Regulation of Companies' Data Security Practices under the Federal Trade Commission Act and California Unfair Competition Law

By Kathryn F. Russo

News of data breaches dominates the headlines. Technology is advancing at a dizzying speed. Companies are collecting more sensitive personal information about consumers than ever before while hackers are devising new strategies to access this information.

In the context of this data-driven world, it is no surprise that companies' data security practices are coming under increasingly stricter scrutiny. The Bureau of Justice Statistics estimates that approximately 7 percent of all US residents age 16 or older were victims of identity theft in 2012.[1] Both the Federal Trade Commission (FTC) and the California Attorney General have made it a priority to pursue enforcement actions against companies that do not have reasonable data security practices.

For more than a decade the FTC has used its authority under § 5 of the Federal Trade Commission Act[2] (FTC Act) to enforce the prohibition against unfair and deceptive acts or practices in the field of data security. In evaluating whether a company's data security practices are unfair, the FTC uses a reasonableness standard and considers each company's data security practices on a case-by-case basis. The majority of the FTC's data security enforcement actions have resulted in settlements. However, for the first time, the FTC is facing a challenge to its authority to regulate companies' data security practices.

Companies also face challenges to their data security programs under California law. The California Attorney General has made it clear that investigating breaches of personal information is an enforcement priority. Further, companies that experience data breach incidents face the additional burden of private lawsuits. Even though litigants bringing data security lawsuits have faced hurdles establishing constitutional standing under Article III and have had difficulty establishing a quantifiable harm, companies have chosen to settle these cases for significant sums.

Companies that store, transmit, and use consumer information would be well-advised to reassess their data security practices to reduce the likelihood of data breaches and to avoid costly regulatory and private litigations that may arise following a breach.

The FTC's Enforcement of Reasonable Data Security Practices

The FTC Evaluates Reasonableness of Data Security Practices on a Case-by-Case Basis

Pursuant to § 5 of the FTC Act, Congress delegated broad authority to the FTC to protect consumers from unfair and deceptive trade practices.[3] Under § 5 of the FTC Act, an act or practice is unfair if the act or practice: (1) "causes or is likely to cause substantial injury to consumers," (2) "is not reasonably avoidable by consumers themselves," and (3) is "not outweighed by countervailing benefits to consumers or to competition."[4] The FTC assesses these three factors whenever it examines whether a particular practice is "unfair."[5]

In the context of evaluating a company's data security practices, the FTC has held that a company's failure to implement reasonable data security practices can be considered an unfair practice under this three-part standard.[6] First, the FTC has stated that failing to reasonably protect consumers' personal and financial information can cause significant injury to consumers.[7] Such failures increase the likelihood of unauthorized charges to consumers' financial accounts and put consumers at an increased risk of identity theft. Second, the FTC has stated that consumers cannot reasonably avoid such harms because the consumer has no way of independently knowing whether the company has unreasonable security practices and turning over confidential financial and personal information generally is required of a consumer to complete a transaction with a company.[8] Third, the FTC has stated that when a company employs unreasonable data security practices and does not implement low-cost technologies that reduce the risk of data breaches, harm to consumers caused by a company's unreasonable data security practices is not

Kathryn F. Russo is a lawyer at Nelson Hardiman, LLP in Los Angeles, CA. The opinions set forth in this article are hers alone and do not necessarily reflect the positions of the firm or its clients. This article updates two articles published by *Competition*, the journal of the Antitrust and Unfair Competition Law Section of the State Bar of California [Vol. 23, No. 1 (Spring 2014) and Vol. 23, No. 2 (Fall 2014)].

outweighed by the countervailing benefits to consumers or to competition.[9] Although a hacker may devise a way to breach even the most expensive state-of-the-art data security measure, requiring onerous data security measures could raise costs to businesses, making them less competitive and ultimately harming consumers. Therefore, this factor is flexible and allows the FTC to determine whether a company's data security measures employed are sufficient, given the particular situation.

Accordingly, the FTC uses its authority under § 5 of the FTC Act to evaluate a company's data security practices on a case-by-case basis, considering the unique characteristics of the business, and current security threats and technology. In a statement before Congress, the FTC emphasized that "[i]n the data security context, the FTC conducts its investigations with a focus on reasonableness—a company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities."[10] In considering whether a company's data security practices are reasonable, the FTC "examines such factors as whether the risks at issue were well known or reasonably foreseeable, the costs and benefits of implementing various protections, and the tools that are currently available and used in the marketplace."[11] Further, the FTC stated that "it does not require perfect security; that reasonable and appropriate security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; and that the mere fact that a breach occurred does not mean that a company has violated the law."[12]

The FTC stated that "it does not require perfect security; that reasonable and appropriate security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; and that the mere fact that a breach occurred does not mean that a company has violated the law."

