MERGERMARKET

SHEARMAN & STERLING LLP

SAFE SECRETS

DEALING WITH DATA PRIVACY ISSUES IN M&A

PARTICIPANTS:

JS **Jeewon Serrato, Co-head of Privacy and Data Protection, Shearman & Sterling**
Jeewon is counsel and co-head of the Global Privacy and Data Protection Group where she advises companies on privacy, cybersecurity, data protection and crisis management issues.

JA **Jordan Altman, Partner, IP Transactions, Shearman & Sterling**
Jordan is a partner in the IP Transactions Group. He specializes in structuring, drafting and negotiating agreements that focus on the development, transfer, procurement, commercialization and maintenance of IP and technology.

AG **Al Ghous, Senior Director Cyber Security, GE Digital**
With more than 20 years' experience in cyber, information and product security, risk management and strategy, Ghous is currently responsible for the delivery of secure cloud infrastructure and platforms for GE Digital's Industrial Internet Cloud.

AP **Arun Perinkolam, Principal/Partner, Deloitte Cyber Risk Services Advisory Practice**
Perinkolam has served multiple Fortune 50 and Fortune 100 clients on initiatives from cyber risk strategy development to detailed design and deployment of enterprise and consumer-facing cyber risk solutions for more than 15 years.

QUESTION & ANSWER:

WHAT ARE SOME OF THE MOST COMMON DATA PRIVACY CONCERNS RAISED IN M&A? WHICH SECTORS POSE THE MOST COMPLEX ISSUES?

AG If we start by looking at an acquisition that involves a target with customers – one concern is IP, the other is sensitive data. If the target has customers, who may actually be competitors of the acquiring company, there are a lot of sensitivities in terms of the customer data that has to be taken into account. There have to be some controls and commitments made to the competitors put in place by the acquirer to make sure they don't jump ship and leave, therefore reducing revenues. That can be tricky to navigate. Another concern would be that the target company doesn't have appropriate data privacy controls, putting the acquiring company at risk. Or it may be the acquiring company doesn't have adequate controls that could lead to liability. For example, if you are acquiring a company that is highly regulated and they have controls in place in terms of data protection and privacy, and you as the acquiring company don't have those, in order to integrate that company you have to reduce their level of security. That creates some liability and risk for the target company. All of these have to be accounted for, ahead of time, so that there's no added risk on either side during the integration process.

When it comes to looking at sectors, having been in multiple industries, I would say probably healthcare, because in the US you have HIPAA regulations and that's critical if you're acquiring

a company that has healthcare customers. There are certain things that you need to do in order to become compliant and be able to store and process protected health information. And it's the same thing, more or less, for the financial sector and the government sector.

AP When gauging the security and data privacy capabilities of an intended target, acquirers want to have some level of understanding of the security program they are inheriting. They want to know what specific data privacy, security and compliance risks they're going to take on – not just from an enterprise perspective, but also from new third parties and vendors involved. Another very important point is compliance – if the acquirer has very specific security & privacy regulatory and industry directives, like the PCI DSS payment card industry standard as an example, the acquisition of a target can potentially impair the acquirer's compliance posture. Lastly, acquirers need to assess how quickly they can integrate the target acquisition into the business without really impairing or compromising security measures. If the target handles a lot of consumer data, things like consumer choice, consent and breach notification will be of immediate interest. If there are serious issues unearthed during diligence, there will likely be a need to remediate before the deal closes.

Looking at various industries when it comes to data privacy, security risk, and compliance, most sectors have some level of complexity and specific requirements. For example, the financial services sector is highly regulated. Top of mind is making sure that any target does not compromise the acquirer's regulatory directives and compliance posture. In the healthcare sector there have been a spate of recent cyberattacks as it relates to ransomware, as an example. That will be a focus for acquirers in that sector, ensuring they are not taking on any vulnerabilities that would open them up for an attack. Then, looking at the technology sector, intellectual property (IP) protection is always top of mind.

