funny fact that doesn't get much attention though, it was not just Solarwinds. Solarwinds allowed them into DOJ's network. They actually then took advantage of a flaw in Microsoft software to move laterally within DOJ. They're this very sophisticated actor, two previously unknown vulnerabilities that they were taking advantage of to go after DOJ specifically and others and they gathered all this information. Discovered, remediated, we worked very closely with Solarwinds throughout our investigation and we continue to do so. They were very, very open to law enforcement, shared lots of information with us, provided witnesses. I think that it was a very bad day for them and for the U.S. government and for a lot of other companies in December when this all came to light.

Ms. George: Right around Christmas.

Mr. Newell: Right around Christmas as these things tend to happen.

Ms. George: I was just trying to remember what ruined my Christmas that year. That was this. Spencer, this was a terrible moment for the United States Government. I think like a proof of concept for CISA. How did you guys react? What were the lessons learned as a victim in the government? And then what were the practices that you think that the government actually nailed this time that companies should be thinking about when they have a similar situation?

Mr. Fisher: Great question. Thank you. I share your pain. First of all, I was not at CISA. I've only been at CISA for a year. I was at the White House working at the National Security Council and got a call, I think the day before Christmas to come in and discuss something. I definitely understand the impact on Christmas that year, in December 2020.

In the immediate aftermath of the Solarwinds campaign, CISA, as Sean alluded to, DHS, CISA worked with the government, private sector and international partners sharing information and resources. Since then, CISA has addressed many of the lessons learned and implemented changes, recommended or authorized through things like the Biden Administration's Cybersecurity Executive Order. The NDAA has touched on this as well, the National Defense Authorization Act, the Cybersecurity Strategy, the CSAC Cybersecurity Advisory Council, I know I'm just throwing acronyms at you all. But that's what we do from the government.

These are all things that I think have been informed over the last three years by the Solarwinds hack. Using those authorities, and I come at this from the legal perspective, so we're using those authorities, working with our clients within the ambit of those authorities. We've made some strides in cybersecurity across both

federal and critical infrastructure networks. I'll just talk a little bit about that because it goes to CISA's mission.

CISA's mission includes, I talked about critical infrastructure earlier. CISA's mission includes defending the FCEB, I'm throwing another one at you guys, the Federal Civilian Executive Branch Network, which is the largest computer network in the world. For federal networks, we've stood up a federal dashboard that provides granular data in the cybersecurity risk across civilian agencies. We've deployed endpoint detection and response capabilities across thousands of hosts and gained unprecedented visibility. And we've also deployed new shared services, so protective DNS to prevent intrusions at scale. We've issued numerous binding operational directives, which my staff works with our clients on, that have transformed how agencies prioritize vulnerabilities and set requirements for agencies to report information on assets and vulnerabilities to CISA. Big part of our work is this cyber defense mission.

Across critical infrastructures, broadening out from the federal government, we've published cyber performance goals. This is a voluntary baseline framework. You can think about it along the same lines as the NIST framework (National Institute of Science and Technology, OMB Guidance, FISMA (Federal Information Security Modernization Act) to establish a baseline of cybersecurity practices across sectors. We've expanded our cyber sentry program to nearly 20 of the nation's most critical entities. We've established a novel model of persistent collaboration that brings public and private sector partners together through the Joint Cyber Defense Collaborative JCDC. Most of critical infrastructure sits in the private sector. CISA works very diligently and very hard at forming those partnerships between—and I know this has become a little bit of a cliché—but the public-private partnership is vital to our mission. It's something we place a lot of priority on.

We drive collaborative efforts to drive down cyber risks to the nation's critical infrastructure. That requires identifying what the risks are, information sharing, conducting risk and vulnerability assessments, deploying threat detection, so threat-hunt capabilities, and leveraging our capacity to assist the private sector.

Our hope is that we're helping agencies as the nation's Cyber Defense Agency to prevent and respond to cyber attacks. In the wake of Solarwinds, we're offering assistance to victim organizations, using information from incident reports to protect other possible victims. When those things are reported and reported quickly, they can contribute to stopping attacks and cyber incidents that are underway.

As we look ahead, my hope is that CISA working with our inter-agency partners, will be able to look back and see that our nation companies and people have worked together to learn and form a collective ability to respond and recover to things like Solarwinds and work towards resilience. It really is, and I know I'll throw another cliché, but it really is a whole of nation, whole of government effort to keep us safe. Thank you.

