Consumer Data Privacy Class Actions, Coming to a Jurisdiction Near You

March 4, 2014
Jennifer Furey and Matthew Horvitz

Do you accept credit cards? It is the rare business, organization, or institution that answers this question in the negative. The prevalence of electronic payment and credit card transactions has fueled an explosion in the volume, collection, and usage of consumer data. This data is also the target of criminal efforts to steal and exploit personal information about consumers. Today's headlines are filled with stories about large-scale data breaches and mounting evidence that some electronic payment and information management systems lack adequate security.

The boom in the collection of consumer data has been accompanied with a recent surge of consumer privacy class actions. This developing litigation trend underscores the need for businesses to take aggressive and proactive steps now, *before* receiving a complaint from an enterprising plaintiff's attorney or an investigative subpoena from a state attorney general.

Consumer Privacy Litigation

The recent proliferation of consumer privacy litigation emanates from the California Supreme Court's 2011 ruling in *Pineda v. Williams-Sonoma Stores, Inc.* Many companies collect ZIP codes in connection with credit card transactions and use that information for marketing and analysis purposes. In *Pineda*, the court held in a matter of first impression that the collection of ZIP codes from consumers violated the Song-Beverly Credit Card Act, Cal. Civ. Code § 1747.08. This statute forbids businesses from requesting or recording consumers' "personal identification information" in connection with credit card transactions. In the wake of this decision, California experienced a deluge of consumer privacy class actions.

Massachusetts was the next jurisdiction to experience a wave of consumer privacy class actions. Massachusetts General Laws Chapter 93, Section 105(a) provides that, when accepting credit card payments, a merchant cannot record the credit card holder's personal identification information or demand that the credit card holder provide personal identification information, unless that information is required by the credit card issuer to process the transaction or necessary to complete the transaction. Violations of this statute are also violations of Massachusetts' Consumer Protection Act, Gen. Laws Chapter 93A, which allows for the recovery of attorneys' fees and treble damages. Even when violations and resulting harms are not quantifiable, nominal damages are available in the amount of $25 per violation.

In 2013, the Supreme Judicial Court (SJC), the highest court in Massachusetts, followed the *Pineda* decision in *Tyler v. Michael's Stores, Inc.* The SJC held that ZIP codes requested by merchants in

credit card transactions constituted personal identification information and could support claims under Section 105(a) and Chapter 93A. Like the decision of the California Supreme Court in *Pineda*, the *Tyler* decision has prompted a surge of consumer data privacy class actions. We have followed this proliferation of consumer privacy litigation. In less than one year, there have been at least fifteen separate class actions filed in Massachusetts alleging violations based on the alleged improper collection and use of consumers' personal identification information.[1]

Next stop...

Which is the next state that will be targeted by class action attorneys or state attorney general investigations? Other jurisdictions have laws similar to **California** and **Massachusetts** regulating the use of personal identifying information in credit card transactions, including: **Delaware** (Del. Code tit. 11, § 914), the **District of Columbia**[2] (D.C. Code § 47-3153), **Georgia** (O.C.G.A. § 10-1-393.3), **Kansas** (Kan. Stat. § 50-669a), **Maryland** (Md. Code Com. Law § 13-317), **Minnesota** (Minn. Stat. § 325F.982), **Nevada** (NRS § 597.940), **New Jersey** (N.J. Stat. § 56:11-17), **New York** (N.Y. Gen. Bus. Law § 520-A(3)), **Ohio** (ORC Ann. 1349.17), **Oregon** (ORS § 646.894), **Pennsylvania** (69 P.S. § 2602), **Rhode Island** (R.I. Gen. Laws § 6-13-16), and **Wisconsin** (Wis. Stat. § 423.401). The purpose behind these statutes generally is to protect consumer privacy and prevent fraud. Given these statutes, creative plaintiffs' attorneys and ambitious attorney generals in other jurisdictions could seek to bring actions similar to *Pineda* and *Tyler* under their states' consumer protection statutes.

The experiences of businesses in California and Massachusetts provide a clear message that proactive measures should be taken now. If history and experience are any indicators, it is unlikely that plaintiffs' attorneys or attorney generals will ignore any potential consumer protection and class action litigation opportunities.