JS There are two things in terms of the more recent changes that I see in the M&A due diligence stage. The first one is in data transfer restrictions. There are over 170 different countries that have passed data privacy laws that have some kind of restrictions on what kind of data can be transferred out of that country and also how that data may be used. Further, there are some countries like the European Union countries that have restrictions on certain agreements that need to be in place before that data can be transferred. What that means is that, in the scenario where an M&A transaction has been contemplated, even before such a deal has been finalized, certain data needs to be transferred between the buyer and seller and those transfer restrictions need to be considered early on in this phase. Sometimes that means that in addition to antitrust, tax, or any other company risk considerations that might come into play in M&A due diligence, data privacy could be right up there. Second, is that some of these countries that have data privacy restrictions also have containment policies that say data needs to be processed within the country. So if you are targeting data in a country with a law specifying that their citizens' data cannot be processed outside of the country, that could cause some trouble if the customer data is part of the asset being acquired. So the data containment and the data transfer restrictions are the two biggest challenges I see the most.

JA The most common data privacy concerns are data security, disaster recovery, business continuity and compliance with applicable data privacy laws. A purchaser is going to want to know whether the target has privacy policies and procedures that it makes its employees and its vendors follow. It also wants to know whether the target has security measures implemented to secure its data and that the target regularly self-tests those security measures for vulnerability. A purchaser will want to confirm that the target has a plan for disaster recovery and business continuity in some event of an outage, and that the target has its data backed up somewhere where it can be recovered quickly to resume business. Lastly, the acquirer wants to know that the target's data handling is compliant with applicable law. In terms of sectors, any sectors that have separate federal regulations are typically the most complex. Not only do targets in those sectors need to safeguard their customers' data to avoid losing business and customers, but they also have to be mindful that their handling of that data adheres to federal governing law. Sectors that fall into this category include financial services and healthcare.

AT WHAT STAGE IN M&A DUE DILIGENCE SHOULD DATA PRIVACY ISSUES ENTER THE DISCUSSION? WHAT QUESTIONS SHOULD THE ACQUIRER BE FOCUSED ON? HOW MUCH INFORMATION SHOULD THE TARGET BE PREPARED TO PROVIDE?

AG In general, regulations and data privacy implications should be discussed in the screening phase – just so they're prepared in case they come across a company that is highly regulated and data privacy is going to be of the

> "The most common data privacy concerns are data security, disaster recovery, business continuity and compliance with applicable data privacy laws."
>
> Jordan Altman, Partner, IP Transactions, Shearman &Sterling

utmost concern. Then they can discuss a plan for how to navigate through that. The actual discussions with the target company should happen immediately because there's a lot of implications downstream in terms of what steps both sides need to take to ensure that they maintain integrity from a data privacy perspective. These discussions should focus on the type of data, how they're classified, and the context, because different levels of classification can mean different things for different organizations. Parties should discuss the data custodians if they have third-parties that are working on their behalf, and how the data is regulated – is it in scope for HIPAA or is it in scope for EU data privacy law and things of that nature. As an acquirer, you want to get as much information as you possibly can from a target to make decisions that help with putting proper valuation on the target company. It also helps you to understand what you might need to do if that target company has customers. Often certain customers contractually require a certain level of data protection and you don't want to violate those.

AP Security and data privacy discussions need to start at the due diligence phase and continue through transaction execution and integration. The due diligence phase will help garner what some of the key data privacy-related risks are and whether there are any deal-breakers or risks to be remediated before closing the deal. There may also be significant issues an acquirer might want to get a handle on that would drive deal value up or down. Once you get into the transaction execution phase, it is really about remediating some of those high-priority, critical gaps before you can close the deal. As soon as a deal is public, the target gains a bullseye and takes on the same risk profile as the acquirer, so you want to be ahead of that curve.

I really feel that going through a cyber due diligence exercise benefits the target as much as the acquirer. A lot of acquisition targets haven't been through a proper cyber risk assessment; and cybersecurity due diligence gives both targets and potential acquirers a chance to assess true security posture. And most importantly, it helps expedite integration by outlining a clear-cut approach that factors in capability synergies between the acquirer and the target.

