KEEPING UP WITH THE FTC

Understanding the Impact of Rapidly Evolving Cybersecurity and Data Privacy Standards

The vast majority of businesses digitally handle and store individuals' confidential data in some capacity and rely on virtual systems for their day-to-day operations. However, the value add of technology comes with a price: you're responsible for implementing a cybersecurity strategy that protects sensitive data and all your digital assets. **When it comes to your cybersecurity and data privacy strategy, you can't just set it and forget it – cyber risk is dynamic.**

In addition to staying abreast of threat vectors and bad actors' tactics, you also need to be in tune with changes in the regulatory landscape. With the digital world in a state of constant flux, regulatory and legislative bodies at both the state and Federal government levels continue to enact more laws and decrees that are reshaping the expectations, standards, and legal liabilities for companies with a digital footprint.

We recently talked about the uptick in lawsuits related to biometric data privacy laws. Today, we want to discuss another area of growing regulatory cyber risk – the Federal Trade Commission's enactment, enhancement, and execution of data privacy and cybersecurity rules.

The FTC has recently ramped up its setting, scrutiny, and enforcement of cybersecurity and data privacy standards, and this impacts organizations far and wide. In fact, in February of 2023, the FTC announced the creation of the Office of Technology which has the following goals:

- Strengthen and support law enforcement investigations and actions
- Advise and engage with the FTC on policy and research initiatives
- Engage with the public and relevant experts to understand trends and advance the Commission's work.

This course of action from the FTC doesn't exist in a vacuum. The Biden administration has demonstrated that cybersecurity is a key area of interest, which is why the FTC and other federal agencies are following suit. So, what does this look like in practice? And what are the implications for your business? **Here's what you should keep in mind.**

FTC RULES AND ENFORCEMENT, IN ACTION

The FTC has used its authority to promulgate and amend data privacy rules, and businesses that aren't compliant are paying the price. Though this is not an exhaustive list of the FTC's cybersecurity and data privacy rules and expectations, these are notable samples that demonstrate the agency's commitment to holding companies liable for failing to comply with its rules.

AHT INSURANCE
A BALDWIN RISK PARTNER

Health Breach Notification Rule (HBN Rule)

The FTC issued a policy statement in September 2021 regarding the HBN Rule (originally enacted in 2009). Since the HBN Rule was issued over a decade ago, the statement clarified that this rule also applies to most health applications, connected devices, and similar products, which have now become commonplace.

The consequences:

The FTC first enforced this rule in February 2023 when they slapped GoodRx with a $1.5 million penalty for sharing users' personal health information with third parties without properly disclosing their practices or obtaining users' consent.

Hot off the heels of the GoodRx incident, in March 2023 the FTC announced a consent decree with online therapy provider BetterHelp to address claims that the mental health provider deceived customers when it sold their sensitive data to third parties for ad targeting. The settlement requires BetterHelp to pay $7.8 million to consumers to settle these charges.

Children's Online Privacy Protection Act (COPPA)

Though the FTC last amended COPPA in 2013, the agency hasn't shied away from enforcing the rule in recent months. COPPA is designed to protect children under the age of 13 from the collection, use, and disclosure of their personal information by commercial entities and online services.

The consequences:

In December 2022, the FTC reached an agreement with Fortnite owner, Epic Games, ordering the gaming giant to pay a total of $520 million in refunds and fines. $275 million of that total amount was a penalty for violating COPPA while the remaining $245 million is to refund affected users. The FTC alleged that Epic Games collected personal data from children under 13 without parental consent, enabled voice and text chat by default, and used deceptive practices to bill Fortnite players for unintended in-game purchases.

Fair Credit Reporting Act

In addition to creating its own rules, the FTC also helps enforce laws enacted by Congress, like the Fair Credit Reporting Act. Under this act, companies that provide information to consumer reporting agencies must comply with specific legal requirements or face certain consequences.

The consequences:

In September 2022, the FTC reached a $3 million settlement with personal finance company Credit Karma. The FTC alleged that Credit Karma would lure customers in by making false claims that they were preapproved for lines of credit. The individuals would then apply for these offers only to be denied.

