Macy's, Inc. ***and*** **United Food and Commercial Workers Union, Local 1445.** Case 01–CA–123640

August 14, 2017

DECISION AND ORDER

BY CHAIRMAN MISCIMARRA AND MEMBERS PEARCE AND MCFERRAN

On May 12, 2015, Administrative Law Judge Joel P. Biblowitz issued the attached decision. The Respondent filed exceptions[1] and a supporting brief, the General Counsel filed an answering brief, and the Charging Party filed an opposition to the exceptions.

The National Labor Relations Board has delegated its authority in this proceeding to a three-member panel.

The Board has considered the decision and the record in light of the exceptions and briefs and has decided to affirm the judge's rulings, findings, and conclusions only to the extent consistent with this Decision and Order.[2]

The Respondent has excepted only to the judge's finding and conclusion that the Respondent's rules prohibiting the use of customer information violate Section 8(a)(1). We find merit to this exception. While employees generally have a Section 7 right to appeal to their employer's customers for support in a labor dispute, the disputed rules do not restrict such appeals. Instead, they prohibit the disclosure of information about customers obtained from the Respondent's confidential records. For the reasons stated below, this prohibition does not violate the Act.

Facts

At issue here are the restrictions on use of customer information in the following rules. The relevant portions at issue are italicized.

CONFIDENTIAL INFORMATION

What To Know

Confidential information about our Company, its business, associates, customers and business partners should be protected. It can be used only to pursue the Company's business interests or to comply with the Company's legal or other obligations.

What is confidential information? It could be business or marketing plans, pricing strategies, financial performance before public disclosure, 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 and proprietary information of others be respected.

What To Do

In performing our duties, we as associates may have access to confidential information relating to our Company, its business, customers, business partners or our co-workers.

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.

Here are some simple rules to follow.

Confidential information should:

- Be stored in locked file cabinets or drawers and not be left where others can see it,
- Be clearly marked as confidential whenever possible,
- Be shared only with those who need to see it for Company business purposes,
- Not be sent to unattended fax machines or printers,
- Not be discussed where others may hear,
- Be shredded when no longer needed.

Always respect the confidentiality of the information of third parties. We must not use or disclose any of it ex-

[1] The Respondent does not except to the judge's findings that the Respondent violated Sec. 8(a)(1) by maintaining handbook rules prohibiting the use of information about employees, restricting use of the Respondent's logo, or requiring employees to notify the human resources department prior to participating in a government investigation.

[2] We shall modify the judge's recommended Order to conform to our findings and to *Guardsmark, LLC,* 344 NLRB 809, 812 (2005), enfd. in relevant part 475 F.3d 369 (D.C. Cir. 2007), and to provide for the posting of the notice in accordance with *J. Picini Flooring*, 356 NLRB 11 (2010). We shall substitute a new notice to conform to the Order as modified.

cept as authorized under a written agreement approved by our Law Department.

USE AND PROTECTION OF PERSONAL DATA

What To Know

The Company has certain personal data of its present and former associates, *customers* and vendors. It respects the privacy of this personal 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.

What To Do

We have a strict obligation to use such personal data in a manner that:

- respects the privacy of our co-workers and our Company's customers and vendors,
- complies with all applicable laws and regulations, and Company policies,
- upholds any confidentiality or privacy obligations of the Company in its contracts.

In addition, we must follow all policies and measures adopted by the Company for the protection of such data from unauthorized use, disclosure or access. If any of us becomes aware of any instance of data being accessed or being used in an unauthorized manner, we must report it immediately to our Divisional Security Administrator or the Law Department.

CONFIDENTIALITY AND ACCEPTABLE USE OF COMPANY SYSTEMS

The following standards and procedures apply to your use of, or access to, all Confidential Information.

1. All Non-Public Information is Sensitive

Any information that is not generally available to the public that relates to the Company or the Company' customers, employees, vendors, contractors, service providers, Systems, etc., that you receive or to 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" under the Macy's Information Security Policy. As is set forth in the Macy's Information Security Policy, internal access to Confidential Information should only be granted on a "need to know" basis, and such information should not be shared with third parties without prior approval from your Company supervisor and consultation with the Law Department.

. . .

3. Use and Protection of Personal Data

Company maintains certain information regarding its present and former associates, customers and vendors. Company respects the privacy of this data where it includes personally-identifiable information ("Personal Data"). Personal Data includes names, home and office contact information, social security numbers, driver's license numbers, account numbers and other similar data. Company is committed to handling Personal Data responsibly and using it only as appropriate for legitimate business purposes. This commitment requires that all Company employees, contractors, and third parties who are granted access to Personal Data by Company follow all policies adopted by the Company for the protection of such data against unauthorized use, disclosure or access. Such policies, including those set forth in the Macy's Information Security Policy, may vary depending on the sensitivity of the Personal Data at issue.

Personal Data may not be shared with any third party without the written approval of your senior Sales Promotion executive or, for support organizations, your Chief Executive Officer.

Judge's Decision

As pertinent here, the judge found that the rules violate Section 8(a)(1) insofar as they restrict the use of information regarding customers. He reasoned that employees have a Section 7 right to communicate with customers regarding matters affecting their employment, and he found that the rules were unlawful because they restrict such communications.

Analysis

"In determining whether a work rule violates Section 8(a)(1), the appropriate inquiry is whether the rule would reasonably tend to chill employees in the exercise of their Section 7 rights." *Lafayette Park Hotel*, 326 NLRB 824, 825 (1998), enfd. mem. 203 F.3d 52 (D.C. Cir. 1999). If the rule explicitly restricts Section 7 rights, it is unlawful. *Lutheran Heritage Village-Livonia*, 343 NLRB 646, 646 (2004). If it does not, "the violation is

dependent upon a showing of one of the following: (1) employees would reasonably construe the language to prohibit Section 7 activity; (2) the rule was promulgated in response to union activity; or (3) the rule has been applied to restrict the exercise of Section 7 rights." Id. at 647.[3] There is no allegation in this case that the rules at issue explicitly restrict Section 7 rights, have been promulgated in response to union activity, or have been applied to restrict the exercise of Section 7 rights, so the question is whether employees would reasonably understand the rules to restrict Section 7 activity.