JS The sooner the buyer starts thinking about whether the data is part of the value that should be considered, the sooner they can evaluate if there are any risks associated with the transfer of that data. In order to really assess where all that data is and any restrictions that may apply, they need to do some due diligence. Even pre-merger due diligence requires certain agreements to be in place, and so the analysis of what restrictions are in place and how they go about doing it really needs to be thought through and it needs to be done in a certain way. Once the deal has completed, some of those restrictions will be lifted, as now the buyer has acquired the data, but pre-merger due diligence can be quite complicated.

JA Data privacy is relevant in every M&A deal, but it isn't expressly negotiated in every M&A deal. For example, every target business in an M&A deal has employees, and each of those target businesses collects personal information about those employees such as Social Security numbers, bank account details and data about where such employees live. The collection of customer data could be a central factor to the conduct of such target businesses. If that business does waste disposal or it raises and sells livestock, it would be normal if a business was negotiating an M&A deal with one of those companies and the words "data privacy" were not mentioned. You should get a feel during the due diligence process for the role that customer data plays in the target business. If, unlike those waste disposal and livestock business examples, you see that customer data plays an important role in how that business operates, then, assuming you're the buyer, you usually raise the issue in the context of a purchase agreement

by requesting certain representations and warranties that are focused on privacy issues. The target should be prepared to provide privacy policies; any business continuity and disaster recovery plans; any data security breaches; and they should also disclose any pending or threatening claims from third parties regarding data privacy regulations. If the government is investigating them for mishandling customer data, they should disclose that, and if they have identified a third-party hacker trying to infiltrate their system and they are pursuing a claim, they should also disclose that.

DURING NEGOTIATIONS AND DRAFTING OF AGREEMENTS, WHAT AREAS TEND TO BE THE MOST IMPORTANT? DOES THIS VARY BY JURISDICTION (BY STATE, BY COUNTRY, CROSS-BORDER)?

AG I think some of the areas to cover during the due diligence and negotiation phase would be: impact to employees and to customers; whose data privacy might be impacted and how they would be communicated to; and whether there are certain jurisdictions you have to notify. The acquirer will also need to ask itself whether it has the capabilities to delete and expunge any customer data required by the target's contracts and agreements. If one of the customers in the contract has written in their contract that if they are acquired, you must delete or expunge all data, for whatever reason, then there has to be controls and steps put in place to comply with that. A lot of companies don't think about that, but when a customer leaves, especially if you're a processor of data, you're required contractually to delete the data, and that's a fairly standard clause in every contract out there. It does vary by jurisdiction – country to country, state to state, region to region. For example, if a US company was acquiring a German company with customer data and employee data, the US company would need to take into account any country data residency requirements. All these things have to be accounted for and discussed at the screening phase. You don't want to bite off more than you can chew.

AP Typically, when we have assisted acquirers, the appropriate due diligence requirements are drafted in contractually. If an acquirer wants to do a focused cyber risk and data privacy due diligence, it is negotiated upfront. These negotiations also discuss target management buy-in, appropriate stakeholder involvement, and address what documents will need to be shared by the target. I don't necessarily feel there are any nuances by jurisdiction as it pertains to an agreement to conduct a cyber due diligence, but obviously with regards to privacy, the acquirer may have certain jurisdictional privacy requirements it cares most about depending on where each party is located.

JS The difference between jurisdictions can include the definition of personal information – so whether a certain law is applicable or not can vary in different jurisdictions. We can generalize different regional differences in how they think about these laws and how they're treated, but in the end each law has a different way of defining the scope, and the applicability of the law. Not only that, but in addition to jurisdictional differences, it can also vary across industries. So it might be that there is a different law even within the same country that deals with exponential data – for example, the financial records of a customer, like credit card information or bank account details. How it is used can also encounter different laws. If it's used for marketing purposes there can be additional laws, versus if it's used for processing transactions, for example.

JA During the stages of a transaction where the relevant agreements are still being drafted and negotiated, if you're a buyer and you're in a sector where customer data is important, you'll most certainly want to know about any data security breaches, whether successful or not, that have affected the target business and how they were resolved. You'll want to know that the target company has taken reasonable precautions to safeguard the data of its customers. I think you'll want to see that the target has implemented electronic measures such as firewalls and it has instructed its employees to follow a privacy policy with respect to the data that they receive from customers. You will also want to see the target company make a representation that it is compliant with applicable data privacy laws, including notification laws in the event of a breach. These laws can vary state by state, and in fact data privacy laws can be very different from country to country.