The FTC has undertaken efforts to provide guidance to companies in developing reasonable data security programs. The FTC publically publishes its complaints and consent decrees related to its data security enforcement actions.[13] Additionally, the FTC holds workshops on issues that affect consumer data. Its recent workshops included a workshop on Big Data,[14] the Internet of Things,[15] mobile security issues,[16] and child identity theft.[17] Further, the FTC published a business guide on data security with the goal of helping companies develop reasonable data security programs.[18] Companies should review the consent decrees, workshops, and other guidance published by the FTC to help assess whether their data security program is reasonable.

The FTC Is Pursuing Data Security Enforcement Actions under the Unfairness Prong

For more than a decade, the FTC has used its authority under § 5 of the FTC Act to enforce the prohibition against unfair and deceptive acts or practices in the field of consumer privacy and data security. Initially, the FTC focused its enforcement efforts on companies' "deceptive" data security practices.[19] In 2005, the FTC began pursuing enforcement actions against companies engaging in "unfair" data security practices.[20]

Companies should expect and be prepared for the FTC to continue to aggressively pursue actions against businesses that engage in unfair data security practices. The FTC released a report stating that it has "redoubled its efforts to protect consumer privacy, including through law enforcement . . . ."[21] Further, on January 31, 2014, the FTC issued a statement marking its 50th data security settlement.[22] More than 20 of these settlements included allegations that a company's failure to reasonably safeguard consumer data was an unfair practice.[23]

Companies should be aware that the majority of the FTC's data security investigations have resulted in consent decrees. In the context of data security actions, the FTC's consent decrees typically require a company to establish, implement, and maintain a comprehensive information security program and to obtain, on a biannual basis, an assessment and report from a third-party professional regarding the company's data security safeguards for a period of time ranging from 10 to 20 years.[24] However, two companies recently challenged the FTC's authority to regulate companies' data security practices as described below.

FTC's Authority to Regulate Data Security Practices Challenged

Although the majority of the FTC's data security investigations have resulted in consent decrees, recently, two companies, LabMD Inc. and Wyndham Worldwide Corporation and three of its subsidiaries, are challenging the FTC's authority to regulate data security practices of businesses.[25] Both LabMD and Wyndham argue that the FTC lacks authority to regulate companies' data security practices under § 5 of the FTC Act, and that the FTC has failed to provide fair notice of what constitutes

reasonable data security standards.[26] As discussed below, in a landmark decision, the court denied Wyndham's motion to dismiss,[27] which marks the first time a federal court has held that the FTC has authority under § 5 of the FTC Act to enforce the prohibition against unfair and deceptive acts or practices in the field of data security. Additionally, the FTC issued an order in the LabMD case affirming its authority under the FTC Act to regulate and enforce data security practices of businesses.[28]

FTC v. Wyndham Worldwide Corporation, et al.

In August 2012, the FTC brought an action[29] against Wyndham Worldwide Corporation and three of its subsidiaries pursuant to § 5 of the FTC Act[30] alleging Wyndham violated § 5(a)'s prohibition of "acts or practices in or affecting commerce" that are "unfair" or "deceptive." The FTC alleged that Wyndham's failure to maintain reasonable and appropriate data security standards for consumers' sensitive personal information allowed hackers to gain unauthorized access to Wyndham's computer networks on three occasions and resulted in "more than $10.6 million in fraud loss, and the export of hundreds of thousands of consumers' payment card account information to a domain registered in Russia."[31] Specifically, the FTC alleged that Wyndham (1) failed to use firewalls; (2) stored payment card information in clear readable text; (3) failed to implement adequate information security policies and procedures; (4) failed to remedy known security vulnerabilities; (5) used default user IDs and passwords; (6) did not require the use of complex passwords; (7) failed to adequately inventory computers; (8) failed to employ reasonable measures to detect and prevent unauthorized access to computer networks; (9) failed to follow proper incident response procedures; and (10) failed to adequately restrict third-party vendors' access to Wyndham's network.[32] The FTC alleged that taken together, such data security failures unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft.[33] Further, the FTC argued that such unreasonable exposure has caused and is likely to cause substantial injury to consumers and businesses.[34] For example, the FTC stated that consumers and businesses suffered financial injury including, "unreimbursed fraudulent charges, increased costs, and lost access to funds or credit."[35] Based on Wyndham's alleged unfair and deceptive acts and practices in violation of § 5, the FTC requested that the court enter a permanent injunction and grant other relief the court deemed proper.[36]

