

August 11, 2021

MERGERS & ACQUISITIONS

Evaluating Privacy and Cybersecurity Risks in Emerging Technology Transactions: Biometrics, Fintech and Cryptocurrency

By [Sujit Raman](#), [Sharon Flanagan](#), [Michael R. Roberts](#) and [Francesca Blythe](#), [Sidley Austin LLP](#)

Stakeholders must carefully monitor privacy and cybersecurity regulatory developments not only for their existing businesses, but also for potential transactions with target companies because a target's non-compliance with these responsibilities can undermine its financial valuation, ability to complete a successful sale, initial public offering or another strategic transaction. It also can impact the target company's reputation and customers' confidence in the business.

In this two-part article series, we examine U.S., U.K. and E.U. regulatory trends in four key emerging technology sectors that recently have seen vastly increasing amounts of transactional activity. Based on our experience assessing the privacy and cybersecurity aspects of several recent transactions in these data-intensive sectors, we outline many of the key issues that stakeholders may wish to consider when evaluating the privacy, data protection and cybersecurity risk profiles of target companies in those industries.

This second installment addresses biometrics, as well as financial technology and cryptocurrency transactions. [Part one](#) outlined considerations for artificial intelligence and education technology transactions.

See "[Privacy and Cyber Due Diligence in M&A Transactions](#)" (Mar. 11, 2020).

Biometrics

Biometric data has also been a key focus area for investors and dealmakers. As noted in a [recent FTC enforcement action](#), biometric information is "data that depicts or describes the physical or biological traits of an identified or identifiable person," though some U.S. state laws define the term more specifically. Diligence in this area should focus on a target company's compliance with existing regulations and guidance, and on risks associated with third-party vendors that may have access to this sensitive data.

Consider U.S. Issues

The parties should take steps during due diligence to confirm that the target company has insurance, contractual and compliance protections in place with respect to any collection, use and other processing of biometric data. To assess these risks, stakeholders should take the following steps:

1. *Request and review the target company's cybersecurity insurance policy.* Review the policy to identify any references to

laws related to the use, collection and other processing of biometrics data, including Illinois' Biometric Information Privacy Act (BIPA) and other state and local biometrics laws (e.g., Texas, Washington, New York City), as well as any biometric information that may constitute PHI under HIPAA or covered medical information under state laws.

2. *Review contracts with vendors that may be involved in the processing of biometric collection on behalf of the target company.* Determine if these contracts contain indemnification provisions that might limit the exposure related to a violation of any applicable biometric information privacy laws.
3. *Review regulatory enforcement actions and guidance from the FTC.* For example, the agency recently brought an [enforcement action](#) under Section 5 of the FTC Act related to the commercial collection and use of biometric information, based upon allegations that a company had deceived consumers about its use of facial recognition technology and its retention of the photos and videos of users who deactivated their accounts.
 - Based on these FTC actions, key issues may include whether a target company could be viewed as deceiving consumers about its use of biometric technologies and whether the target company has been transparent regarding its retention of both current and former user data.
 - Stakeholders should also diligence whether the target company provides notice to, and obtains consent from, users and customers with respect to the use of biometric technologies

and data; whether the target company shares biometric data with third parties; and whether the target company has maintained and implemented reasonable information security policies, procedures and safeguards appropriate to the nature of the biometric information.

See CSLR's three-part series on the rise of facial recognition technology: "[Uses and Risks](#)" (Jan. 22, 2020); "[Mapping the Legal Framework](#)" (Jan. 29, 2020) and "[Mitigating Risk](#)" (Feb. 5, 2020).

Consider E.U./U.K. Regulations and Opinions

Given the sensitive nature of biometric data, stakeholders should focus on the lawfulness of the processing of this data, and of the security measures implemented to safeguard it. Stakeholders should also confirm that all necessary data protection impact assessments have been carried out, and that steps have been taken to address official requirements related to [privacy by design](#) and [privacy by default](#).

Stakeholders should also consider the various approaches taken by regulators at a national level regarding biometric data, as certain countries have very restrictive rules regarding such data and its use in particular environments, such as the workplace.