Take Proactive Measures

When is the last time your company conducted a thorough data privacy and security audit? The time to address compliance issues is now, *before* your company is named in a class action or targeted by an investigative subpoena. The resources needed to analyze data privacy and security issues are likely to be far less than the costs of litigating a consumer class action. We recommend partnering with knowledgeable counsel to audit your business practices and discuss an overall strategy which is specifically tailored to your needs and objectives.

Determining whether there is risk and how best to minimize such risk requires a careful analysis of a business's data collection practices. Information relevant to this analysis includes:

- What information do your brick-and-mortar locations collect from customers?
- What information do your e-commerce sites collect from customers?
- When is that information collected?
- Are consumers informed about this collection?
- How is that information stored and used?

- What information does your point-of-sale (POS) processing system require?
- Where is that information transmitted or stored?
- What type of data do you collect about customers?
- Is that data used for marketing or other purposes?
- Do you sell or share data about your customers with third parties?
- Do you have a company Privacy Policy or Terms of Use agreement?
- Is data collected consistent with these policies and terms of use?

Depending on your business requirements, there are a multitude of strategies that may help reduce risk. Companies may consider establishing opt-in procedures before collecting personal identification information. A well crafted and publicly available Privacy Policy or Terms of Use agreement may deter potential class action attorneys and attorney generals. Clear statements of company policy will also assist in qualifying for certain exemptions or safe harbors. Employee education and training about company practices and policies will ensure there is uniform compliance with company policies and practices. Any analysis of whether a particular strategy is appropriate necessarily requires an individualized and fact-intensive analysis.

Based on developing litigation trends, we recommend that companies take aggressive and proactive steps now, *before* receiving a complaint from an enterprising plaintiff's attorney or an investigative subpoena from a state attorney general.

For more information on this topic, please contact your usual Goulston & Storrs attorney, any of the attorneys in our Retail, Restaurant & Consumer group, or either of the following attorneys:

Jennifer Furey
(617) 574-3575
jfurey@goulstonstorrs.com

Matthew P. Horvitz
(617) 574-4053
mhorvitz@goulstonstorrs.com

---

[1] *Kokobaeva v. The Donna Karan Co. Store, LLC*, No. 1:13-cv-13272; *Alberts, et al. v. CVS Caremark Corp.*, No. 1:13-cv-12250; *Crohn v. DSW, Inc.*, No. 1:13-cv-12248; *Christensen, et al. v. Apple, Inc.*, No. 1:14-cv-10100; *Alberts, et al. v. Kohl's Dept. Stores, Inc.*, No. 1:13-cv-12523; *Alberts, et al. v. PetSmart, Inc.*, No. 1:13-cv-12261; *Alberts, et al. v. Paylerss Shoesource, Inc.*, No. 1:13-cv-12262; *Nielan v. Guitar Center, Inc.*, No. 1:13-cv-11284; *Pietrantonio v. Ann, Inc.*, No. 1:13-cv-12721; *Brenner v. Kohl's,* No. 1:13-cv-10935; *Brenner v. Williams Sonoma,* No. 13-cv-10931; *Tyler v. Bed Bath & Beyond, Inc.,* No. 13-cv-10639; *Whiting v. Bed Bath & Beyond, Inc.*, No. 1:13-cv-10714; *Monteferrante v. Restoration Hardware Holdings, Inc.,* No. 13-cv-10932; *Monteferrante v. The Container Store, Inc.,* No. 13-cv-11362; *Brenner v. J.C. Penney Co., Inc.*, No. 1:13-cv-11212; *D'Esposito v. Michaels Stores, Inc.*, No. 1:13-cv-106080.

[2] In *Hancock v. Urban Outfitters, Inc., et al.*, 1:13-cv-00939 (D.D.C. filed Jun. 21, 2013), plaintiffs asserted nearly identical claims to those asserted in *Pineda* and *Tyler*. In response to this complaint, the defendants filed a motion to dismiss based on D.C.'s specific statutory language. This motion remains pending.