As the judge observed, employees indisputably have a Section 7 right to concertedly appeal to their employer's customers for support in a labor dispute. *Trinity Protection Services*, 357 NLRB 1382, 1383 (2011); *Kinder-Care Learning Centers*, 299 NLRB 1171, 1171–1172 (1990).[4] Contrary to the judge, however, the disputed rules do not interfere with this right insofar as they restrict the use or disclosure of social security numbers and credit card numbers, or to the extent that they restrict the use of customer contact information obtained from the Respondent's own confidential records. Accordingly, for the reasons that follow, we find that employees would not reasonably construe the rules at issue here to prohibit Section 7 activity.

The "Confidential Information" rule specifically defines the confidential information to which it applies.[5] The only information covered by that rule that arguably relates to customers is "social security numbers or credit

[3] Chairman Miscimarra agrees that the rules are lawful under *Lutheran Heritage Village* for the reasons articulated in the text. However, for the reasons explained in his separate opinion in *William Beaumont Hospital*, 363 NLRB No. 162, slip op. at 7–24 (2016) (Member Miscimarra, concurring in part and dissenting in part), he believes that the *Lutheran Heritage* "reasonably construe" test should be overruled by the Board or repudiated by the courts. In Chairman Miscimarra's view, the Board should evaluate an employer's workplace rules, policies and handbook provisions by striking a proper balance that takes into account (i) the legitimate justifications associated with the disputed rules and (ii) any potential adverse impact of the rules on NLRA-protected activity. See *NLRB v. Great Dane Trailers, Inc.*, 388 U.S. 26, 33–34 (1967) (referring to the Board"s "duty to strike the proper balance between . . . asserted business justifications and the invasion of employee rights in light of the Act and its policy"). In striking this balance, Chairman Miscimarra believes the Board must take into account relevant considerations, which may include, depending on the case, reasonable distinctions between types of rules and justifications, evidence regarding the particular industry or work setting, specific events that may bear on the disputed rule, and the possibility that the rule may be lawfully maintained even though application of the rule against NLRA-protected conduct may be unlawful. See *William Beaumont Hospital*, supra, slip op. at 15, 18–20 (Member Miscimarra, concurring in part and dissenting in part).

Applying this balancing test here, Chairman Miscimarra agrees that the rules are lawful. The impact on Sec. 7 rights is comparatively slight, since the rules only limit employees' use of information maintained in the Respondent's confidential records, and the rules erect no barrier to communications with customers using information from any other source. Moreover, the Respondent has compelling justifications for protecting the customer information at issue here: names, home and office contact information, social security numbers, driver's license numbers, account numbers, and other similar data. See *Schwan's Home Service,* 364 NLRB No. 20, slip op. at 16 (2016) (then-Member Miscimarra, concurring in part and dissenting in part).

Member McFerran notes Chairman Miscimarra's view that the standard set forth in *Lutheran Heritage Village* should be changed, but she disagrees with that view for the reasons stated in *William Beaumont Hospital*, supra, slip op. at 2–6 (2016).

[4] Chairman Miscimarra notes that such appeals are subject to an employee's duty of loyalty to his or her employer as defined in *NLRB v. Electrical Workers Local 1229 (Jefferson Standard Broadcasting Co.)*, 346 U.S. 464 (1953), and to the duty to refrain from making maliciously false statements as set forth in *Linn v. Plant Guards Local 114*, 383 U.S. 53 (1966).

[5] "What is confidential information? It could be business or marketing plans, pricing strategies, financial performance before public disclosure, 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."

Our dissenting colleague does not contend that the Respondent's Confidential Information rule violates the Act insofar as it prohibits the disclosure of customers' social security numbers or credit card numbers. Focusing solely on the rule's final clause—i.e., "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"—the dissent instead argues that the rule sweeps more broadly "to encompass general information about customers, including information by employees in furtherance of their Section 7 rights." It is well settled, however, that in "determining whether a challenged rule is unlawful, the Board must . . . give the rule a reasonable reading. It must refrain from reading particular phrases in isolation, and it must not presume improper interference with employee rights." *Lutheran Heritage Village*, 343 NLRB at 646. The dissent says that we have disregarded these principles, but it is our colleague who does so. Employees would not reasonably read the definition quoted above to encompass "customer information" other than social security numbers or credit card numbers when the provision is read as a whole, including the list of specific covered items. Even if the rule were susceptible to the broader interpretation our colleague places on it, the only example he provides of additional information that would be covered under his proposed reading of the rule is customer contact information. Restrictions on the disclosure of customer contact information obtained from the Respondent's own confidential records are lawful for the reasons stated below.

Chairman Miscimarra observes that the dissent mischaracterizes our interpretation of the Confidential Information rule when he says that we "deconstruct" it. Despite our disagreement regarding the reasonable construction of the rule, we and our colleague both proceed from the assumption that the rule *may* be interpreted and that different interpretations may be more or less reasonable. Chairman Miscimarra notes that deconstruction proceeds from a view of language that rejects these assumptions. See https://en.wikipedia.org/wiki/Deconstruction (last visited June 19, 2017) (summarizing, with questionable success, the philosophy of deconstruction as expounded by Jacques Derrida, its subsequent development by the critical theorists of the Yale School and Jean-Luc Nancy, and the critiques leveled against Derrida's views by several philosophers, including John Searle and Jürgen Habermas).

card numbers." The General Counsel concedes that customers' social security numbers and credit card numbers are "sensitive" information, and he does not argue that employees have a right to use that information for Section 7 purposes.[6] Neither is there any basis for inferring such a right, since social security numbers and credit card numbers would be of no valid use in appealing to customers regarding employees' work-related concerns or engaging in any other activity protected by Section 7. To the extent that the Respondent's rules prohibit the unauthorized use or disclosure of customers' social security numbers or credit card numbers, they are lawful.