The use of biometric data has been the subject of recent high-profile enforcement actions by E.U. data protection supervisory authorities and courts, including in connection with the use of facial recognition technology at schools in Sweden and in France, as well as of opinions of courts and of public authorities in the U.K.

Likewise, the European Data Protection Board (EDPB) has raised concerns around the high level of risk presented by the combination of “sensitive personal data,” such as biometric data, in the context of mergers.

The EDPB declared in August 2018, for example, that “it is essential to assess longer-term implications for the protection of economic, data protection and consumer rights whenever a significant merger is proposed,” and reiterated [in February 2020](#) that parties engaged in significant mergers should, “in accordance with the principle of accountability... conduct in a transparent way a full assessment of the data protection requirements and privacy implications” of those mergers.

Stakeholders should therefore evaluate a target company’s compliance program for the collection, use and other processing of biometric data to determine if it aligns with the requirements of the GDPR, with the EDPB’s expectations, and – to the extent that country-specific requirements may differ from the GDPR – with the requirements of national member-states.

See “[Navigating Today’s Biometric Landscape](#)” (Apr. 3, 2019).

Review Personal Data Provisions and Account for Appropriate Risk

Review transactional agreements to determine if provisions related to personal data include biometric information and if these provisions incorporate reference to and/or requirements of Illinois’ BIPA, other U.S. state laws that govern the privacy of biometric data, as well as applicable E.U./U.K. requirements.

Stakeholders should ensure that transactional agreement provisions properly account for the risk posed by the volume of biometric information at issue. Parties should, among other steps, determine the appropriate lookbacks for representations that involve biometric information-collection practices and compliance programs, and identify whether more specific representations are needed to track the compliance requirements of applicable laws and standards.

See “[Big Questions for BIPA Case Law in 2021](#)” (Feb. 17, 2021).

Identify Risks in Disclosure Schedules

Companies should review and analyze the target company’s disclosure schedules to identify any risks related to biometric data outside of the privacy, data protection and cybersecurity representations and warranties.

Because biometric information creates risks in a multitude of legal areas, transactional stakeholders should seek to identify any relevant disclosures outside of privacy and security, including representations related to litigation, material contracts, intellectual property and employment issues.

See “[Effective M&A Contract Drafting and Internal Cyber Diligence and Disclosure](#)” (Dec. 20, 2017).

FinTech and Cryptocurrency

In recent months, there has also been tremendous activity in the financial technology (FinTech) space, most notably with respect to

cryptocurrency businesses. Diligence in these areas can be especially challenging, as regulatory frameworks remain uncertain. Below, we offer several key considerations for stakeholders working on deals in the FinTech and cryptocurrency space.

Review Compliance Program for Alignment With Regulatory Guidance and Industry Standards

During due diligence, stakeholders should review the target company's privacy, data protection and cybersecurity compliance programs to determine if they align with recommendations and guidance from government agencies and industry standards organizations. These due diligence considerations also apply to the stakeholders' review and negotiation of the transactional agreements.

U.S. Regulatory Actions, Statements and Guidance

With respect to U.S. agencies, stakeholders should review recent privacy and cybersecurity-related actions as well as published statements and guidance in the FinTech and cryptocurrency spaces from regulators, including the FTC, the Consumer Financial Protection Bureau, the SEC, the Commodity Futures Trading Commission, the Office of the Comptroller of the Currency, and the Financial Crimes Enforcement Network. Stakeholders will also want to ensure that they sufficiently diligence whether any specific contractual requirements or best practices should be in place for the transactional agreements to confirm that steps are taken for compliance purposes.

Common Key Regulations

Stakeholders should diligence compliance programs to determine the applicability of common key regulations addressing privacy and security issues, such as the Gramm-Leach Bliley Act (GLBA), the FCRA, and the U.S. Anti-Money Laundering (AML) regulations, and address these topics in the transactional agreements.

Ensure Reasonable Security Safeguards Were Implemented and Maintained

Stakeholders should determine whether the target company has maintained and implemented reasonable information security safeguards to protect pertinent sensitive data as well as disaster recovery and business continuity policies, procedures and regular testing processes.