Ms. George: Jorge, I know that we have limited time with you. How many minutes do I have left?

Mr. Tenreiro: I could probably stick another 15. Thank you. Sorry.

Ms. George: Got it. I got it. I'm good. Thank you. Solarwinds is probably the biggest enforcement action I think the private sector has seen from the SEC. I'm going to talk a little bit about it because I know that you can't, and then I'll let you talk more generally.

Solarwinds had 18,000 customers. If you were a customer of Solarwinds sometime in like say February, March, April, you got a letter from the SEC saying, "You are a user of Solarwinds. Solarwinds told us that you were a customer. Did you have this software in place? Have you been breached? And so forth. Have you assessed materiality of this incident? Did you disclose it? If you didn't disclose, then why?" We saw this in law firms because it was not one client, it was like 20 clients, 30 clients, 40 clients, getting these letters from the SEC. We thought, "Well, SEC is really taking this quite seriously." This all culminates in, I think maybe a couple of months ago, the SEC files charges against the CISO. This is the first time we've seen a CISO [Chief Information Security Officer] held accountable by the SEC around disclosures.

Two things that really came out in the complaint. One is that the CISO was putting out marketing materials touting Solarwinds cybersecurity, while at the same time having received tons of emails that I think most CISOs received that say things like, "Our security is crap. We have a massive amount of cybersecurity debt. This place is a steaming pile of..." You know. And the disclosures from Solarwinds probably reads like almost every other company's disclosures. "We could be subject to a cyber attack. We have this

Cybersecurity ➔

Cybersecurity

continued

kind of material and we have that kind of material and that in the event that we had an incident, it could be problematic for our company in a myriad of ways."

The CISO and the company have been charged, interestingly to all of us on the outside, not other executives, both for fraud and for controls, failures around disclosures. I know that, Jorge, you cannot talk about this case, which is devastating to me, but let's talk about the hypothetical situation of CISOs and companies out there that are looking at this complaint from the SEC, which is definitely the most aggressive posture we have seen towards a victim company, I think. Maybe to the exclusion of the FTC, maybe the FTC has played this tough as well. What lessons should companies be taking from this action from the SEC in terms of the expectations today of what they should be talking about when they're talking about cybersecurity. Every company I know has a massive amount of cybersecurity debt. How much do they need to be putting that out there in their disclosures? From your regulatory perspective, what are you guys expecting?

Mr. Tenreiro: You're right, I can't talk about Solarwinds. It's an active litigation. Sorry, maybe one day, but taking a step back, just several degrees to address the question without referencing any particular matter, I think obviously we know that the issue of personal liability has garnered a lot of attention. Look, we look at the facts and circumstances. I know that's not very satisfactory. But I think we don't look at titles, we look at what did the person know or should have known in their position, what did they do or did not do, and how does that measure up to statutes and the law, really the rules and regulations? I think generally speaking, and I think higher ranking people and enforcement have said it if you are operating in good faith and take reasonable steps, you're unlikely to hear from us.

In some ways, when I think about these issues, and people ask me, I think back on my career when I was a staff attorney and working on my own investigations, I once had a case where we sued a company, I don't want to name them to the public because I don't want to bring this up back for them, but basically they were talking about the safety of their product, and they had all these reports that said, "These products are not safe." It does remind me of that situation where you're eternally getting very specific information that something is wrong, and then outwardly you're saying, "Oh, nothing's wrong." Or you're giving these, what I think you described as boilerplate disclosures. Cases, situations like that have always been troubling for the SEC. I don't think it's necessarily new in this context, although I presume that all of those notices that we sent out made some of the law firm people very busy.

But going back to the CISOs question because I don't want to completely skirt answering, I think there's three sets of things that they and others in similar positions can do to advance our entities preparedness and improve outcomes in that process. I think we think about maybe education, engagement, and execution. Educate people about the meaning of the rules and what the expectations are. Engage with the stakeholders in the company and impacted groups internally to understand business units, sources of risk, opportunity, where we are, where you are in achieving compliance with what you've said publicly. And then execute. Make sure that the company's good plans and policies and procedures are implemented effectively and consistently. I think as I alluded to with my example, if someone was aware of red flags or purposely ignored them, how did the person respond or fail to respond, or how did those actions or awareness implicate internal controls or disclosures? Those are the questions that we're going to be asking.

