AVOID DIGITAL DOUBLE BOGEYS:

The potential pitfalls of collecting, using and sharing customer data through your Golf Management Systems and how to avoid them

This article specifically addresses the collection of customer data. However, you (as a golf course owner, operator, or PGA professional) may collect personal information from other persons during the course of your business, including but not limited to: employees, vendors...etc. that may require the implementation of separate data privacy procedures, practices and notices.

Times are changing, and golf courses must also keep up with the times. Utilizing up-to-date, state of the art Golf Management Systems (GMS) offering Point of Sale (POS) systems with integrated tee sheets is a non-negotiable in the digital age. However, by using these golf management systems and other digital marketing tools, you may be collecting your customers' personal information, including but not limited to: names, phone numbers, e-mail addresses, physical addresses and customer activity ("**Customer Data'**). This Customer Data is being stored in your golf management systems and made available not only for your use, but also the use of third parties such as your software providers.

By collecting Customer Data, whether directly or indirectly, knowingly or unknowingly, you are taking upon yourselves a duty to not only make commercially reasonable efforts to keep that information safe but also to be transparent about the collection, use, sale, license, assignment transfer and disclosure of the information you collect.

Now, if you're saying to yourself, 'this article sounds nice but it doesn't apply to me' or 'I don't collect personal information from customers. I just book the tee times and sell golf balls.' Let me stop you right there because this article likely does apply to you and you need to keep reading. To determine whether or not you are collecting private customer information, ask yourself a few questions:

1. Does my facility use a POS/tee sheet that is owned or operated by an Online Tee Time Agent (OTTA) or Golf Management System (GMS)? This includes but is not limited to: GolfNow, Supreme Golf Solutions, EZLinks, Teesnap, Chronogolf, ForeUp, Club Prophet, Jonas, Clubessential, Tee-On, etc.
2. Does my course, either on its own or through a third party manage and maintain a website that allows customers to book tee times directly through our website?
3. Does my course, either on its own or through a third party have and use a list-serv of customer e-mails to regularly communicate with members and/or customers?

Well, if your answer to any of those questions was yes, then put down that pitching wedge and pay attention. You will need to know and understand the legal implications of collecting Customer Data through any medium, digital or otherwise and how to avoid legal pitfalls as you navigate the evolution of golf course operations in the age of technology.

Why is any of this important and how did we get here?

Well, let's take it from the top! Recently a software and digital marketing company **("Vendor")** that provides POS and tee sheet software to various golf courses became the subject of debate. This Vendor requires client golf courses to sign their standard agreement prior to doing business together.

These agreements generally include a provision that requires a golf course to allow the Vendor and its "affiliates" to access and use customer data stored in the Golf Management System database for marketing or other purposes. According to the definition of "affiliate" provided in the agreement, the parent company of this Vendor would be considered an "affiliate" of the subsidiary, thereby eligible to receive customer data from the Vendor, through its golf course clients' use of the software.

Sometime recently, the Vendor's parent company sent an email to customers who were subscribed to the mailing lists of some of the Vendor's golf course clients. The emails that were sent to the golf course's customers read, "An update from xyz golf course," but the contents of the email advertised deals that were not specifically related to the golf course's services. Some golf course customers on the receiving end of these emails were upset by what they deemed to be a breach of trust between themselves and the golf course due to the golf course's disclosure of their personal information to third parties without either their knowledge or permission.

While breach of customer trust can have a negative impact on the public image, brand reputation and goodwill of a company, is the disclosure of information to third parties without prior written notice or consent to customers merely a case of hurt feelings or a violation of the law that could result in civil or criminal litigation?

If you are reading this and do not want your Vendor sharing your Customer Data without your permission, you need to let your software provider know that and thoroughly review your agreement. In the aforementioned example, the Vendor earned the right to access and use Customer Data for marketing or other purposes, when its golf course clients signed their agreements.

So here, the unethical conduct was not that the Vendor accessed the data, but that the Vendor sent emails, on behalf of golf courses, that were misleading at best. These questionable business decisions now lead us to examine the issue of privacy and permission in sharing of data.

To explore these issues, this article will answer the following two questions:

1. Is it against the law to share Customer Data with third parties? and
2. What can I as a golf course owner/operator do to protect my facility from government reprimand and customers who are dissatisfied with my handling of their personal information?

Is it against the law to share Customer Data with third parties?

There is currently no federal law (depending on your state of residence, there may be a state law that affects you. See California Consumer Privacy Act (CCPA) of 2018) restricting or prohibiting the sale, transfer, assignment, lease or general disclosure of customer information to third parties. However, if you collect and store personal information from customers through ANY digital platform including but not limited to: online tee sheets, digital POS systems, websites, payment portals, "Contact Us" forms and digital "Sign Up" sheets, federal regulations mandate that you: (a) provide a clear, conspicuous and easily accessible notice to customers that you are collecting and storing their personal information that includes a plan for protecting Customer Data and (b) disclose to customers your intended use(s) for their personal information.

What can I as a golf course owner/operator do to protect my facility from government reprimand and customers who are dissatisfied with my sharing of their personal information?

To comply with federal regulations, regarding the collection, storage, license and transfer of Customer Data and protect yourself from penalty, sanction and/or litigation, all golf course owners that collect

Customer Data through any digital platform should implement company privacy policies. A privacy policy is a legal document or notice that discloses a website owner's practices for collecting, using, maintaining, protecting and/or disclosing the information it gathers through its website or other digital platforms under its direction and/or control from its visitors, users and customers. Accordingly, if you are collecting personal information of customers through POS systems and tee sheets or any other digital platform, it is important to employ a legal mechanism, in the form of a privacy policy, that not only informs customers of what you do with their private information but also provides you some protection in the event their information ends up in the wrong hands. In such an event, federal regulations only require that a company act reasonably given the circumstances. Reasonable action generally means following whatever terms you have set forth for protection or disclosure of Customer Data in your privacy policy.

So, what exactly should be in a privacy policy? The corresponding documents (www.teetimecoalition.org/dataprivacy) provide some best practices for crafting a comprehensive privacy policy as well as a copy of a sample privacy policy that protects both you and your customers when you use Customer Data to engage in email marketing.

Press Contact:
Jared Williams, J.D.
Managing Director
Golf USA Tee Time Coalition
jwilliams@teetimecoalition.org

About the authors

This article was written by Sydnee Mack, Esq. in collaboration with the Golf USA Tee Time Coalition. Sydnee Mack is owner of Sydnee Mack Attorney at Law, a boutique Sports & Entertainment and Small business law firm in Atlanta, GA. Sydnee focuses her sports practice on issues central to the golf community and is also a professor of sports law at the Georgia State University College of Law, also located in Atlanta, Ga.

Works Cited

Fair Credit Reporting Act15 U.S. Code § 45(a)(1)and(2) - Unfair methods of competition unlawful; prevention.

Federal Trade Commission (2003) FTC Working to Protect Consumers and Businesses From Information Security Breaches

L. Jolly, Loeb & Loeb LLP. US Privacy and Data Security Law: Overview

15 U.S.C. § 7701-13- Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)

8-617-7036 Westlaw Intellectual Property and Technology FTC Data Security Standards and Enforcement

ABA Business Law Journal Volume 14 Number 2 (2004). B. Henderson. Hey, that's personal! When companies sell customer information gathered through the Internet