WHAT SHOULD COMPANIES BE DOING TO PREPARE FOR THE EU GDPR, WHICH WILL GO INTO EFFECT NEXT YEAR? HOW WILL COMPANIES BE IMPACTED BY THIS NEW REGULATION, AND WHAT ARE SOME STEPS THEY CAN TAKE NOW TO PREPARE FOR IT?

AG Any company within the scope of the new EU GDPR should leverage their in-house or outside legal counsel to fully understand the implications of the general data protection regulation that's coming up as it pertains to their business and their M&A pipeline. They should take advantage of the moratorium – the two years that they provide to implement the proper levels of controls and assess how they will be impacted in terms of an M&A pipeline and their strategy – and then revise their strategy if they have to. Companies should already be more of less compliant if they're doing business in the region. Companies are also required to appoint a data protection officer. Some smaller companies may require organizational change, so there is some impact there. If they don't comply, they're going to have fines levied against them, so they have to consider the implications, because it's going to be very expensive for them going forward not to comply. If they can't afford to put in the necessary measures, then they can't do business in that region. For many companies, EU GDPR is going to be hard to navigate, so leveraging outside expertise is a good idea.

AP The EU GDPR is a hot topic these days. Companies should think of it as replacing the former EU data protection directive. In the EU GDPR, they have harmonized a number of different data privacy principles and requirements that organizations will need to comply with. Both EU and non-EU companies that process personal information in relation to the offering of goods and services to EU data subjects – which could be both employees and customers – or that monitor EU data subject behaviors will need to comply.

> "One of the biggest challenges compared to the previous laws is that the scope of the GDPR is quite expansive. "
>
> Jeewon Serrato, Co-head of Privacy and Data Protection, Shearman & Sterling

The new EU GDPR has upgraded the former directive and includes clauses around breach notification, data security, privacy by design, and information management. Most of the clients that we are assisting with are undertaking GDPR readiness assessment efforts. This involves taking a look at all of the control objectives that the GDPR is mandating, and then from a business, technology, and organizational perspective, trying to figure out what the gaps are and coming up with a remediation plan to address identified gaps. An important principle here is to "follow the data" – make sure you have clear-cut data maps of where the data is flowing, how it is being housed, and what controls are applied around that. A number of GDPR remediation initiatives that organizations will need to undertake are not just IT focused, but it will impact an organization across several business functions including business partners and vendors.

JS One of the biggest challenges compared to the previous laws is that the scope of the GDPR is quite expansive. Organizations based outside of the EU can still be in the scope of this law, as long as the company is processing data that belongs to EU residents. Let's say there's a US organization that is processing EU residents' data, this law will apply to that US organization. The second reason that this is getting a lot of attention is that the fine can be quite significant and could be as much as 4% of the worldwide revenue of the company. This is definitely not something that companies can afford to ignore; it needs to become a part of their risk assessment. If you have assessed that you are within the scope of this law, the organization needs to be creating a data processing register, which is like a data flow map. They need to understand what kind of data is processed, where it is stored, how it stored and with whom it is shared. For example, if EU residents' customer data is being transferred to the US, and this US organization has a central processing center that uses third parties to process the data, the third party also needs to comply with the GDPR. Practically speaking, the organization

needs to not only look through their own data privacy programs to ensure they meet the requirements, but they also need to be looking at the contracts they have with third-party vendors to make sure they are also EU GDPR compliant.

JA Companies subject to the EU GDPR will generally have to spend more time and resources than companies have ever before spent in respect to data privacy matters to ensure that they are complying with this law. This is because the obligations that bind companies and the collection of customer data in the EU GDPR have been significantly expanded with more rules that are skewed to protect the data. If you're a company operating under the EU GDPR, you should ensure that you have individuals on your legal or privacy team, internal counsel, who are aware of this law. Depending on whether your company deals with the processing of personal information – the type of information that the EU mandates be protected – the GDPR even requires that companies have a data protection officer on premises that has expert knowledge in this law. It's like having a mini-regulatory unit working inside your company. The data protection officer is not beholden to your company, or your board; this officer is beholden to the data regulator in the EU. In order to prepare for this new law, you must train and hire personnel to carry out these functions, and you should do it as soon as possible.