The "Use and Protection of Personal Data" and "Confidentiality and Acceptable Use of Company Systems" rules are similarly lawful to the extent they prohibit the use or disclosure of social security numbers or account numbers.[7] We recognize that those rules also limit the use or disclosure of customer names and contact information, which employees could use for the purpose of appealing to customers regarding a labor dispute or their terms and conditions of employment. But both rules, by their terms, only apply to customer names and contact information obtained from the Respondent's own confidential records.[8] The Act does not protect employees who divulge information that their employer lawfully may conceal. See, e.g., *International Business Machines Corp.,* 265 NLRB 638 (1982) (employee lawfully discharged for disclosing wage data employer had compiled and classified as confidential). Thus, the Board has repeatedly held that employees may be lawfully disciplined or discharged for using for organizational purposes information improperly obtained from their employer's private or confidential records. See *Ridgeley Mfg. Co.,* 207 NLRB 193, 196–197 (1973), enfd. 510 F.2d 185 (D.C. Cir. 1975); see also *Flex Frac Logistics, LLC*, 360 NLRB 1004, 1005 (2014) (employee lawfully discharged for revealing confidential information contained in employer's files despite the fact that the information "arguably implicated concerns underlying the Section 7 rights of others"); *International Business Machines Corp.,* supra (employee had Sec. 7 right to discuss wages and attempt to learn what others were paid, but not to disseminate employer's own confidential compilation of wage data).[9] Consistent with these cases, because the "Use and Protection of Personal Data" and "Confidentiality and Acceptable Use of Company Systems" rules only restrict the use or disclosure of confidential customer contact information that the Respondent "has" or "maintains," they are lawful.[10]

[6] To the contrary, the General Counsel contends that the disputed rules are "overbroad, as they are not narrowly tailored to protect sensitive customer information such as social security numbers and account numbers." GC Answering Br. at 16–17.

[7] In this regard, we find that social security numbers and credit card numbers are the only types of customer information covered by the first paragraph of the "Confidentiality and Acceptable Use of Company Systems" rule. By its terms, that portion of the rule applies only to "Confidential Information," and we find that employees would reasonably construe that term to have the same meaning as in the Confidential Information rule discussed above. As we have explained, social security numbers and credit card numbers are the only types of customer information arguably covered by the "Confidential Information" rule.

[8] The Use and Protection of Personal Data rule states: "*The Company has certain personal data of its present and former . . . customers* . . . . [W]e must follow all policies and measures adopted by the Company for the protection of *such data* from unauthorized use . . . ." (emphasis added). The "Confidentiality and Acceptable Use of Company Systems" rule similarly states: "*Company maintains certain information regarding its present and former . . . customers* . . . . Company respects the privacy of *this data* where it includes personally-identifiable information ("*Personal Data"*) . . . . *Personal Data* may not be shared with any third party without the written approval of your senior Sales Promotion executive or, for support organizations, your Chief Executive Officer" (emphasis added).

[9] See also *Food Services of America, Inc.,* 360 NLRB 1012, 1012 fn. 4 (2014) (employee lawfully discharged for transferring hundreds of business emails, many of which contained confidential business information, to personal email accounts), vacated pursuant to settlement by 365 NLRB No. 85 (2017); *Cook County College Teachers Union Local 1600*, 331 NLRB 118, 119–120 (2000) (employee lawfully disciplined for providing list of names, home addresses, and telephone numbers of respondent union's officials, maintained in respondent union's confidential internal directory, to charging party union); *Roadway Express,* 271 NLRB 1238, 1239–1240 (1984) (employee lawfully discharged for taking bills of lading from employer's files, copying them, and providing copies to the union); *Bullock's,* 251 NLRB 425, 426 (1980) (employee lawfully discharged for wrongfully obtaining and copying confidential performance reviews in connection with challenge to employer's evaluation policy).

The "Use and Protection of Personal Data" and "Confidentiality and Acceptable Use of Company Systems" rules also restrict the use of driver's license numbers and account numbers obtained from the Respondent's records. Those restrictions are lawful because the information is of no valid use for the purpose of Sec. 7 activity and because, in any event, the restriction only applies to the disclosure of information obtained from the Respondent's own confidential records.

[10] *Schwan's Home Service,* 364 NLRB No. 20, slip op. at 3 fn. 8 (2016), where the Board found unlawful a "near-complete prohibition of disclosure or use of 'information concerning customers,'" is distinguishable because in that case the prohibition was not limited to information obtained from the employer's confidential records. The rules at issue here explicitly contain such a limitation.

Chairman Miscimarra relevantly dissented in *Schwan's,* and he adheres to the views he expressed therein. See *Schwan's Home Service,* supra, slip op. at 16 (then-Member Miscimarra, concurring in part and dissenting in part). However, he agrees that *Schwan's* is distinguishable on the basis stated above.

Our dissenting colleague contends that the Respondent could not lawfully restrict the use or disclosure of confidential customer contact information from its records because employees "likely" had access to them as part of their "normal employment duties." This argument fails for two reasons. First, it is not the case that the Act protects any disclosure of confidential information from an employer's records, regardless of the circumstances, whenever the employee has access to the information as part of his or her duties. See, e.g., *Food Services of America*,

ORDER

The Respondent, Macy's, Inc., Saugus, Massachusetts, its officers, agents, successors, and assigns, shall

1. Cease and desist from

(a) Maintaining a rule that restricts its employees' use of information regarding fellow employees.

(b) Maintaining a rule that restricts the use of the Respondent's logo.

(c) Maintaining a rule that requires employees to notify the Respondent's human resources department prior to participating in a government investigation.

(d) In any like or related manner interfering with, restraining, or coercing employees in the exercise of the rights guaranteed them by Section 7 of the Act.