It may be essential to work with third-party consultants to examine the target company's current or planned security and custodial practices with respect to protecting its digital exchange, including keys, wallets and stored assets, against cyberattacks (such as DDoS, ransomware and malware attacks), as well as against other security threats.

Assess Third-Party Service Provider Use

As part of their diligence, stakeholders will also want to understand whether the target company uses, or is in negotiations to use, third-party service providers for custodial services of any customer assets on its exchanges.

Understand Potential Vulnerabilities of Digital Wallets and Keys

Other important diligence issues, which should also be addressed in the transactional agreements, include confirming:

- whether the target company has reviewed its digital keys, wallets and currencies to understand whether any assets are potentially vulnerable to cyberattacks or threats; and
- whether the target company plans to implement any policies or procedures to secure its keys, wallets and any stored currencies. These policies and procedures may include using “cold storage” for virtual currencies on its exchange; “air-gapping” assets from the internet; and employing additional layers of protection (e.g., using multiple digital wallets for customer assets and access, and employing approval controls for such wallets and associated transactions, or using multi-signature and management controls).

Evaluate Plan for Addressing Evolving Blockchain Risks

From an E.U./U.K. perspective, tensions exist between E.U./U.K. privacy laws and the blockchain technology leveraged by cryptocurrencies. In turn, stakeholders should evaluate how target companies intend to address the evolving privacy, data protection and cybersecurity risks presented by FinTech and cryptocurrency technologies, including the uncertain nature of relevant processing responsibilities and the impact of evolving legal implications of international data transfers.

Stakeholders should diligence how the target company is addressing issues presented by the blockchain’s decentralized structure, including how to allocate privacy and security responsibilities to the various actors. Stakeholders should also consider how the target company is meeting its obligations to, for example, erase personal data on request. These obligations become increasingly complex in the blockchain context because of processes used in the blockchain to ensure data integrity that may affect the feasibility of data amendment.

See [“New Sidley Partner Lilya Tessler Discusses the FinTech and Blockchain Space”](#) (Sep. 26, 2018).

Assess International Data Transfer Compliance

Stakeholders should also assess compliance with restrictions on international transfers under E.U./U.K. privacy laws following the Schrems II decision. Because blockchain technologies may keep the ledger on multiple nodes in various jurisdictions both inside and outside the E.U., stakeholders should diligence any permissions and access controls for the network for such technologies to determine which parties may be involved in any international data transfers and how such transfers are legitimized.

See CSLR’s two part series on EDPB recommendations: [“Personal Data Transfers After Year Zero: A More Appealing Set of EDPB Recommendations?”](#) (Jul. 14, 2021).

Sujit Raman is a partner in Sidley's privacy and cybersecurity group, with a wide-ranging practice spanning government investigations and litigation, data protection, information security and management, and cyber governance and preparedness. Before joining the firm, Raman served as Associate Deputy Attorney General at the DOJ where he assisted the Attorney General and Deputy Attorney General in their oversight of the nation's cyber-related criminal and national security investigations and prosecutions, and led DOJ's policy formulation in a number of critical areas, including cybersecurity, cross-border data transfers and protection, 5G/supply chain security, and emerging technologies such as facial recognition, cryptocurrency and encryption. He is based in Sidley's Washington, D.C. office.

Sharon Flanagan is a partner in Sidley's M&A practice and serves as a member of the firm's management committee, executive committee and its global life sciences leadership council.

She represents companies in a broad range of M&A transactions, securities offerings and corporate governance matters, with a particular focus on life sciences/healthcare and technology industries. She serves as managing partner of Sidley's San Francisco office.

Michael Roberts is an associate in Sidley's privacy and cybersecurity practice, advising clients on regulatory, compliance and transactional matters related to data privacy, cybersecurity and data protection. He is based in the firm's New York office.

Francesca Blythe is a senior associate in Sidley's privacy and cybersecurity practice, advising international clients on a wide range of data protection, privacy and cybersecurity issues, with a focus on certain key industries including life sciences, asset management and private equity, payments, technology, e-commerce and manufacturing. She is based in the firm's London office.