Data security and privacy standards, for all companies

If you're thinking that you might be in the clear because your company doesn't deal with the aforementioned variables, think again. The FTC expects all companies, regardless of industry, to comply with its cybersecurity and data privacy standards, both in the present and as they evolve.

The consequences:

è In January 2023, the FTC ordered online alcohol marketplace Drizly and its CEO to rectify security failures that exposed the personal information of about 2.3 million consumers. The FTC also ordered education technology provider Chegg Inc. to implement corrective measures for "careless data security practices." In both instances, the FTC didn't impose a monetary penalty since it was the agency's first complaint against both entities.

Failure to listen to the FTC the first time might have them knocking on your door again, but with a fine in tow. Take Twitter as an example. The FTC originally reached a consent decree with the social media giant in 2011, where Twitter agreed to improve the ways it protected its users' personal information, with significant financial consequences if it failed to do so. Fast forward to 2022, and the FTC found that Twitter violated the 2011 order. The FTC imposed a $150 million civil penalty for violations of the original order and imposed a new order with additional provisions.

Standards for Safeguarding Customer Information (Safeguards Rule)

The FTC amended the Safeguards Rule in 2021 to ensure that the rule keeps pace with current technology. This rule covers certain financial institutions, including mortgage lenders, wire transferers, collection agencies, and more. Changes to the Safeguards Rule expand pre-existing information security requirements for these institutions and their third-party service providers by requiring them to develop, implement, and maintain a comprehensive information security program. Organizations are expected to meet new compliance requirements by June 9, 2023.

The consequences:

Though the updated Safeguards Rule is not yet in effect, look at recent consent decrees as indicators that the FTC will enforce these new standards. Fines and penalties can easily reach thousands to millions of dollars.

USING FTC RULES AS GUIDELINES FOR YOUR BUSINESS

You may be wondering how exactly you might be able to adhere to so many rules and regulations, especially with the FTC continuing to make changes. It's important for you to align your legal team, IT department, executives, insurance advisor, and any other relevant parties so that you're on the same page about your cybersecurity and data privacy posture. This enables your business to build strategies that reduce your cyber risk and help you remain legally compliant. And as regulations change, this alignment improves your ability to adapt so that you're less likely to get hit with a penalty.

It's important for you to align your legal team, IT department, executives, insurance advisor, and any other relevant parties so that you're on the same page about your cybersecurity and data privacy posture.

Though recent actions from the FTC might be concerning, you have an opportunity to use these consent decrees and rules as suggested guidelines for your cybersecurity and data privacy practices. The FTC has also created a vast resource library that provides detailed recommendations about how organizations can remain compliant. Businesses interested in learning about how they can comply with the FTC's data privacy and security guidelines can visit this resource hub on their website.

Additionally, if you've purchased cyber insurance, you might even notice that there's some overlap between the FTC's recommendations and certain carrier requirements for coverage.

HOW DOES INSURANCE FIT INTO THE PICTURE?

With regulatory scrutiny increasing, now is the time for a thorough review of your cyber policy with your insurance advisor. Though comprehensive cyber coverage typically covers attorney fees and costs that stem from regulatory investigations, penalties, or fines, not all cyber policies are created equal.

When it comes to cyber coverage, the devil is in the details. Some policies may have exclusionary language for regulatory fines, in which case you'll need to see if there's a carve back so that you're covered for these situations. And if your policy has outright exclusionary language, then you might be vulnerable to the pitfalls of a coverage gap. It's also important to note that some cyber policies exclude coverage for claims arising from unauthorized data collection practices.

HOW CAN YOUR ADVISOR HELP?

Though there isn't a set of standardized guidelines that organizations can follow, implementing the recommendations in the FTC's consent decrees, as well as carrier requirements for coverage, can be a good foundation from which you can build on.

And you don't have to navigate the complexities of cyber risk alone. Our team of experienced cyber experts is here to help you determine what your risk is and provide resources that help you improve your cybersecurity posture and remain compliant. We can also help you understand what your cyber policy covers and enhance it for your particular needs as they continue to evolve.

Connect with one of our Cyber experts to help protect your organization.

AHT INSURANCE
A BALDWIN RISK PARTNER