2. Take the following affirmative actions necessary to effectuate the policies of the Act.

(a) Rescind or revise the rules in its employee handbook that restrict the use of information regarding fellow employees.

(b) Rescind or revise the rule in its employee handbook that restricts the use of the Respondent's logo.

(c) Rescind or revise the rule in its employee handbook that requires employees to notify the Respondent's human resources department prior to participating in a government investigation.

(d) Furnish all current employees with inserts for the current employee handbook that (1) advise that the unlawful provisions have been rescinded or (2) provide lawfully worded provisions on adhesive backing that will cover the unlawful provisions; or publish and distribute to employees revised employee handbooks that (1) do not contain the unlawful provisions or (2) provide lawfully worded provisions.

(e) Within 14 days after service by the Region, post at all its facilities nationwide copies of the attached notice marked "Appendix."[11] Copies of the notice, on forms provided by the Regional Director for Region 1, after being signed by the Respondent's authorized representative, shall be posted by the Respondent and maintained for 60 consecutive days in conspicuous places including all places where notices to employees are customarily posted. In addition to physical posting of paper notices, notices shall be distributed electronically, such as by email, posting on an intranet or an internet site, or other electronic means, if the Respondent customarily communicates with its employees by such means. Reasonable steps shall be taken by the Respondent to ensure that the notices are not altered, defaced, or covered by any other material. In the event that, during the pendency of these proceedings, the Respondent has gone out of business or closed the facility involved in these proceedings, the Respondent shall duplicate and mail, at its own expense, a copy of the notice to all current employees and former employees employed by the Respondent at any time since September 5, 2013.

(f) Within 21 days after service by the Region, file with the Regional Director for Region 1 a sworn certification of a responsible official on a form provided by the Region attesting to the steps that the Respondent has taken to comply.

Dated, Washington, D.C. August 14, 2017

_____

Philip A. Miscimarra, Chairman

_____

Lauren McFerran, Member

(SEAL) NATIONAL LABOR RELATIONS BOARD

MEMBER PEARCE, dissenting.

The General Counsel alleged, and the judge found, that the Respondent's rules restricting employees' use and disclosure of certain customer information violated Section 8(a)(1) of the Act. Contrary to the majority, who interpret the rules more narrowly than as written, I agree with the judge that employees would reasonably understand the rules to broadly prohibit the disclosure of general information about customers—information that

supra (finding the Act did not protect employee who copied hundreds of business emails from his own work account that included "the names of vendors and customers, . . . as well as other information. By whatever name, whether proprietary or confidential, this is information that any company would not want out of its possession."); *Cook County College Teachers Union Local 1600*, supra (finding the Act did not protect employee's disclosure of respondent union's directory to charging party where employee had access to directory and used it as part of her work). Second, there is in any event no evidence in this case that the Respondent's customer contact information was available to "all employees," as the dissent contends, much less that it was used by them in the course of their normal employment duties. To the contrary, the parties agreed to submit this case to the judge on the basis of a stipulated record, and the parties' stipulation does not address this issue in any way. Our colleague's unsupported speculation as to the Respondent's "likely" practices cannot substitute for evidence not in the record.

[11] If this Order is enforced by a judgment of a United States court of appeals, the words in the notice reading "Posted by Order of the National Labor Relations Board" shall read "Posted Pursuant to a Judgment of the United States Court of Appeals Enforcing an Order of the National Labor Relations Board."

could be used by employees in furtherance of their protected, concerted activities.[1]

It is well settled that a rule which restricts or prohibits employees' disclosure of a broad range of customer information violates Section 8(a)(1). See *Schwan's Home Service*, 364 NLRB No. 20, slip op. at 3 fn. 8 (2016) (finding "the rule's near-complete prohibition of disclosure or use of 'information concerning customers'" to be unlawful); *Boch Honda*, 362 NLRB No. 83, slip op. at 1 fn. 4 (2015), enfd. 826 F.3d 558 (1st Cir. 2016) (finding that employer unlawfully treated "information about prospective customers and suppliers" as confidential). The rules at issue here broadly encompass such disclosures. The Respondent's "Confidential Information" rule requires employees to keep confidential "information about our Company, its business, associates, customers . . . " and further defines confidential information as "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." The Respondent's rules, "Use and Protection of Personal Data" and "Confidentiality and Acceptable Use of Company Systems" broadly restrict disclosure of "certain personal data of its present and former associates, customers," including "names, home and office contact information, social security numbers, driver's license numbers, account numbers and other similar data."

Because many of the Respondent's employees, like those in *Boch Honda* and *Schwan's*, work in retail or customer service, they 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. For example, employee interaction with customers could give rise to customer complaints about employee performance. See *Schwan's*, supra, slip op. at 3 fn. 8 (observing that "'information concerning customers' is inextricably intertwined in many aspects of [the employees'] work, including their interaction with customers, potential customer complaints about their performance . . . their commission-based compensation, and their ability to meet the Respondent's scheduling targets."). This language would also reasonably be understood by employees to prevent them from contacting customers to appeal for support in connection with their concerted, protected activities aimed at improving their terms and conditions of employment. Id.

My colleagues assert that *Schwan's* and *Boch Honda* are distinguishable because the "Confidential Information" rule can only be reasonably read to prohibit the disclosure of confidential information such as social security and credit card numbers, and that the "Use and Protection of Personal Data" and "Confidentiality and Acceptable Use of Company Systems" rules apply solely to social security and credit card numbers as well as customer contact information drawn from the Respondent's confidential records. However, my colleagues' focus on a few isolated words and phrases runs counter to Board precedent requiring that the language of the rule not be read in isolation[2] and fails to acknowledge how an average employee would interpret the rules.[3] By focusing on the phrase "documents that show social security numbers or credit card numbers," my colleagues ignore the accompanying broad language defining confidential information as "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." This latter expansive language would reasonably be read by employees to encompass general information about customers, including information by employees in furtherance of their Section 7 rights. For example, the disclosure of contact information or addresses could certainly "benefit" an outside entity, such as a union seeking to solicit support for employee organizing efforts from the Respondent's customers. Alternatively, information about a dispute between an employee and customer could similarly "harm" either party, but would be relevant in the grievance or disciplinary process.