Wyndham's Motion to Dismiss

In response to the FTC's complaint, Wyndham filed a motion to dismiss arguing, among other things, that (1) the FTC lacks authority to regulate data security under § 5 of the FTC Act, (2) the FTC failed to provide fair notice of what constitutes reasonable data security standards, and (3) § 5 does not govern the security of payment card data.[37]

First, Wyndham argued that the FTC's unfairness authority under § 5 of the FTC Act does not extend to the regulation of data security practices of private companies.[38] Wyndham equated the FTC's action with *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000).[39] In *Brown & Williamson*, the US Supreme Court held that Congress did not grant the US Food and Drug Administration (FDA) jurisdiction to regulate tobacco products and stated, "if tobacco products were within the FDA's jurisdiction, the Act would require the FDA to remove them from the market entirely. But a ban would contradict Congress' clear intent as expressed in its more recent, tobacco-specific legislation."[40] Wyndham contended that akin to *Brown & Williamson*, since the enactment of the FTC Act, Congress has "settled on 'a less extensive regulatory scheme' and passed narrowly tailored legislation."[41] Wyndham cited various laws including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), the Children's Online Privacy Protection Act (COPPA), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as evidence that the FTC lacks general authority under § 5 to regulate data security practices.[42] Additionally, Wyndham argued that in light of pending cybersecurity legislation and the "important economic and political considerations involved in establishing data-security standards for the private sector ... it defies common sense to think that Congress would have delegated that responsibility to the FTC ...."[43] Further, Wyndham contended that like the FDA in *Brown & Williamson*, the FTC disclaimed its authority to regulate data security under its § 5 unfairness authority on various occasions.[44]

Second, Wyndham argued that even if the FTC has authority under § 5 of the FTC Act to regulate data security standards for private companies, Wyndham cannot be held liable because the FTC did not provide fair notice of what § 5 requires.[45] Wyndham argued that fair notice requires the FTC to publish data security rules and regulations establishing guidance and performance measures for companies to follow.[46] Wyndham stated, "[b]ecause the FTC has not published any rules, regulations, or other guidelines explaining what data-security practices the Commission believes Section 5 to forbid or require, it would violate basic principles of fair notice and due process to hold [Wyndham] liable in this case."[47] Additionally, Wyndham argued that agencies in general "cannot use enforcement actions simultaneously

to make new rules and to hold a party liable for violating the newly announced rule."[48] In sum, Wyndham argued that the FTC would have to promulgate data security rules before holding Wyndham liable for any violations of § 5 related to data security.

Third, Wyndham argued that § 5 does not govern the security of payment card data.[49] Pursuant to § 5, an act or practice is unfair if the act or practice "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[50] Wyndham argued that consumer injury from the theft of payment card data is "never substantial and always avoidable" because federal law limits a consumer's liability for unauthorized use of payment card data to $50 and all major credit card brands waive liability for any unauthorized charges.[51] Wyndham argued that because the injury posed by the theft of payment card data is not substantial and is reasonably avoidable by consumers themselves, the FTC cannot meet the unfairness requirements under § 5 in its current action.

The District Court's Order Denying Wyndham's Motion to Dismiss

On April 7, 2014, the US District Court for the District of New Jersey denied Wyndham's motion to dismiss and held, among other things, that (1) the FTC has authority pursuant to § 5 of the FTC Act to assert an unfairness claim in the data security context, (2) the FTC provided fair notice of what constitutes an unfair data security practice and is not required to issue regulations before bringing an unfairness claim, and (3) the FTC's complaint sufficiently pled an unfairness claim under the FTC Act.[52]

First, the court rejected Wyndham's claim that this case is analogous to *Brown & Williamson*.[53] The court stated that unlike *Brown & Williamson*, where Congress acted to preclude the FDA from exercising its authority in the area of tobacco products, "[h]ere, subsequent data-security legislation seems to complement—not preclude—the FTC's authority."[54] The court stated that statutes such as the FCRA, the GLBA, and the COPPA grant the FTC tools in addition to its authority under § 5.[55] Indeed, the court stated, "the FTC's unfairness authority over data security can coexist with the existing data-security regulatory scheme."[56] Further, the court analyzed the statements put forth by Wyndham as evidence that the FTC disclaimed its authority to regulate data security. Following an analysis of these statements, the court made clear that it was "not convinced" that the statements made by the FTC "equate to a resolute, unequivocal position under *Brown & Williamson* that the FTC has no authority to bring any unfairness claim involving data security."[57] The court, guided by precedent, rejected Wyndham's arguments and concluded that the FTC has authority pursuant to § 5 to assert an unfairness claim in the data security context.