HOW CAN THE PRIVACY-RELATED ISSUES DURING DILIGENCE INFLUENCE THE SUCCESS OF A DEAL IN TERMS OF INTEGRATION OF THE BUSINESSES?

AG I'd say for one, lack of proper data privacy or data protection controls within a target company will require a larger integration budget. Companies need to estimate what it would cost to integrate, and in doing this they need to assess what controls are already in place and how to bring the target company into compliance internally. If they don't have adequate controls, then it will obviously require a longer period of time for integration. All these due diligence measures impact the bottom line for that acquisition and need to be accounted for before agreeing to move forward with the acquisition. The second thing is, if a target doesn't have the proper controls in place in terms of data privacy and protection and it costs a lot more to bring them into compliance, then that should impact the valuation of the company. I've seen many times where not enough due diligence is done upfront and when it comes to integraton, the cost is great. If the information had been on-hand upfront the acquirer probably would not have paid as much as they did. Due diligence impacts the bottom line, it impacts budgets, it affects the financials, so I think those two things are critical.

AP As an acquirer, I would really like to know the critical data protection and security issues that need to be remediated before deal closing. If there are levers that I can use to specifically negotiate deal valuation, that's an option I would want to have. Though, the big incentive really is getting an early view of the capability synergies that both the target and the acquirer can capitalize on. In a lot of recent trend reports we see seamless integration post-close as the number-one pain point most organizations face. Engaging early in a cyber due diligence effort and coming up with a clear-cut remediation plan offers a leg up in terms of integration success, not just with IT but with the rest of the business.

JS I would say in two ways: one is to help businesses assess risk and the other to assess value. It helps the company during the pre-merger due diligence to really set itself up in terms of assessing privacy risk so that it is successful post-merger. For example, if you're acquiring customers, then you want to have certain notices and consents from the customers and potentially from the data protection authorities. And you want to make sure all of that work is done so that day one they can hit the ground running. The pre-merger work is helpful not only pre-merger in assessing whether to move forward, the value and the risk, but also post-merger so that the transition is as smooth as possible.

JA Due diligence should give you a good sense of what the target company does to protect its data and as a buyer. You should be looking at whether those measures are sufficient. If they're not, then you'll have to revise those and implement remedial measures at closing in order to address that insufficiency. If you're trying to acquire a business and integrate it into another business, you want to make sure that the measures the target business takes to protect its information are compatible with the company you hope to integrate it with. Inconsistencies in privacy policies need to be addressed. One way to address a lack of information or consistency is to have a period after closing where a seller provides transitional support with respect to data processing functions. This allows the buyer more time to integrate those data processing functions with minimal disruptions to the target.

PRIMER ON THE NEW NYDFS CYBERSECURITY REGULATION

BY JEEWON KIM SERRATO, COUNSEL AND REENA SAHNI, PARTNER AT SHEARMAN & STERLING LLP.

The New York Department of Financial Services (NYDFS) Cybersecurity Requirements for Financial Services Companies (the Final Regulation)[1] took effect on March 1, 2017. We discussed in our earlier publication the background on how the original proposal of the regulation was updated in the context of other recent developments in the financial services industry.[2] In the introductory section (§ 500.00) of the Final Regulation, the NYDFS stated that: "The financial services industry is a significant target of cybersecurity threats…Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted… Adoption of the program outlined in these regulations is a priority for New York State."

The NYDFS regulation confirms once more how cybersecurity concerns are at the top of the agenda of priorities for many state and federal regulators in the banking and financial services industry. Pursuant to the Final Regulation, certain banks, insurers and other financial services institutions holding a New York state license will be required to conduct periodic assessments of their cybersecurity risks and implement and maintain a cybersecurity program designed to address such risks.

Who is affected?