I think you asked a hypothetical about someone who's maybe talking internally and maybe they're not getting the response that they want. That's a serious issue. We have had public enforcement actions where in the charging documents, we've mentioned that there were breakdowns in communications, maybe not necessarily that somebody was being ignored on purpose, which sounds more problematic, but there were breakdowns in policies and procedures on disclosure, making sure the information from here gets up to here.

I don't know if you were referring to something more. I guess what I would say, again, just from my perspective for cyber security professionals if they feel like they're not being heard internally, is please continue your efforts to make sure that you are heard. Hopefully our enforcement efforts are helping to show why it is in the company's interest to listen and keep those internal lines open and effective. I don't know if you're referring to a more extreme situation of someone raising an alarm, or blowing a whistle and not being heard. I mean, obviously that

veers into other territory, but I think that's what the expectations are, and they're not necessarily that different than what you see in other contexts despite obviously the interest in cyber is great and I understand that.

Ms. George: I think that's helpful. I think that from the CISO community, there was a massive allergic reaction to this enforcement proceeding in part because I think CISOs have long felt like their head has always been on the chopping block. If I can just make it through this job for two years, but if we have a breach, I'm definitely going to be the person who gets fired. I think there's a massive amount of risk that they are having to deal with. And I think even when you're talking about the United States Government, it was also subject to this hack. It was a very impressive company that was actually able to detect it. Putting this pressure on CISOs, I think it's going to be a whole new level of education to understand what their roles are in terms of public companies and disclosures. For this crowd, when you're acquiring another company and you're looking at what's internal to them, I think that most targets of acquisitions tend to have weaker cybersecurity standards than the parent company ends up having.

While we're with you, I want to talk a little bit about the recent SEC rule requiring companies to issue a 8-Ks within four days of determining a cybersecurity incident is material. I'm going to give an anecdote from my time in the Obama Administration, there was a period of time where there were major Iranian-based attacks on banks leading up to the Iran deal, trying to put pressure on the United States government and the banks, mostly New York-based banks were proxies for that pressure and there were large number of DDoS attacks. I don't remember how many people in this room remember this, it was 2015, 2016.

I remember this very distinctly because we were in a meeting at the Treasury Department and the bank officials were pushing on the United States Government to do something about these DDoS attacks, in part because the banks were saying, "We're spending 20 million, 30 million, 40 million, 50 million dollars a month to divert these attacks away from us." And this is about your foreign policy and this is a foreign state and you should be protecting us. I remember a Treasury official asked one bank official, "Well, if it's $15 million a month, are you disclosing it in your securities filings?" And they said, "No, it's not material." Which at the time, as a lowly paid government official, I thought, "That's insane." Now I'm sitting in Silicon Valley and I'm like, "This is probably right."

But to put this in context, we have this 8-K, four days, you must disclose this materiality. What I have seen from my little foxhole proofreading people's 8-Ks coming up is that a lot of companies are disclosing that they have incidents, but are also putting in this caveat saying "But it's not material or we haven't determined it's material yet." This belies the question of why are we disclosing it in the first place, but for it to meet this rule. But if you're disclosing it and you're still saying it's not material, did you really meet the rules? I think that companies are still really struggling with how to attack these particular new rules around disclosures.

Jorge, I have two questions for you around this. One, have you found it surprising the number of disclosures that are happening that are saying, "We had this incident, may have involved a nation state, we haven't determined it's material, or we don't think it's material"? And then second, you're a company, you've put out this 8-K, you've said it's not material. What should you expect from the SEC?

Mr. Tenreiro: Just because I'm running a little short of time, I apologize, just to level set the rule for those, I think everyone is aware, but basically in July '23, the commissioner adopted rules that now require public companies to disclose material cybersecurity incidents and material information regarding their cybersecurity risk management. I'm being very general here in the interest of time.

Now, I think the SEC found that companies already provide this information, but on different timelines, in a different levels of detail, in different sections, and so on. The heart of the idea was that investors need more timely and consistent cybersecurity disclosures to make informed investment decisions. That I think was the SEC's stated goal, I think, of adopting the rule, or one of the stated goals.

As you noted, the core is that registrants, public companies rather, must determine whether is material without a reasonable delay and then four days to make a filing about that determination in Item 105 of Form 8-K. And then you have some requirements of what we're supposed to disclose and describe, etc.

Am I surprised that people are filing the item saying, "We have this, but it's not material"? I guess yes and no is my answer, but as you alluded to, this is pretty new and it's developing. I think I'm just going to leave it at that for now

Cybersecurity ➔

Cybersecurity

continued

because it is something that as the companies are working through it, I think it's fair to infer that the SEC's going to be looking and thinking about that, as you do. I mean these are iterative processes in some ways.