Second, the court rejected Wyndham's claim that fair notice requires the FTC to formally issue rules and regulations before it can file an unfairness claim in the data security context.[58] The court stated, "Circuit Courts of Appeal have affirmed FTC unfairness actions in a variety of contexts without preexisting rules or regulations specifically addressing the conduct-at-issue."[59] Additionally, the court stated that requiring the FTC to publish rules and regulations before bringing an enforcement action would "require the Court to sidestep longstanding precedent," including the Third Circuit's affirmation that the FTC has discretion as to whether it pursues ad hoc litigation or regulation.[60] Further, the court stated that it was not persuaded by Wyndham's argument that regulations are the only means of providing sufficient fair notice, and cited the three-prong test of § 5, which defines what constitutes an unfair act or practice.[61] The court also pointed to the FTC's "many public complaints and consent agreements" as a "body of experience and informed judgment to which courts and litigants may properly resort for guidance."[62] The court concluded that accepting Wyndham's argument that the FTC must promulgate rules and regulations before bringing unfairness actions is untenable and would produce a result that is "in direct contradiction with the flexibility necessarily inherent in Section 5 of the FTC Act."[63]

The court concluded that accepting Wyndham's argument that the FTC must promulgate rules and regulations before bringing unfairness actions is untenable and would produce a result that is "in direct contradiction with the flexibility necessarily inherent in Section 5 of the FTC Act."

Third, the court held that the FTC's complaint sufficiently pled an unfairness claim under the FTC Act.[64] An act or practice is unfair if it (1) "causes or is likely to cause substantial injury to consumers," (2) "is not reasonably avoidable by consumers themselves," and (3) is "not outweighed by countervailing benefits to consumers or to competition."[65] The court found that the FTC adequately pled the "substantial injury" requirement because the FTC alleged that some consumers suffered financial injury.[66] Additionally, the court found that the FTC adequately pled that the alleged substantial injury

was "not reasonably avoidable" and stated that this issue is fact-dependent.[67]

Wyndham's Interlocutory Appeal to the Third Circuit

Following the district court's order denying Wyndham's motion to dismiss, Wyndham immediately filed a motion to certify the order for interlocutory appeal to the Third Circuit.[68] The district court, noting the "novelty of liability issues relating to data-security breaches" and "the nationwide significance of the issues," granted Wyndham's request for interlocutory appeal.[69] The district court certified the following two questions to the Third Circuit: (1) whether the FTC can bring an unfairness claim involving data security under § 5 of the FTC Act; and (2) whether the FTC must formally promulgate regulations before bringing its unfairness claim under § 5 of the FTC Act.[70] On March 3, 2015, the Third Circuit held oral argument on this appeal. If the Third Circuit reverses the district court as to either of these controlling questions of law, the trial will be limited to the FTC's deception count.[71]

In the Matter of LabMD, Inc.

In the *LabMD* case, the FTC filed an administrative complaint against LabMD, alleging that it "engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks."[72] LabMD is a clinical laboratory that conducts tests on specimen samples from patients and reports the test results to patients' health care providers.[73] In conducting such tests, LabMD obtains a variety of types of sensitive personal information about patients.[74] The FTC alleged that as a result of LabMD's security failures, a file containing the personal information of approximately 9,300 patients was shared to a public file-sharing network, Limewire.[75] LabMD filed a motion to dismiss the FTC's complaint, arguing, among other things, that the FTC lacks authority to regulate companies' data security practices under § 5 of the FTC Act and that the FTC failed to provide fair notice of what constitutes reasonable data security standards.[76]

The FTC's Order Denying LabMD's Motion to Dismiss

On January 16, 2014, the FTC issued an order denying LabMD's motion to dismiss and held, among other things, that the FTC Act's prohibition of "unfair ... acts or practices" applies to a company's failure to implement reasonable and appropriate data security measures.[77] In support of its holding, the FTC referenced Congress' intent to delegate broad authority to the FTC to proscribe activities that qualify as "unfair acts or practices," as well as the FTC's long history of applying the three "unfairness" factors to prohibit a wide range of unfair acts and practices.[78] The FTC also rejected LabMD's due process arguments that the FTC must first adopt regulations before bringing enforcement actions in the field of data security.[79] In support of its holding, the FTC reasoned that the three-part statutory standard governing whether an act or practice is unfair provides fair notice of what conduct is prohibited. The FTC also highlighted the fact that companies are subject to tort liability for violating uncodified standards of care on a regular basis.[80]

In support of its holding, the FTC reasoned that the three-part statutory standard governing whether an act or practice is unfair provides fair notice of what conduct is prohibited.