The regulation applies to any entity that holds a certificate, permit, accreditation or similar authorization under banking, insurance or financial services laws (each, a covered entity). The definition appears to be broad, especially considering that the concept of "similar authorization" may apply to service providers and/or independent contractors of covered entities operating under any relevant certificate or permit required by New York banking, insurance or financial services law.

Affiliates and extraterrestrial research

Comment letters on the Original Proposed Regulation raised concerns with respect to the extraterritorial scope – in particular with respect to the broad definition of foreign banking organizations (FBOs).

In response, the NYDFS clarified that a New York branch of a foreign bank falls within the definition of covered entity, and therefore is subject to the applicable cybersecurity requirements. In addition, the Final Regulation provides that a covered entity can satisfy the applicable cybersecurity requirements by adopting a cybersecurity program maintained by an affiliate (defined in § 500.01) provided that the affiliate's program is compliant with the applicable cybersecurity requirements introduced by the NYDFS. Therefore, under the Final Regulation, the New York branch of an FBO may comply with the newly introduced cybersecurity requirements either by:

- Establishing and maintaining its own cybersecurity program, or
- Adopting the program of the FBO itself, if it is compliant with the regulation.

Exemptions

The Final Regulation includes an exemption from some of the cybersecurity requirements for covered entities whose number of employees, revenues and assets do not exceed certain thresholds. Covered entities meeting any of the following criteria are exempted from a number of cybersecurity requirements under the Final Regulation (including the requirements to appoint a CISO, encrypt non-public information, and adopt an incident response plan):

- Fewer than 10 employees, including any independent contractors of the covered entity or its affiliates located in New York or responsible for business of the covered entity

> "The financial services industry is a significant target of cybersecurity threats …given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted."
>
> The New York Department of Financial Services

1 Available at http: http://www.dfs.ny.gov/legal/regulations/adoptions/rf23-nycrr-500_cybersecurity.pdf (23 N.Y.C.R.R. pt. 500).
2 Available at http://www.shearman.com/en/newsinsights/publications/2017/01/cybersecurity-protection-of-financial-data

- Less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the covered entity and its affiliates
- Less than $10,000,000 in year-end total assets, calculated in accordance with GAAP, including assets of all Affiliates

In addition, the limited exemption applicable to covered entities with less than $5 million in gross revenue for each of the last three fiscal years is now further expanded to include covered entities with less than $5 million in gross revenue "from its New York business operations (or its affiliates' operations)." Therefore, certain larger financial institutions with smaller New York operations may now qualify for either of these new exemptions. Each covered entity that qualifies for the exemption above is required to file a Notice of Exemption with the NYDFS.

Timeline for compliance

The regulation went into effect on March 1, 2017. Pursuant to the Final Regulation, each Covered Entity is required to establish and maintain a cybersecurity program tailored to address the certain critical cybersecurity concerns by August 28, 2017 (180 days from the effective date). This program should include the following elements, among others:

- Written cybersecurity policy (§ 500.03)
- Appointment of a chief information security officer (CISO) (§ 500.04(a)) and additional cybersecurity personnel (§ 500.10)
- Access privileges to protect non-public information (§ 500.07) Incident response plan designed to promptly respond to a cybersecurity event (§ 500.16)
- Procedures to promptly notify NYDFS of any cybersecurity events (§ 500.17)

One of the main changes from earlier proposals is that the Final Regulation allows for a more flexible and risk-based approach. Compared to the Original Proposed Regulation, which drew criticism because it was seen as a one-size-fits-all approach, the covered entity's cybersecurity program may now use risk assessments to identify the particular risks that are relevant to its business operations and assess the availability and effectiveness of controls that are designed to respond to those threats. Each covered entity is required to conduct the risk assessment periodically (and not annually as provided for by the Original Proposed Regulation).

The implementation of the program will provide covered entities with the foundation for a robust and successful plan to protect against cyber threats.