And then in more general terms, should the companies expect the SEC review filing? I mean, as I mentioned in my first question, the Division of Corporation Finance reviews filings, and you can expect that that's probably what they're doing.

In terms of the Division of Enforcement, we enforce the rules. It's actually in another big part of the work that I do in my unit, which I'm very glad you have not asked me about because I welcome one day not talking about crypto, but you hear regulation by enforcement is something I hear. It's interesting to me when I hear that because we have regulations, we have to enforce them, we have these rules, companies, clearly, they're figuring out the rules and they're going to want to comply. I think it's fair to infer generally at a very general level that the Division of Enforcement looks at the rules that we have that we have to enforce. Eventually, I think it's fair to—again I'm not going to talk about anything in particular, but it's something that the division will look at or is probably generally looking at. I'm just going to leave it at that level of generality, but I think companies should expect with every public filing that the SEC is looking at the public filings.

Ms. George: Thank you, Jorge. And I know you might have to pop off real fast, so thank you and I appreciate you joining us today. I'm sorry you're running a little late.

Mr. Tenreiro: Thank you for having me.

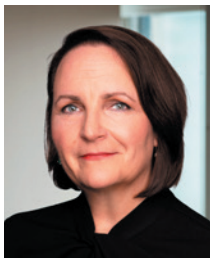
Ms. George: Sean, one of the pieces of the rules that came out, I remember the proposed rule came out and it said, "You have four days within which to determine whether there is material that requires this disclosure." I, as well as many other law firms commented, "You're putting these companies in a terrible situation because particularly when it's a nation state actor, you may not want to publicly acknowledge that they're on your system, but you may know it's a material incident. Now you're going to have to disclose that there's a nation state actor, for example, on your system tipping them off that you know they're there merely because you've got to meet this SEC requirement". The SEC came in and in its amended final rule said, "Well, if you find yourself in this situation, you can go to the Attorney General and ask for a delay from making this SEC disclosure." How many calls have you gotten?

Mr. Newell: That's right. The delay is if the Attorney General determines there's substantial risk to national security or public safety, by the disclosure, not the incident. The incident is not at issue, it's the disclosure that must pose that risk. So I think a lot of times the SEC would tell the companies, you don't have to put all that nitty-gritty stuff in there that would harm national security, public safety. But nonetheless, that did make it up in the final rule. To date in the four months, five months maybe that we've had this rule in place, we've had zero requests to delay disclosure, which is interesting given how many law firms commented, this is absolutely necessary in order to protect national security. But we're ready. When that first one comes in, we have a team of lawyers ready to pounce [*laughter*].

Ms. George: All right. Well, we're at the top of the hour. Thank you both for joining us today, and thank you all for having us.

~~MA~~

Coping with Leaks



Sheila Ennis
Managing Director and
Head of Investor Relations
at H/Advisors Abernathy

It's contagious and the epidemic is spreading. The latest available figures show that seventy percent of the 20 largest U.S. deals in the first half of 2024 were hit by leaks to the media. One might respond by saying "So what?" But that would be naïve. A leak can be as damaging as a drone strike, causing painful complications for transactions not yet ready for prime time.

"A leak can cement public perception about a deal before the parties have the opportunity to communicate its rationale or structure," says Sheila Ennis, managing director and Head of Investor Relations at H-Advisor Abernathy, a communications advisor to CEOs, board members, and executives on shareholder communications and engagement. "This can delay or derail deal negotiations, stoke employee or regulator concern, and may cause lasting reputational impact if a deal is not ultimately reached."

Ms. Ennis and her team realized that leaks were becoming ever more common. "We were seeing a steady increase in leaks and wanted to be sure our clients were ready to manage through them. The leak strategy is now the first document we develop for our clients," she says. "Every situation is different so it's crucial to map the moments where the universe of awareness is likely to widen, or motivations change. What's more, being prepared to react within the same news cycle is imperative."

Here are what the firm calls the "essential steps for dealmakers to navigate M&S leak scenarios:

- Get a plan on the shelf… early. Outline potential scenarios for public speculation and align on a rapid response strategy.

- Ensure active dialogue and close collaboration among the deal team. Media inquiries may not come directly to the client, but to advisors.

- Anticipate moments where the universe of awareness widens. Are new parties being engaged? Have certain bidders been informed of a decision to move forward without them?