The FTC's Grant of Immunity and Evidentiary Hearing

On December 29, 2014, the administrative law judge in the LabMD case granted immunity to an ex-employee of the security firm Tiversa, who provided key evidence to the FTC in its case against LabMD, and set an evidentiary hearing for March 3, 2015, which was subsequently rescheduled to May 5, 2015.[81] The ex-employee of Tiversa is expected to give testimony calling into question the FTC's argument that LabMD failed to provide reasonable and appropriate security for personal information on its computer networks.

The California Attorney General and Data Security Enforcement Actions

The Unfair Competition Law and Data Security

Pursuant to California's unfair competition law, any "unlawful, unfair or fraudulent business act or practice" is prohibited.[82] The California Supreme Court has affirmed that an act or practice may be independently actionable as "unfair," even if the act or practice is "not specifically proscribed by some other law."[83] In the context of consumer cases, there is a three-way split among the courts as to what definition of "unfair" should be applied.[84]

First, some courts apply the definition of unfair set forth in the California Supreme Court's *Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.*[85] decision. In *Cel-Tech*, the California Supreme Court stated that in competitor cases "unfair" should apply to "conduct that threatens an incipient violation of an antitrust law, or violates the policy or spirit of one of

those laws because its effects are comparable to or the same as a violation of the law, or otherwise significantly threatens or harms competition."[86]

In the context of consumer cases, there is a three-way split among the courts as to what definition of "unfair" should be applied.

Second, some courts apply the accepted definition of unfair business practice in place before the *Cel-Tech* decision, which is that "an 'unfair' business practice occurs when that practice 'offends an established public policy or when the practice is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers.'"[87] Typically, a broad balancing test is used to determine whether a practice is unfair under this definition. Third, some California courts of appeal have applied the FTC's three-prong definition of unfair as described above.[88]

As discussed above, the FTC has interpreted its three-prong unfairness test, which generally is regarded as the most restrictive of the three possible tests for unfairness under unfair competition law,[89] as covering lax data security practices that result in breaches. Because even the most restrictive test under the law has been interpreted to cover unreasonable data security practices that result in breaches, the question regarding which unfairness test should be applied would likely not change the outcome. Under any of these tests, unreasonable data security practices likely expose companies to potential liability under unfair competition law. Therefore, companies should take care to ensure that their data security practices would not be deemed unfair under any of the three standards. Additionally, companies should be aware that the California Customer Records Act requires a business that owns or licenses personal information about a California resident to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[90] Although there have not been many actions brought alleging violations of this statutory provision, companies should make sure that they are maintaining reasonable and appropriate security procedures as a precautionary measure.

The Attorney General Has Made Investigating Data Breaches an Enforcement Priority

The California Attorney General has made clear that investigating breaches of personal information is an enforcement priority. In July 2012, the California Attorney General announced the creation of the Privacy Enforcement and Protection Unit in the Department of Justice, which focuses on "protecting consumer and individual privacy through civil prosecution of state and federal privacy laws."[91] The Data Breach Report released by the California Attorney General in July 2013, found that "[m]ore than 2.5 million Californians were put at risk by data breaches in 2012" and "[m]ore than 1.4 million Californians would not have been put at risk, and 28 percent of the data breaches would not have required notification, if the data had been encrypted."[92] Additionally, in October 2014, the California Attorney General released a report that found in 2013 there was a 28 percent increase in reported data breaches and a 600 percent increase in total records of California residents that were put at risk.[93] The California Attorney General's Office stated that it "will make it an enforcement priority to investigate breaches involving unencrypted personal information, and encourage [their] allied law enforcement agencies to similarly prioritize these investigations."[94] Further, the Attorney General's data breach report states, "[c]ompanies and agencies have legal and moral obligations to protect personal information with reasonable and appropriate safeguards."[95]

Companies that store, transmit, and use consumer information about Californians should reassess their data security programs to make sure they include reasonable and appropriate safeguards for personal information.

Companies that store, transmit, and use consumer information about Californians should reassess their data security programs to make sure they include reasonable and appropriate safeguards for personal information. On January 24, 2014, the California Attorney General's office filed a complaint in state court against the Kaiser Foundation Health Plan, Inc. alleging Kaiser violated California's unfair competition law.[96] Specifically, the complaint alleges that Kaiser violated the law by publicly posting and displaying the Social Security numbers of more than 20,000 Californians on an unencrypted hard drive, in violation of California Civil Code § 1798.85, and delayed notification of security breach in violation of California Civil Code § 1798.82.[97] The California Attorney General's action against Kaiser highlights the growing trend of state attorneys general increasing their role in protecting consumers' data privacy and security. Companies should expect more data security enforcement actions to come and should take

care to ensure their data security practices do not run afoul of California law.