With regard to the "Use and Protection of Personal Data" and "Confidentiality and Acceptable Use of Company Systems" rules, my colleagues assert that the rules restricting the use of customer names and contact information are limited by their terms to information obtained from the Respondent's confidential records. That an employer maintains certain information in its records, however, is not the same as an employer creating a confidential record with that information. Indeed, under my colleagues' interpretation, *any* customer information obtained by an employer and maintained in its files can become a "confidential record" if an employer designates

[1] I agree with my colleagues that the applicable inquiry here is whether a reasonable employee would read the Respondent's rules to restrict their Sec. 7 activity. *Lutheran Heritage Village-Livonia*, 343 NLRB 646, 647 (2004).

[2] *Lafayette Park Hotel*, 326 NLRB 824, 825 (1998), enfd. 203 F.3d 52 (D.C. Cir. 1999).

[3] While my colleagues' sophisticated attempt to deconstruct the language might seem reasonable from the standpoint of a practicing labor lawyer, their approach fails to appreciate that "[r]ank-and-file employees do not generally carry lawbooks to work or apply legal analysis to company rules as do lawyers, and cannot be expected to have the expertise to examine company rules from a legal standpoint." *Ingram Book Co.*, 315 NLRB 515, 516 fn. 2 (1994).

it as such in its confidentiality policies. This proposition is contrary to B–-197 (1973), enfd. 510 F.2d 185 (D.C. Cir. 1975), a case relied upon by my colleagues, the Board emphasized that the relevant inquiry for whether the information obtained by an employee constituted confidential records was "whether timecards located by the timeclock fall into the category of private or confidential records of the Employer or constitute information available to all employees in the course of their normal work relationship." Cf. *Flex Frac Logistics, LLC*, 360 NLRB 1004, 1004 (2014) (observing that the confidential records obtained by an employee were "closely guarded" by the employer and, although the employee had access to the underlying information, she never needed to utilize it in the performance of her duties); *International Business Machines Corp.*, 265 NLRB 638, 638 (1982) (explaining that the employer's confidential wage data had been compiled for internal use only and was not generally available to employees).

Here, the Respondent's "Use and Protection" rule makes no such distinction; the customer names and contact information are available to all employees and used in the course of their normal employment duties. The Respondent likely maintains customer names and addresses in its computer system, which are accessed by employees, either by entering them into the system or utilizing them later as part of customer service. The Respondent's rules, therefore, encompass information broader than the type of records that the Board has found to be protected from disclosure as confidential.[4] Indeed, they cannot be meaningfully distinguished from the rules found unlawful in *Schwan's* and *Boch Honda.*

In sum, contrary to my colleagues, I find that the Respondent's overly broad rules barring disclosure of customer information would reasonably tend to chill employees in the exercise of the Section 7 rights. Accordingly, I respectfully dissent from my colleagues' dismissal of this 8(a)(1) allegation.

Dated, Washington, D.C. August 14, 2017

Mark Gaston Pearce, Member

(NATIONAL LABOR RELATIONS BOARD

[4] Contrary to my colleagues, I am not contending that the Act protects "any disclosure of confidential information from an employer's records, regardless of the circumstances, whenever the employee has access to the information as part of his or her duties." Rather, I find that, under the Board's precedent, if an employer has not treated information as a confidential record, and if the information could otherwise be lawfully disclosed, the employer cannot prohibit such disclosure on the basis of a conclusory statement that the information is "confidential" and the employer "maintains" the information.

APPENDIX

NOTICE TO EMPLOYEES
POSTED BY ORDER OF THE
NATIONAL LABOR RELATIONS BOARD
An Agency of the United States Government

The National Labor Relations Board has found that we violated Federal labor law and has ordered us to post and obey this notice.

FEDERAL LAW GIVES YOU THE RIGHT TO

Form, join, or assist a union

Choose representatives to bargain with us on your behalf

Act together with other employees for your benefit and protection

Choose not to engage in any of these protected activities.

WE WILL NOT maintain a rule that restricts your use of information regarding other employees.

WE WILL NOT maintain a rule that restricts your right to use our logo.

WE WILL NOT maintain a rule that requires you to notify our human resources department prior to participating in a government investigation.

WE WILL NOT in any like or related manner interfere with, restrain, or coerce you in the exercise of the rights listed above.

WE WILL rescind or revise the rules in our employee handbook that restrict the use of information regarding other employees.

WE WILL rescind or revise the rule in our employee handbook that restricts the use of our logo.

WE WILL rescind or revise the rule in our employee handbook that requires you to notify our human resources department before participating in a government investigation.

WE WILL furnish you with inserts for the current employee handbook that (1) advise that the unlawful provisions have been rescinded or (2) provide lawfully worded provisions, or WE WILL publish and distribute revised employee handbooks that (1) do not contain the unlawful provisions or (2) provide lawfully worded provisions.

MACY'S, INC.

The Board's decision can be found at www.nlrb.gov/case/01–CA–123640 or by using the QR code below. Alternatively, you can obtain a copy of the decision from the Executive Secretary, National Labor Relations Board, 1015 Half Street, S.E., Washington, D.C. 20570, or by calling (202) 273-1940.

Alejandra Hung, Esq., for the General Counsel.
William Joy, Esq. (Morgan, Brown & Joy), for the Respondent.
Alfred O'Connell, Esq. (Pyle Rome Ehrenberg P.C.), for the Charging Party.