- Evaluate announcement timing. Stakeholder engagement within in the same news cycle of the leak is essential. Can we accelerate planned timing of the transaction announcement? Do we need to position reporting as "early stages"?

- Understand your regulatory and disclosure requirements. Disclosure requirements in a transaction leak scenario vary greatly if you are subject to regulations of the United States, United Kingdom or Hong Kong, for example. Legal obligations may affect the response strategy to a leak.

- Consider accuracy of the planned reporting. Is valuation or stages of negotiation way inaccurate? Is there an opportunity to course correct and limit problematic/inaccurate details

There are important questions to address in the plan. First, philosophical differences can emerge as the parties put together the plan, all of which should be resolved before a leak hits. This way, the basic approach has been crafted before there is an actual leak. Ms. Ennis and her team help the company identify the members of a working group that can be convened quickly to

Leaks ➔

Leaks

continued

determine whether and/or how to respond just as soon as there is word of a leak.

There are myriad ways by which companies can learn about a leak. A reporter might contact the parties directly or approach advisors working with the company. The first question is often whether or not the company should respond at all, and if it decides that is best, Ms. Ennis says that she and the team remind clients to be sure their employees know who is responsible for responding to " inbounds from the media."

How much does the reporter know? Is the journalist merely fishing ? "We assess the accuracy and level of detail that the reporter has already developed," Ms. Ennis says, "and then we assess the maturity of the negotiations. Movement in the stock price is one key driver of the client's next move. Internal chatter is another. Often, it is best to ignore the inbounds and stick to the negotiations, but not always. Each situation is different."

Leaks have become so ubiquitous that definitive merger agreement announcements now tend to account for the effect of a leak on the calculation of the premium compared to the unaffected stock price. "This can sometimes involve two or three calculations," explains Ms. Ennis. "The premium over the price at the last close of trading is the easiest methodology, but may be misleading if speculation has moved the target's stock price significantly. In these cases we will often include either the premium over the 60-day volume-weighted average price or the premium relative to the trading price on a specific day prior to speculation about the transaction.

~~MA~~

1Q 2024 M&A Leak Trends

H/ADVISORS Abernathy

Target Industry	Target	Acquirer	Deal Value	Leak Outlet	Time to Announce
Financial Services	DISCOVER	Capital One	$35.3B	Bloomberg	Same day
Technology	Ansys	synopsys	$33.6B	Bloomberg	11 days
Healthcare	Catalent	novo holdings	$17.3B	Reuters	5 months
Technology	juniper	Hewlett Packard Enterprise	$14.3B	WSJ	1 day
Energy	equitrans	EQT	$13.9B	Bloomberg	3 months
Energy	SWN	CHESAPEAKE	$11.7B	WSJ	6 days
Energy	NuStar	SUNOCO	$6.6B	Transaction did not leak	N/A
Technology	Altium	RENESAS	$5.9B	Transaction did not leak	N/A
Real Estate	MDC	SEKISUI HOUSE	$5.1B	Transaction did not leak	N/A
Healthcare	CYMABAY	GILEAD	$4.5B	Transaction did not leak	N/A
Energy	CALLON	APA Corporation	$4.3B	Bloomberg	20 days
Healthcare	Axonics	Boston Scientific	$3.7B	Transaction did not leak	N/A
Business Services	McGRATH	WILLSCOT | mobile mini	$3.7B	WSJ	1 day
Material Services	PGT	MIWD	$3.2B	Reuters	3 months
Technology	Sterling	First Advantage	$2.5B	Transaction did not leak	N/A
Healthcare	INHIBRX	sanofi	$2.4B	Transaction did not leak	N/A
Technology	VIZIO	Walmart	$2.3B	WSJ	7 days
Healthcare	AMBRX	Johnson&Johnson	$2.1B	Transaction did not leak	N/A
Aerospace and Defense	KAMAN	ARCLINE	$2.0B	Transaction did not leak	N/A
Technology	Severbridge	THOMABRAVO	$1.8B	Transaction did not leak	N/A