Private Data Security Actions

In addition to state and federal regulatory enforcement actions, companies that experience data breach incidents may face the additional burden of private lawsuits. The data breach class actions brought to date usually arise from an unauthorized third party gaining access to a company's stored data and involve claims that the company failed to properly secure such data. Litigants bringing data breach lawsuits have faced hurdles establishing constitutional standing under Article III and have had difficulty establishing a quantifiable harm. Even in the face of these difficulties, plaintiffs have still brought data breach cases against companies that result in settlement due to the enormous cost of litigation.[98]

Practitioners and companies should take note of the Ninth Circuit's decision in *Krottner v. Starbucks Corp.* in which the court held that "Plaintiffs-Appellants, whose personal information has been stolen but not misused, have suffered an injury sufficient to confer standing under Article III, Section 2 of the U.S. Constitution."[99] A recent class action lawsuit, *In re Sony Gaming Networks & Customer Data Sec. Breach Litigation*,[100] arising out of criminal intrusion into a computer network system, cited *Krottner* and held that the defendants established Article III standing because the plaintiffs sufficiently alleged a loss of money or property as a result of the defendants' alleged unfair business practices. The court stated, "... where sensitive personal data, such as names, addresses, social security numbers and credit card numbers are improperly disclosed or disseminated into the public, increasing the risk of future harm, injury-in-fact has been recognized."[101] Further, the court held that "even though Sony alleges no harm has yet occurred, in certain circumstances,... future harm may be regarded as a cognizable loss sufficient to satisfy Article III's injury-in-fact requirement."[102]

Following the *Krottner* and *Sony* decisions, the US Supreme Court held in a non-data security related case, *Clapper v. Amnesty International USA*,[103] that the plaintiffs "lack Article III standing because they cannot demonstrate that the future injury they purportedly fear is certainly impending and because they cannot manufacture standing by incurring costs in anticipation of non-imminent harm."[104] Although *Clapper* is not a data security case, the reasoning behind the decision is likely to be used to argue that plaintiffs alleging future harm resulting from data breaches is not sufficient for purposes of Article III standing.

Indeed, the Supreme Court's recent decision in *Clapper* was raised to challenge the plaintiffs' Article III standing in the *Sony* case.[105] In light of the *Clapper* decision, the district court reconsidered its prior ruling that the plaintiffs had sufficiently alleged that their sensitive personal information was wrongfully disseminated, increasing the risk of future harm, regardless of whether actual harm had occurred.[106] After reconsidering its prior ruling, the district court rejected Sony's argument that *Clapper* tightened the "injury-in-fact" analysis set forth by the Ninth Circuit in *Krottner*.[107] Instead, the district court found that "although the Supreme Court's word choice in *Clapper* differed from the Ninth Circuit's word choice in *Krottner*, stating that the harm must be 'certainly impending,' rather than 'real and immediate,' the Supreme Court's decision in *Clapper* did not set forth a new Article III framework, nor did the Supreme Court's decision overrule previous precedent requirement that the harm be 'real and immediate."[108] The district court stated, "the Supreme Court's decision in *Clapper* simply reiterated an already well-established framework for assessing whether a plaintiff had sufficiently alleged an 'injury-in-fact' for purposes of establishing Article III standing."[109] On July 10, 2014, preliminary settlement was reached in the *Sony* case.[110]

Although the plaintiffs in *Sony* survived the defendants' motion to dismiss, the question remains as to whether the plaintiffs could have established the required quantifiable harm to succeed. Even if such lawsuits ultimately are untenable, the cost of litigation represents a real threat to businesses that store, use, and transmit consumer information.

With the FTC and the California Attorney General declaring it a priority to pursue data security enforcement actions, companies can expect to see more enforcement actions in the near future.

Conclusion

With the FTC and the California Attorney General declaring it a priority to pursue data security enforcement actions, companies can expect to see more enforcement actions in the near future. Companies should take a proactive approach and assess whether their data security practices are reasonable and appropriate given their unique circumstances. Companies should make use of the resources provided by the FTC and the California Attorney General's office to assist them in protecting themselves against costly regulatory and private actions.