DECISION

STATEMENT OF THE CASE

JOEL P. BIBLOWITZ, ADMINISTRATIVE LAW JUDGE. The parties herein waived a hearing and submitted this case directly to me by way of a Joint Motion and Stipulation of Facts dated April 2, 2015, which states as follows:

This is a joint motion by the parties to this case: Macy's, Inc. (Respondent); the Charging Party, United Food and Commercial Workers Union, Local 1445 (the Union); and the General Counsel, to transfer this case to an administrative law judge pursuant to Section 102.35(a)(9) of the Board's Rules and Regulations. The transfer of the case will effectuate the purposes of the Act and avoid unnecessary costs and delay.

If this motion is granted, the parties agree to the following:[1]

1. The record in this case consists of the charge in Case 01–CA–123640, the complaint, the answer, the stipulation of facts, the statement of issues

Presented, and each party's Statement of Position.

2. This case is submitted directly to an Administrative Law Judge for issuance of findings of facts, conclusions of law, and an Order.

3. The parties waive a hearing before an Administrative Law Judge.

4. An administrative law judge should set the time for the filing of briefs.

I. STIPULATION OF FACTS

1. (a) The charge in Case 01–CA–123640 was filed by the Union on March 3, 2014. (A copy of the charge and affidavit of service are attached hereto as Exhs. A and B respectively.)

2. (a) On August 28, 2014, the Regional Director for Region 1 of the Board issued a complaint and notice of hearing (the complaint) alleging that Respondent violated the National Labor Relations Act (the Act). (A copy of the complaint is attached hereto as Exh. C). The hearing in this matter has been postponed indefinitely by oral agreement of the parties.

(b) On September 8, 2014, Respondent filed a timely answer to the complaint, denying that it had committed any violation of the Act. (A copy of the answer to the complaint is attached hereto as Exh. D).

3. Respondent is a corporation engaged in the operation of retail department stores throughout the United States, including a store located in Saugus, Massachusetts (the Saugus store). Annually, Respondent, in conducting its business operations derives gross revenues in excess of $500,000 and purchases and receives at the Saugus store goods valued in excess of $5000 directly from points outside the Commonwealth of Massachusetts. At all material times, Respondent has been an employer engaged in commerce within the meaning of Section 2(2), (6), and (7) of the Act.

4. The Union is a labor organization within the meaning of Section 2(5) of the Act.

5. At all material times, Lori Barroso and Danielle McKay have been Respondent's human resources manager and store manager at its Saugus store, respectively, and have been supervisors of Respondent within the meaning of Section 2(11) of the and agents of Respondent within the meaning of Section 2(13) of the Act.

6. At all material times, and since at least September 5, 2013, Respondent has maintained an employee handbook entitled: "Code of Conduct" (the Handbook) that includes the following policy regarding Confidential Information:

> Being Honest . . . Company Assets and Information
>
> Our Company's assets must be used, purchased or disposed of only for the Company's benefit. We are all obligated to protect the assets of the Company and use them appropriately.
>
> In addition to merchandise, equipment furnishings and other property, our Company's assets include Company information, the personal information of the Company's employees and customers, any work product we may develop in the course of our employment and any business or financial opportunity that the Company could avail itself of.
>
> Confidential Information
>
> What To Know
>
> Confidential information about our Company, its business, associates, customers and business partners should be protected. It can be used only to pursue the Company's business interests or to comply with the Company's legal or other obligations.
>
> What is confidential information? It could be business or marketing plans, pricing strategies, financial performance before public disclosure, 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 and proprietary information of others be respected.
>
> What To Do

[1] By Order dated April 6, 2015, I accepted the stipulated record and set May 4, 2015 as the date briefs are due.

In performing our duties, we as associates may have access to confidential information relating to our Company, its business, customers, business partners or our co-workers.

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.

Here are some simple rules to follow.

Confidential information should:

- Be stored in locked file cabinets or drawers and not be left where others can see it,
- Be clearly marked as confidential whenever possible,
- Be shared only with those who need to see it for Company business purposes,
- Not be sent to unattended fax machines or printers,
- Not be discussed where others may hear,
- Be shredded when no longer needed.

Always respect the confidentiality of the information of third parties. We must not use or disclose any of it except as authorized under a written agreement approved by our Law Department.

7. At all material times, and since at least September 5, 2013, Respondent has maintained a Handbook policy regarding the Use and Protection of Personal Data, which states in relevant part:

What To Know

The Company has certain personal data of its present and former associates, customers and vendors. It respects the privacy of this personal 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.

What To Do

We have a strict obligation to use such personal data in a manner that:

- respects the privacy of our co-workers and our Company's customers and vendors,
- complies with all applicable laws and regulations, and Company policies,
- upholds any confidentiality or privacy obligations of the Company in its contracts.

In addition, we must follow all policies and measures adopted by the Company for the protection of such data from unauthorized use, disclosure or access. If any of us becomes aware of any instance of data being accessed or being used in an unauthorized manner, we must report it immediately to our Divisional Security Administrator or the Law Department.

8. At all material times, and since at least September 5, 2013, Respondent has maintained the following Handbook policy regarding Intellectual Property:

What To Know

Trademarks, trade names, copyrights, trade secrets, rights of publicity and other similar proprietary information are considered intellectual property.
Our Company owns many valuable intellectual property rights, such as our trademarks INC and Alfani.

Our Company may lose its rights in the intellectual property that it already owns, or risk lawsuits and other penalties if we fail to comply with certain laws.

Our Company also has the right to use the intellectual property of certain business partners under agreements. American Rag is one such example.
We must use our Company's or a business partner's intellectual property only as authorized.

If we violate the terms of these agreements, our Company may not only lose the right to use the licensed intellectual property, but may also be subject to substantial damage claims.

What To Do

We must not use the intellectual property rights of others without their permission.

We may use the intellectual property of the Company only for the benefit of the Company, and should not allow others to use our logo or other intellectual property except in accordance with prescribed procedures.
Similarly, if and when the Company is permitted to use the intellectual property of its business partners, we must follow the reasonable usage guidelines provided by the business partner.

We must not provide to or accept from third parties any proprietary information or the right to use intellectual property without a written agreement that is prepared by our Law Department.