CISO report, testing and training

A number of requirements detailed in the Final Regulation have a 12-month transition period for covered entities to comply. These requirements must be met by March 1, 2018:

- CISO report on the covered entity's program (§ 500.04(b))
- Testing and vulnerability assessments (§ 500.05)
- Periodic risk assessments (§ 500.09)
- Multi-factor authentication to protect non-public information (§ 500.12)
- Cybersecurity awareness training for all personnel (§ 500.14(b))

Cybersecurity risks and third-party service providers

Further requirements of the Final Regulation have an 18-month transitional period for compliance and must be implemented by September 1, 2018. These include:

- Audit trail (§ 500.06)
- Application security policies for the development of in-house applications (§ 500.08)
- Data retention policies (§ 500.13)
- Monitoring of authorized users (§ 500.14(a))
- Encryption of nonpublic information (§ 500.15)

Risk management for third-party service providers

The Final Regulation specifically addresses scenarios under which third-party service providers have access or hold non-public information pertaining to a covered entity (§ 500.11). Covered entities will have until March 1, 2019 (two years from the effective date) to implement policies related to third-party service providers.

In those circumstances, a covered entity is required to implement written policies and procedures to ensure the security and integrity of such non-public information, by providing for:

- Minimum cybersecurity practices to be met by third-party service providers
- Due diligence processes to evaluate the adequacy of the cybersecurity practices of third-party service providers
- Periodic assessments of third-party service providers from a cybersecurity risk management perspective

Conclusion

The cybersecurity regulation adopted by the NYDFS imposes significant new requirements and obligations on covered entities. In light of the 180-day compliance window and the staggered implementation schedule, covered entities should immediately begin assessing their cybersecurity risks, implementing effective policies and developing robust cybersecurity programs to achieve compliance with the new cybersecurity requirements.

ABOUT SHEARMAN & STERLING LLP

Shearman & Sterling's Privacy & Data Protection team has the specialized skill sets and expertise required to provide clients with a comprehensive privacy management approach. From startups to multinational companies, business executives across every sector are looking for advisors with the knowledge and experience to advise on mission-critical initiatives and compliance issues. The cross-disciplinary and responsive team provides actionable intelligence and a practical approach to international data transfers, product counseling for new and enhanced product launches, development of compliance policies and programs, and data security breaches.

CONTACTS:

Richard C. Hsu
Partner
+1 650 838 3774
richard.hsu@shearman.com

Jordan J. Altman
Partner
+1 212 848 7125
jordan.altman@shearman.com

Jeewon Kim Serrato
Counsel
+1 415 616 1101
jeewon.serrato@shearman.com

SHEARMAN & STERLING LLP

Shearman & Sterling provides strategic, tactical and technical advice on M&A transactions that will transform our clients' organizations.

ABU DHABI | BEIJING | BRUSSELS | DUBAI | FRANKFURT | HONG KONG | LONDON | MENLO PARK | MILAN | NEW YORK
PARIS | ROME | SAN FRANCISCO | SÃO PAULO | SAUDI ARABIA* | SHANGHAI | SINGAPORE | TOKYO | TORONTO | WASHINGTON, DC

*Dr. Sultan Almasoud & Partners in association with Shearman & Sterling LLP

shearman.com

ABOUT MERGERMARKET

Mergermarket is an unparalleled, independent mergers & acquisitions (M&A) proprietary intelligence tool. Unlike any other service of its kind, Mergermarket provides a complete overview of the M&A market by offering both a forward-looking intelligence database and a historical deals database, achieving real revenues for Mergermarket clients.

Remark, the events and publications arm of The Mergermarket Group, offers a range of publishing, research and events services that enable clients to enhance their own profile, and to develop new business opportunities with their target audience.

To find out more, please visit
www.mergermarketgroup.com/events-publications

For more information, please contact:
Kathryn Cara
Sales Director, Remark
Tel: +1 646 412 5368

Part of the Mergermarket Group

www.mergermarketgroup.com

330 Hudson St. FL 4
New York, NY 10013
USA

t: +1 212.686.5606
f: +1 212.686.2664
sales.us@mergermarket.com

10 Queen Street Place
London
EC4R 1BE
United Kingdom

t: +44 (0)20 7059 6100
f: +44 (0)20 7059 6101
sales@mergermarket.com

Suite 1602-6
Grand Millennium Plaza
181 Queen's Road, Central
Hong Kong

t: +852 2158 9700
f: +852 2158 9701
sales.asia@mergermarket.com