Notes

1. *See* Bureau of Justice Statistics, Victims of Identity Theft, 2012 (Dec. 2013), available at *http://www.bjs.gov/content/pub/pdf/vit12.pdf.*
2. 15 U.S.C. § 45(a)(1).
3. *Id.*
4. 15 U.S.C. § 45(n); FTC v. Neovi, Inc., 604 F.3d 1150, 1153 (9th Cir. 2010).
5. FTC Policy Statement on Unfairness, *appended to* Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984), *available at http://www.ftc.gov/ftc-policy-statement-on-unfairness.* Of course, to the extent that a company has made an explicit promise to protect consumers' personal and financial information and then fails to protect that information, such action constitutes a misrepresentation that can be challenged under the FTC Act's prohibition against "deceptive acts or practices."
6. *See* In the Matter of LabMD, Inc., Order Denying Respondent LabMD's Motion To Dismiss (January 16, 2014) (LabMD Order).
7. *See* LabMD Order *supra* n.6 at 18-19.
8. *See id.* at 19.
9. *Id.*
10. Prepared Statement of the Federal Trade Commission, "Protecting Consumer Information: Can Data Breaches Be Prevented?" before the Committee on Energy and Commerce, February 5, 2014, (2014 Commission Testimony), available at *http://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federal-trade-commission-protecting-consumer-information-can-data-breaches-be/140205databreaches.pdf.*
11. *Id.* at 4.
12. *Id.*
13. *See http://business.ftc.gov/legal-resources/8/35.*
14. FTC Workshop, "Big Data: A Tool for Inclusion or Exclusion?" (Sept. 15, 2014), available at *http://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion.*
15. FTC Workshop, "Internet of Things: Privacy & Security in a Connected World" (Nov. 19, 2013), available at *http://www.ftc.gov/bcp/workshops/internet-of-things/. See also* FTC Staff Report, "Internet of Things, Privacy & Security in a Connected World," January 2015 available at *http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.*
16. FTC Workshop, "Mobile Security: Potential Threats and Solutions" (June 4, 2013), available at *http://www.ftc.gov/bcp/workshops/mobile-security/.*
17. FTC Workshop, "Stolen Futures: A Forum on Child Identity Theft" (July 12, 2011), available at *http://www.ftc.gov/news-events/events-calendar/2011/07/stolen-futures-forum-child-identity-theft.*
18. *See* "Protecting Personal Information: A Guide for Business," available at *http://www.business.ftc.gov/documents/bus69-protecting-personal-information-guide-business.*
19. *See* LabMD Order *supra* n.6 at 9.
20. *Id.*
21. FTC Report, "Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers," (March 2012), available at *http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.*
22. Commission Statement Marking the FTC's 50th Data Security Settlement, (Jan. 31, 2014), available at *http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.*
23. 2014 Commission Testimony *supra* n.10 at 3-4.
24. *See, e.g.*, Dave & Busters, Inc., No. C-4291 (F.T.C. May 20, 2010), available at *http://www.ftc.gov/sites/default/files/documents/cases/2010/06/100608davebustersdo.pdf*; BJ's Wholesale Club, Inc., No. C-4148 (F.T.C. Sept. 20, 2005), available at *http://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305do0423160.pdf*; DSW Inc., No. C-4157 (F.T.C. March 7, 2006), available at *http://www.ftc.gov/sites/default/files/documents/cases/2006/03/0523096c4157dswdecisionandorder.pdf.*
25. Federal Trade Commission v. Wyndham Worldwide Corporation, *et al.*, Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC (D. N.J. Apr. 26, 2013) (Wyndham Motion to Dismiss); *In the Matter of LabMD, Inc.*, Respondent LabMD, Inc.'s Motion to Dismiss Complaint With Prejudice and to Stay Administrative Proceedings (Nov. 12, 2013) (LabMD Motion to Dismiss).
26. *See id.*
27. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D. N.J. 2014).
28. *See* LabMD Order *supra* n.6.
29. *See* Federal Trade Comm'n v. Wyndham Worldwide Corp., *et al.*, First Amended Complaint for Injunctive and Other Equitable Relief, (D. Ariz. Aug. 9, 2012) (Wyndham Complaint).
30. 15 U.S.C. § 45(a).
31. Wyndham Complaint *supra* n.29 at ¶ 2.
32. *Id.* ¶ 24.
33. *Id.*
34. *Id.* ¶ 40.
35. *Id.*
36. *Id.* at p. 20.
37. *See* Wyndham Motion to Dismiss *supra* n.25.
38. *Id.* at 7.
39. *Id.* at 7-8, 14.
40. FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 143 (2000).
41. Wyndham Motion to Dismiss *supra* n.25 at 14.
42. *Id.* at 9.
43. *Id.* at 13.
44. *Id.* at 10.
45. *Id.* at 14.
46. *Id.* at 15.
47. *Id.*