If any of us makes a discovery, or develops an invention, design, process, concept or idea in the course of our employment with the Company, the Company owns it. We should assist the Company's lawyers in documenting the Company's ownership.

9. At all material times, and since at least September 5, 2013, Respondent has maintained a Handbook policy regarding Government Investigations and Contacts, which states, in relevant part:

What To Know

Our Company's policy is to cooperate with appropriate governmental requests or investigation, and to comply with all applicable laws governing contacts with government officials. Our Law Department is responsible for managing all such requests, investigations or contacts and providing truthful and accurate information.

What To Do

> If we are asked to provide information- verbal or written- for a government investigation, or if a government representative appears at our workplace, we must promptly notify our Human Resources representative or the Law Department and obtain approval for the release of any information. We must not obstruct, influence, mislead or impede the investigation.
>
> Any contacts with government officials for the purpose of influencing legislation, regulations or decision-making may constitute lobbying. We must not contact or communicate with any government official for such purpose on behalf of the Company without having specific authorization. If a need arises to do so, we must contact the Law Department.

10. At all material times, and since at least September 5, 2013, Respondent has maintained a Handbook policy regarding Confidentiality and Acceptable Use of Company Systems, which states, in relevant part:

> The following standards and procedures apply to your use of, or access to, all Confidential Information.
>
> 1. All Non-Public Information is Sensitive
>
> Any information that is not generally available to the public that relates to the Company or the Company's customers, employees, vendors, contractors, service providers, Systems, etc., that you receive or to 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" under the Macy's Information Security Policy. As is set forth in the Macy's Information Security Policy, internal access to Confidential Information should only be granted on a "need to know" basis, and such information should not be shared with third parties without prior approval from your Company supervisor and consultation with the Law Department.
>
> 3. Use and Protection of Personal Data
>
> Company maintains certain information regarding its present and former associates, customers and vendors. Company respects the privacy of this data where it includes personally-identifiable information ("Personal Data"). Personal Data includes names, home and office contact information, social security numbers, driver's license numbers, account numbers and other similar data. Company is committed to handling Personal Data responsibly and using it only as appropriate for legitimate business purposes. This commitment requires that all Company employees, contractors, and third parties who are granted access to Personal Data by Company follow all policies adopted by the Company for the protection of such data against unauthorized use, disclosure or access. Such policies, including those' set forth in the Macy' Information Security Policy, may vary depending on the sensitivity of the Personal Data at issue.
>
> Personal Data may not be shared with any third party without the written approval of your senior Sales Promotion executive or, for support organizations, your Chief Executive Officer.

11. The policies (also referred to herein as rules) described above were not promulgated in response to union activity or applied in any manner to restrict Section 7 rights.

12. Respondent has not, by any other actions, led employees to believe that the rules described above prohibit Section 7 activity.

13. On April1, 2014, Macy's notified its employees through its intranet portal In-Site (the method customarily used by Macy's to notify employees of any changes in company policy) that it had revised its Code of Conduct by adding to the introductory page the following:

> Nothing in the Code or the policies it incorporates, is intended or will be applied, to prohibit employees from exercising their rights protected under federal labor law, including concerted discussion of wages, hours or other terms and conditions of employment. This Code is intended to comply with all federal, state, and local laws, including but not limited to the Federal Trade Commission, Endorsement Guidelines and the National Labor Relations Act, and will not be applied or enforced in a manner that violates such laws.

II. ISSUE PRESENTED

Whether Respondent violated Section 8(a)(1) of the Act by maintaining the rules described above in paragraphs 6–10.

III. POSITIONS OF THE PARTIES

A. General Counsel's Position

Counsel for the General Counsel contends that the cited Handbook provisions are overly broad and have a reasonable tendency to interfere with, restrain, and coerce employees in their exercise of the rights guaranteed in Section 7 of the Act.

The Handbook's Confidential Information Policy violates Section 8(a)(1) of the Act because, by prohibiting employees from disclosing any company information and information about employees, in the absence of clarification, it could be reasonably construed by employees to preclude discussion of wages and other terms of conditions of employment among fellow employees, and restrict the exercise of their Section 7 rights.

The Handbook's Use and Protection of Personal Data Policy contains an unqualified prohibition against the disclosure of any information about employees, former employees, and customers, and violates Section 8(a)(1) of the Act insofar as it could be reasonably construed by employees to restrict discussion of terms and conditions of employment among fellow employees, and restrict the exercise of their Section 7 rights.

The Handbook's Intellectual Property Policy violates Section 8(a)(1) of the Act because it is overbroad and could be reasonably construed by employees to prohibit the use of the Respondent's logo or trademark as a means to identify the Respondent in the course of Section 7 activity related to terms and working

conditions of employment, including its use in employee communications such as leaflets, signs, and even photos, thereby restricting the exercise of their Section 7 rights.

Further, the Handbook's Government Investigations and Contacts Policy violates Section 8(a)(1) because it could be reasonably construed to prohibit employees from participating in government investigations and require employees to notify Respondent' human resources department or law department first. Further, the policy is overbroad to the extent that as it affects employees' contact with the National Labor Relations Board and other law enforcement officials about wages, hours, and working conditions.

The Handbook's Confidentiality and Acceptable Use of Company Systems Policy is overbroad and violates Section 8(a)(1) because it prohibits employees from disclosing any information about the Company, employees, and customers, in the absence of clarification, and could be reasonably construed by employees to preclude discussion of terms and conditions of employment, among fellow employees and restrict the exercise of their Section 7 rights.

Because the Handbook applies to employees at Respondent's facilities throughout the United States, the General Counsel seeks a nationwide remedy for the unfair labor practices. Specifically, the General Counsel seeks rescission of the above-described rules, written notice to employees that the above rules have been rescinded and a notice posting, applicable to all Respondent's facilities.