*Includes full-stake transactions of U.S. public companies

50% of the 20 largest U.S. transactions leaked

2Q 2024 M&A Leak Trends

H/ADVISORS Abernathy

Target Industry	Target	Acquirer	Deal Value	Leak Outlet	Time to Announce
Energy	Marathon Oil	ConocoPhillips	$23.1B	FT	Same day
Healthcare	SHOCKWAVE	Johnson & Johnson	$14.8B	WSJ	10 days
Real Estate	AIR	Blackstone	$9.4B	Transaction did not leak	N/A
Energy	CHAMPIONX	Schlumberger	$8.3B	Transaction did not leak	N/A
Material Services	Stericycle	WM	$8.1B	Bloomberg	10 days
Energy	Atlantica Yield	ECP	$7.7B	Bloomberg	26 days
Technology	HashiCorp	IBM	$7.7B	Bloomberg	1 month
Technology	SQUARESPACE	PERMIRA / GENERAL ATLANTIC	$7.0B	Transaction did not leak	N/A
Energy	ALLETE	GIP / CPP Investments	$5.8B	Reuters	5 months
Technology	PowerSchool	BainCapital	$5.6B	WSJ	1 month
Healthcare		VERTEX	$4.9B	Bloomberg	Same day
Material Services	ENCORE WIRE	Prysmian Group	$4.7B	Transaction did not leak	N/A
Utility	PRIMO	BLUETRITON	$4.7B	Transaction did not leak	N/A
Business Services	PERFICIENT	GIC	$2.9B	Bloomberg	5 days
Financial Services	ASSETMARK	GTCR	$2.7B	Bloomberg	4 months
Healthcare	deciphera	ONO PHARMA	$2.4B	Transaction did not leak	N/A
Energy		NOBLE	$2.3B	Transaction did not leak	N/A
Energy	SilverBow	Crescent Energy	$2.3B	Bloomberg	Same day
Technology	Matterport	CoStar Group	$2.2B	Transaction did not leak	N/A
Financial Services	Heartland	UMB	$2.0B	Bloomberg	3 days

*Includes full-stake transactions of U.S. public companies

60% of the 20 largest U.S. transactions leaked

1H 2024 M&A Leak Trends

H/ADVISORS Abernathy

Target Industry	Target	Acquirer	Deal Value	Leak Outlet	Time to Announce
Financial Services	DISCOVER	Capital One	$35.3B	Bloomberg	Same day
Technology	Ansys	SYNOPSYS	$33.6B	Bloomberg	11 days
Energy	Marathon Oil	ConocoPhillips	$23.1B	FT	Same day
Healthcare	Catalent	novo holdings	$17.3B	Reuters	5 months
Healthcare	SHOCKWAVE	Johnson & Johnson	$14.8B	WSJ	10 days
Technology	juniper	Hewlett Packard Enterprise	$14.3B	WSJ	1 day
Energy	equitrans	EQT	$13.9B	Bloomberg	3 months
Energy	SWN	CHESAPEAKE	$11.7B	WSJ	6 days
Real Estate	AIR	Blackstone	$9.4B	Transaction did not leak	N/A
Energy	CHAMPIONX	Schlumberger	$8.3B	Transaction did not leak	N/A
Material Services	Stericycle	WM	$9.4B	Bloomberg	10 days
Energy	Atlantica Yield	ECP	$7.7B	Bloomberg	26 days
Technology	HashiCorp	IBM	$7.7B	Bloomberg	1 month
Technology	SQUARESPACE	PERMIRA / GENERAL ATLANTIC	$7.0B	Transaction did not leak	N/A
Energy	NuStar	SUNOCO	$6.6B	Transaction did not leak	N/A
Technology	Altium	RENESAS	$5.9B	Transaction did not leak	N/A
Energy	ALLETE	GIP / CPP Investments	$5.8B	Reuters	5 months
Technology	PowerSchool	BainCapital	$5.6B	WSJ	1 month
Real Estate	MDC	SEKISUI HOUSE	$5.1B	Transaction did not leak	N/A
Healthcare		VERTEX	$4.9B	Bloomberg	Same day

*Includes full-stake transactions of U.S. public companies

70% of the 20 largest U.S. transactions leaked

Website: www.themandajournal.com

E-mail: info@themandajournal.com

Editorial Office: 215-309-5724

Orders & Subscriptions: For individual subscriptions, discounted multi-copy institutional subscription rates, or additional copies, please call 215-309-5724 or fax 215-309-5724.

THE M&A JOURNAL
the independent report on deals and dealmakers

Editor/Publisher **John Close**
Design and Production **John Boudreau**
Senior Writers **Gay Jervey, R. L. Weiner**
Writing/Research **Frank Coffee, Jeff Gurner, Terry Lefton**
Circulation **Dan Matisa**
Web Production **John Boudreau**

The M&A Journal, 1008 Spruce Street, Suite 2R, Philadelphia, PA 19107