Bulletin | Cybersecurity, Privacy and Data Protection

January 2023

Privacy, cybersecurity and M&A transactions – A cautionary tale

The U.S. Federal Trade Commission's 2022 privacy and data security enforcement action regarding the CafePress online retail platform resulted in orders against both parties to a 2020 transaction for the sale of the CafePress business and assets. The enforcement action is a cautionary tale for parties to M&A transactions.

The data breach and the transaction

CafePress is a popular online platform that allows consumers to purchase officially licensed merchandise and stock and user-customized on-demand products (e.g., clothing, accessories, drinkware and stationary) from virtual shopkeepers. CafePress was valued at approximately USD$25 million in 2018.

In February 2019, a hacker exploited security vulnerabilities in CafePress' information technology system to access and exfiltrate the personal information of consumers and shopkeepers, including more than twenty million unencrypted email addresses, millions of unencrypted names, physical addresses and security question/answer pairs and more than 180,000 unencrypted social security numbers. In September 2019, after the breach was discovered and publicized by independent third parties, CafePress sent breach notifications to government agencies and affected consumers.

In September 2020, PlanetArt purchased substantially all of CafePress' assets (including the CafePress trade name) and continued operating the CafePress business from the cafepress.com website. A news release explained that the CafePress assets included "a best-of-breed technology toolset" that PlanetArt would use to bring a marketplace facility to its other brands. The terms and financial aspects of the transaction were private. After the transaction, CafePress changed its name to Residual Pumpkin Entity, LLC ("Residual Pumpkin").

FTC enforcement action

In March 2022, more than two years after CafePress reported the February 2019 data breach, the U.S. Federal Trade Commission (FTC) announced enforcement action against both Residual Pumpkin and PlanetArt, alleging that each of them had violated the *Federal Trade Commission Act* by engaging in unfair or deceptive acts or practices regarding the handling of personal information of CafePress consumers and shopkeepers.

The FTC's complaint alleged that each of Residual Pumpkin and PlanetArt engaged in unfair and deceptive acts and practices while operating the CafePress business, including: (1) failing to provide reasonable security for the personal information of consumers and shopkeepers stored on its networks; and (2) making false or misleading statements, including in its privacy policy, regarding its personal information security measures. The complaint alleged that, after the transaction was completed, PlanetArt continued to operate the CafePress business "from the same building, with the same servers, using many of the same vendor accounts, in the same line of business, with many of the same personnel as" Residual Pumpkin. In addition, the complaint alleged that Residual Pumpkin failed to respond adequately to several pre-transaction data security breaches (including the February 2019 data breach) and made false or misleading statements about its responses to data security breaches.

In June 2022, the FTC announced the finalization of decisions and consent orders against each of Residual Pumpkin and PlanetArt. The consent orders require each of Residual Pumpkin and PlanetArt, and any business they control directly or indirectly, to establish, implement and maintain a comprehensive information security program that protects the privacy, security, confidentiality, and integrity of personal information and to report independent assessments of the program to the FTC for the next twenty years. In addition, Residual Pumpkin was required to pay a $500,000 penalty for use by the FTC to provide consumer redress to CafePress customers and shopkeepers, and PlanetArt was required to send a prescribed notice about the February 2019 data breach to all affected consumers.

Comments/recommendations

Privacy and cybersecurity risks are essential considerations for almost all M&A transactions because they can affect the viability and value of the transaction, influence the nature and terms of the transaction and, in some circumstances, cause the parties to abandon the transaction. See BLG bulletins *Managing cyber risks in M&A transactions*, *Cyber risk management guidance for Canadian corporate directors*, and *Privacy Commissioner decision provides guidance for parties to M&A transactions*.

Privacy risks relating to Canadian M&A transactions will soon increase significantly as a result of the modernization of Canadian privacy laws to give privacy commissioners robust enforcement powers, including authority to conduct investigations, make binding orders, enter into compliance agreements, and impose or recommend potentially substantial administrative monetary penalties. For example, commencing September 2023, Québec's Commission d'accès à l'information will be able to impose administrative monetary penalties of up to the greater of $10 million or 2% of worldwide turnover on organizations that contravene Québec's private sector privacy law. See BLG bulletins *Québec adopts Bill 64 – Key requirements for businesses*, *Canada's Consumer Privacy Protection Act (Bill C-27): Impact for businesses*, and *Special committee recommendations to modernize B.C.'s private sector privacy law*.

The FTC's CafePress enforcement action is a cautionary tale with three key takeaways for appropriate action by parties to M&A transactions:

1. Asset purchase transactions can transfer privacy risks to the buyer if the buyer uses purchased assets (including branding, information technology systems and related practices, procedures and notices) and acquired personal information to operate the purchased business.
2. A pre-transaction privacy breach that the seller remediates and reports to regulators and affected individuals before a transaction can result in post-transaction regulatory enforcement action against both the seller and the buyer.

3. Regulatory enforcement action regarding a pre-transaction privacy breach can include scrutiny of the buyer's cybersecurity and privacy practices and result in orders against the buyer regarding all of the buyer's business activities (not just the purchased assets/business).

Parties to an M&A transaction should address those issues, and other privacy and cybersecurity risks, throughout the transaction life cycle. Key steps include:

- Implement cybersecurity controls (e.g., data confidentiality/security agreements, secure online data rooms, and communication protocols) for the deal processes used by the transacting parties and their advisors and to protect commercially sensitive and regulated information (e.g., personal information) disclosed during negotiations and due diligence.
- Ensure non-disclosure agreements and transaction agreements include provisions required by privacy laws for the disclosure and use of personal information in connection with the transaction (e.g., for due diligence purposes and as purchased assets) without the consent of affected individuals.
- Implement a strategy to help assert legal privilege over privacy/cybersecurity due diligence results.
- Conduct appropriate privacy/cybersecurity due diligence of each transacting party to identify and assess risks (including residual risks from pre-transaction privacy breaches) relevant to the transaction and post-transaction activities and to support applications for representation and warranty insurance (if applicable) and post-transaction privacy/cybersecurity insurance.
- Document the decisions and actions by or at the direction of transaction decision-makers (e.g., corporate directors and officers), based on consideration of due diligence results, to establish their compliance with legal obligations (e.g., corporate directors' and officers' risk management duties and continuous disclosure obligations, if applicable).
- To the extent appropriate and practicable, mitigate identified privacy/cybersecurity risks before the transaction is completed (e.g., implementing the data minimization principle) and plan to avoid/address risks after the transaction is completed (e.g., establishing corporate structures and practices/procedures to avoid/minimize unnecessary transfers of risk from seller to buyer).
- Consider privacy/cybersecurity due diligence results when negotiating the nature, structure and terms of the transaction, and include in transaction agreements appropriate risk allocation provisions – representations and warranties, covenants, indemnities and remedies – to address privacy/cybersecurity risks for a reasonable period after the transaction is completed.
- After the transaction is completed, promptly implement privacy practices and cybersecurity controls to address privacy/cybersecurity risks identified during due diligence and additional or increased privacy/cybersecurity risks resulting from the transaction, and consider procuring additional privacy/cybersecurity insurance. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's Cybersecurity, Privacy & Data Protection Group has extensive expertise and experience in cyber risk management and crisis management legal services. Find out more at **blg.com/cybersecurity**.