48. *Id.*
49. *Id.* at 19.
50. 15 U.S.C. § 45(n).
51. Wyndham Motion to Dismiss *supra* n.25 at 19.
52. *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D. N.J. 2014).
53. *Id.* at 607.
54. *Id.* at 613.
55. *Id.*
56. *Id.*
57. *Id.* at 614.
58. *Id.* at 615.
59. *Id.* at 618.
60. *Id.* at 619.
61. *Id.* at 619-620; *see* 15 U.S.C. § 45(n).
62. *Wyndham Worldwide*, 10 F. Supp. 3d 602 at 621.
63. *Id.*
64. *Id.* at 622.
65. 15 U.S.C. § 45(n).
66. *Wyndham Worldwide*, 10 F. Supp. 3d 602 at 622-623.
67. *Id.* at 625.
68. Federal Trade Comm'n v. Wyndham Worldwide Corp., *et al.*, Defendant's Notice of Motion to Certify Order Denying Motion to Dismiss for Interlocutory Appeal (D. N.J. April 17, 2014).
69. Federal Trade Comm'n v. Wyndham Worldwide Corp., *et al.*, Memorandum Opinion and Order (D. N.J. June 23, 2014) (Interlocutory Appeal Order).
70. Interlocutory Appeal Order at 9-10.
71. *Id.* at 8.
72. In the Matter of LabMD, Inc., Complaint, ¶ 10 (August 28, 2013) (LabMD Complaint).
73. *Id.* ¶3.
74. *Id.* ¶6.
75. *Id.* ¶17-19.
76. *See* LabMD Motion to Dismiss *supra* n.25.
77. LabMD Order *supra* n.6 at 2.
78. *Id.* at 3-6.
79. *Id.* at 2.
80. *Id.* at 17.
81. *See* In the Matter of LabMD, Inc., Order Granting Respondent's Renewed Motion For Order Requiring Testimony Under Grant Of Immunity Pursuant To Commission Rule 3.39(b)(2) (December 29, 2014); In the Matter of LabMD, Inc., Order Rescheduling Resumption of Evidentiary Hearing (March 12, 2015).
82. Cal. Bus. & Prof. Code § 17200 et seq.
83. Cel-Tech Comm'ns, Inc., v. Los Angeles Cellular Tele. Co., 20 Cal. 4th 163, 180 (1999).
84. *See* Durell v. Sharp Healthcare, 183 Cal. App. 4th 1350, 1364 (2010); Morgan v. AT&T Wireless Servs. Inc., 177 Cal. App. 4th 1235, 1254-1255 (2009); Klein v. Chevron U.S.A., Inc., 202 Cal. App. 4th 1342, 1376 (2012).
85. *Cel-Tech*, 20 Cal. 4th 163.
86. *Id.* at 187.
87. State Farm Fire & Cas. Co. v. Superior Court, 45 Cal. App. 4th 1093, 1104 (1996).
88. *See Klein v. Chevron* at 1376.
89. *See* David L. Belt, "Should the FTC's Current Criteria for Determining 'Unfair Acts or Practices' Be Applied to State 'Little FTC Acts'?", 10-11, *The Antitrust Source*, (Feb. 2010).
90. California Civil Code § 1798.81.5(b).
91. *See* Press Release, "Attorney General Kamala D. Harris Announces Privacy Enforcement and Protection Unit" (July 19, 2012), available at *http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-privacy-enforcement-and-protection.*
92. Data Breach Report 2012, p. iii, Kamala D. Harris, Attorney General, California Department of Justice (2012 Data Breach Report), available at *http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2012data_breach_rpt.pdf?.*
93. California Data Breach Report October 2014, p. 4, Kamala D. Harris, Attorney General, California Department of Justice (2014 Data Breach Report), available at *http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf?.*
94. 2012 Data Breach Report *supra* n.92 at iv., 14.
95. *Id.* at 14.
96. The People of the State of California v. Kaiser Foundation Health Plan, Inc., Case No. RG14711370, Cal. Sup. Ct., Alameda Co. (January 24, 2014).
97. *Id.*
98. *See* Johansson-Dohrmann v. CBR Sys., 2013 WL 3864341 (S.D. Cal. July 24, 2013); In re TD Ameritrade Account Holder Litig., 2011 WL 4079226 (N.D. Cal. Sept. 13, 2011).
99. Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010).
100. In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942 (S.D. Cal. 2012).
101. *Id.*, 903 F. Supp. 2d at 958.
102. *Id.*
103. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).
104. *Id.* at 1155.
105. *See* In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942 (S.D. Cal. 2014).
106. *Id.* at 960.
107. *Id.* at 961.
108. *Id.*
109. *Id.*
110. *See* In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 2014 WL 7800046 (S.D. Cal July 10, 2014).