Published on *The National Law Review* https://natlawreview.com

Divided NLRB Rules Employer Policy Protecting Customer Information Is Lawful

Article By:

Mark Theodore

Employers can prohibit the use by employees of the names, social security numbers and credit card numbers of customers in furtherance of organizational activities. If this seems like it should have been a foregone conclusion, a recent case from the NLRB shows how the agency's continued parsing of employer policies could easily have turned this notion on its head.

In Macy's, Inc., 365 NLRB No. 116 (August 14, 2017) a number of the employer's policies had been challenged as unlawful. Many of the policies were found to violate the Act. The employer, an operator of department stores, chose to appeal only one aspect of its policies: the Administrative Law Judge's findings that the employer's policies prohibiting the use of customer information were unlawful. The employer had three policies addressing use of customer information.

The first employer policy defined confidential information as follows:

> What is confidential information? It could be business or marketing plans, pricing strategies, financial performance before public disclosures, pending negotiations with business partners, information about employees, documents that show social security numbers or credit card numbers–in short any information, which if known outside the Company could harm the Company or its business partners customers or employees or allow someone to benefit from having this information before it is publicly known.
>
> Just as our Company requires that its own confidential information be protected, our Company also requires that the confidential information and proprietary information of others be respected. . .
>
> We are all trusted to maintain the confidentiality of such information and to ensure that the confidential information, whether verbal, written or electronic, is not disclosed except as specifically authorized. Additionally, it must be used only for the legitimate business of the Company.

The Company also maintained a “USE OF PERSONAL DATA” policy:

> The Company has certain personal data of its present and former associates, customers and vendors. It respects the privacy of this data and is committed to handling this data responsibly and using it only as authorized for legitimate business purposes.
>
> What is considered personal data? It is information such as names, home and office contact information, social security numbers, driver’s license numbers, account numbers and other similar data.

The Use of Personal Data policy stated that employees must follow all “policies and measures adopted by the Company for the protection of such data from unauthorized use, disclosure or access.”

Finally, the Company maintained a “CONFIDENTIALITY AND ACCEPTABLE USE OF COMPANY SYSTEMS” policy:

> Any information that is not generally available to the public that relates to the Company’s or the Company’s customers, employees, vendors, contractors, service providers, Systems etc., that you receive or which you are given access during your employment or while you are performing services for the Company is classified as ‘Confidential’ or ‘Internal Use Only.’

The employer’s Acceptable Use policy prohibited the sharing of such information with third parties.

The Charging Party union challenged these rules as unlawful, asserting that they would lead a “reasonable employee” to interpret them as prohibiting contact with customers during a labor dispute, something that is protected by the Act. Complaint issued.

The Administrative Law Judge’s Decision

The Judge, after discussion of the policies in general, found the restrictions related to customers violated Section 8(a)(1), noting that the General Counsel “challenges the restrictions on the use of information regarding customers and vendors. In certain situations, employees are permitted to use such information in furtherance of their protected concerted activities. . .” There was little discussion of the actual language of the policies other than to note that it referenced “customer” information and that such information might include that used for purposes of protected activity.

Board Majority Sees It Differently

A two person majority (Chairman Miscimarra and Member McFerran) concluded the policies related to use of customer information were lawful. The Board noted the policy identifying the information considered by the employer to be confidential “specifically defines” confidential information and the “only information covered by that rule that arguably relates to customers is ‘social security numbers or credit card numbers.’” The Board noted that the General Counsel had conceded that employees

do not have a right to use such information. As to the Use of Personal Data an Acceptable Use of Company Systems restrictions, the Board held both rules "limit the use or disclosure of customer names and contact information"–information that could arguably be used in a labor dispute, but that "such rules "by their terms, only apply to customer names and contact information obtained from the [employer's] own confidential records."

The Board then cited the numerous cases holding that employees who use information taken from employer systems are outside the protection of the Act, including one where the employee had forwarded hundreds of company emails, some of which included confidential data, to a personal email account.

In a footnote, Chairman Miscimarra reiterated his call, set forth in prior cases as a dissent, that the test as to whether an employee would "reasonably construe" certain language to infringe on rights should be overruled and repudiated by the courts as unworkable.

Dissent Interprets Policies As Restrictive

Member Pearce dissented, stating employees "would reasonably interpret these broad rules as prohibiting or restricting their disclosure and use of customer information, for all purposes, including those that may implicate their terms and conditions of employment." The dissent argued what many employers asserted in defense of handbook policies,– that the majority was reading phrases of the policies "in isolation," to come to its conclusion. Specifically, the dissent noted that the definition of confidential information included "any information, which if known outside the Company could harm the Company…." This phrase arguably isolates a few words while ignoring the more detailed definition preceding it.

Takeaways

This case is another example of how the standard of evaluating the lawfulness of language in a handbook can lead some very smart practitioners to come to widely disparate conclusions. Here we have four seasoned labor professionals (an ALJ and three Board members) coming to different conclusions. Indeed, the fact that the Chairman and Member McFerran were together in the majority is unusual enough (it's probably happened on a case like this only a handful of times) to show that reasonable minds can and do differ as to the meaning of certain policies. If these professionals cannot agree on what language constitutes a violation of the Act, then it certainly makes one wonder whether the "reasonable employee" who is envisioned in the standard would agree with any of the interpretations or hold a different view. It seems likely the standard will be changed in the coming months as the make-up of the Board changes.

Until then, the drafting rules that have helped employers avoid problems of this sort remain in effect. Tailor the policy to achieve the business objective. In this case, the definition of confidential information was very specific, and narrow. The types of information under the Use of Personal Data and Use of Company Systems policies were restricted, appropriately, to information that the employer collects as part of its business.

The case also offers an excellent recitation of all the instances where employee use of confidential information has been found to be unprotected.

National Law Review, Volume VII, Number 228