Data Privacy and Security Concerns for Businesses in the Hospitality and Tourism Markets

Hospitality and tourism is a broad and varied industry that can encompass hotels, restaurants, bars, casinos, theme parks, wineries, breweries, distilleries and more. While these businesses all have very different methods of operation, there are some data privacy and security concerns that all businesses in the industry should be aware of.

Each business likely maintains a vast array of data on its own operations, on its employees and on its customers. The hospitality industry in particular can be a target for cybercrime. Access points can be card readers / point of sale systems, guest Wi-Fi, internet of things (iot) devices, etc. For example, there was a well-publicized attack on the Inter Continental Hotel Group in 2022, impacting its Regent, Crown Plaza and Holiday Inn hotels.

Businesses operating in the hospitality and tourism space should be aware of evolving best practices related to data privacy, including but not limited to: performing risk assessments, training staff regularly on cybersecurity policies and risks, keeping software and hardware updated, requiring multi-factor authentication to access email and network files, external threat monitoring through a cybersecurity vendor, requiring complex passwords and end-to-end encryption, to name a few but the list goes on. Indeed, the list should include reviewing software update policies in the wake of the CrowdStrike debacle.

While the legal, regulatory and technology landscape of data privacy is constantly evolving, there are some particular issues that businesses in the New York hospitality and tourism industry should keep in mind:

1. Payment Card Industry Data Security Standard (PCI DSS) Compliance. The PCI DSS was developed to protect payment card account data and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides technical and operational requirements that businesses should be familiar with. While these standards are not a part of a law or regulation, compliance with PCI DSS is typically required by the major credit card brands, who established the PCI Security Standards Council.

2. Exclusions from Cybersecurity Insurance Coverage. Cyber insurance plays an important part in protecting your business. However, it is key to understand how much coverage you have, what is covered, and, importantly, what exclusions from coverage are included in your policy. Common exclusions to be aware of include:

    a. The policy may require the business to maintain appropriate procedures and controls to protect against cyber attacks and exclude coverage if such procedures or controls were not in place.

    b. Cyber policies may include a retroactive date, such that the business will not be covered for

any acts, incidents or circumstances that were committed, occurred or arose prior to a certain date, even if the incident is not discovered for some time.

c. Bodily injury is often excluded, as well as loss or damage to hardware or any physical property.

d. Failure of critical national infrastructure will commonly be excluded from policies.

e. Jurisdictional limits may be included.

3. Obligations to Protect Consumer Data. Under New York law, businesses must use reasonable safeguards to protect New Yorkers' personal information. If your company conducts business in New York, you must abide by the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act).

The SHIELD Act is meant to protect unencrypted copies of:

- Social security numbers

- Driver's license numbers or non-driver identification card numbers

- Account numbers, credit or debit card numbers, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account

- Account numbers, credit or debit card numbers, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code or password

- Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity

- User names or e-mail addresses in combination with passwords or security questions and answers that would permit access to an online account.

Businesses in possession of such data must take steps to ensure it is physically and technologically secure and disposed of in a reasonable amount of time and in a safe manner. You must also adopt a written cybersecurity program that meets certain requirements. Certain small businesses may be considered compliant if they take reasonable steps to protect data, consistent with the nature and scope of business operations and the sensitivity of data collected from or about consumers.

4. Notice Requirements Should a Data Breach Occur.

The SHIELD Act requires any covered person or business to notify New York State residents about any unauthorized access of their "Private Information" in its computer systems. You must send the notification as soon as possible, subject to certain narrow exceptions (such as the explicit request of law enforcement agencies). You may be allowed to provide the consumer with a "substitute" notification if the cost of providing individual notices will exceed $250,000 or the number of affected individuals exceeds 500,000. Aside from notifying consumers, you also must

notify the New York State Department of State Division of Consumer Protection, the New York State Attorney General and the New York State Division of State Police.

5. Duty to Comply with Employee Privacy Laws. If your business uses electronic devices to monitor or intercept employees' phone transmissions, email or internet usage, the business must provide a formal notice to employees. The notice must be posted in a conspicuous place and provided to employees upon hiring.

These are just a few issues that businesses in the hospitality and tourism industry should be aware of relating to data privacy and security.

For any questions about this issue, please contact Jennifer Tsyn or any attorney in Bond's hospitality and tourism or cybersecurity and data privacy practices or the attorney at the firm with whom you are regularly in contact.