B. Respondent's Position

Respondent asserts that the sections of its code of conduct alleged to be unlawful are not unlawful when considered in the proper context because employees would not reasonably construe the language to prohibit Section 7 activity. There is limiting language in the provisions of the code in question which would clarify to employees that the rule does not restrict Section 7 rights.

Page 16 of the Code of Conduct, Confidential Information, has language which limits the definition to 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." Respondent contends that discussion by employees of wages and conditions of employment could not be reasonably construed by employees as information that would harm the company.

Page 18 of the Code of Conduct, Personal Data, gives examples of data, e.g. "social security numbers, driver's license numbers, account numbers and other similar data" whose disclosure would be illegal or unprotected conduct such that the provision could not be reasonably construed to cover protected activity.

Next, page 22 of the Code of Conduct, Intellectual Property, does not restrict employees in using the Company's logo. The clause prohibits allowing "others" to use the logo. Furthermore, this entire provision, when read in context, would lead any employee to understand that it is to protect intellectual and proprietary property and not to restrict an employee from using the Company's name/logo on a picket sign or for any other Section 7 activity.

Page 24 of the Code of Conduct, Government Investigations, states in the opening sentence that the company policy is to "comply with all applicable laws governing contacts with government officials." The policy does not prohibit employees from speaking to a government official, such as an NLRB agent, and when read in context with the opening sentence would not be reasonably construed to do so.

Page 31 of the Code of Conduct, Confidentiality and Acceptable Use of Company Systems is a detailed seven-page policy. Personal Data lists, as on page 18 of the Code of Conduct, "social security numbers, driver's license numbers, account numbers and other similar data" and thus employees who read the policy as a whole would not believe it extended to terms and conditions of employment.

Furthermore, respondent contends that a "harbor" or "savings clause" in the Code of Conduct informs all of its provisions and precludes a finding that employees would reasonably read any of the challenged work rules as unlawfully restricting their Section 7 rights.

C. Union's Position

The Union concurs with the General Counsel's position.

This stipulation is made without prejudice to any objection that any party may have as to the relevance of any facts stated herein.

Analysis

In determining whether any, or all, of the above-referenced provisions contained in the Employee Handbook violate the Act, the initial inquiry is to *Lutheran Heritage Village- Livonia,* 343 NLRB 646 (2004). Under that test, the initial inquiry is whether the rule at issue explicitly restricts activities that are protected by Section 7 of the Act; if so, it is unlawful. If not, the finding of a violation is dependent upon a showing of one of the following: employees would reasonably construe the rule to prohibit protected activity, or the rule has been applied to restrict the exercise of that activity. As the rule does not explicitly restrict activities protected by Section 7 of the Act, and as the parties, as part of the joint motion and stipulation of facts, agreed these rules were not promulgated in response to union activity, or were applied in a manner to restrict Section 7 rights, the test for each of these challenged restrictions is whether employees could reasonably construe any or all of them to restrict protected activity. If the answer is that they could reasonably be construed to do so, the final question is whether the savings clause contained in the revised Code of Conduct effective April 1, 2014, precludes a finding of a violation of any of these rules.

Confidential Information

There are numerous provisions in the employee handbook that counsel for the General Counsel alleges unlawfully restricts employees in the exercise of their Section 7 rights, under the cover of Confidential Information. Under Being Honest . . . Company Assets and Information, in paragraph 6 of the stipulation of facts, the Handbook states, inter alia: "We are all obligated to protect the assets of the Company and use them appropriately. . .our Company's assets include Company information,

the personal information of the Company's employees and customers." Under Confidential Information What to Know, the Handbook states: "Confidential Information about our Company, its business, associates, customers and business partners should be protected . . . What is confidential information? It could be . . . information about employees . . . 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." Under "*What to Do*," the Handbook continues:

> In performing our duties, we as associates may have access to confidential information relating to our Company, its business, customers, business partners and our co-workers.
>
> 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 specially authorized.
>
> Here are some simple rules to follow.
>
> Confidential information should:
>
> Be shared only with those who need to see it for Company business purposes.
> Not be discussed where others may hear.

In paragraph 7 of the stipulation, under "What to Know," the Handbook states:

> The Company has certain personal data of its present and former associates, customers and vendors. It respects the privacy of this personal 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 . . . and other similar data.

Under "What To Do" the Handbook states: "We have a strict obligation to use such personal data in a manner that:

> Respects the privacy of our co-workers and our Company's customers and vendors."

In paragraph 10, under Confidentiality and Acceptable Use of Company Systems, The section entitled: "All Non-Public Information is Sensitive" states, inter alia:

> Any information that is not generally available to the public that relates to the Company or the Company's customers, employees, vendors, contractors, service providers, Systems, etc., that you receive or to 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" under the Macy's Information Security Policy. As is set forth in the Macy's Information Security Policy, internal access to Confidential Information should only be granted on a "need to know" basis, and such information should not be shared with third parties without prior approval from your Company supervisor and consultation with the Law Department.

The section entitled: "Use and Protection of Personal Data "states:

> Company maintains certain information regarding its present and former associates, customers and vendors. Company respects the privacy of this data where it includes personally-identifiable information ("Personal Data"). Personal Data includes names, home and office contact information, social security numbers, driver's license numbers, account numbers and other similar data. Company is committed to handling Personal Data responsibly and using it only as appropriate for legitimate business purposes. This commitment requires that all Company employees, contractors, and third parties who are granted access to Personal Data by Company follow all policies adopted by the Company for the protection of such data against unauthorized use, disclosure or access. Such policies, including those set forth in the Macy's Information Security Policy, may vary depending on the sensitivity of the Personal Data at issue.
>
> Personal Data may not be shared with any third party without the written approval of your senior Sales Promotion executive or, for support organizations, your Chief Executive Officer.

All of the above provisions prohibit the employees from divulging "the personal information of the Company's employees and customers," "information about employees . . . which if known outside the Company could harm the Company or its . . . employees," "confidential information," "information such as names, home and office contact information," "any information that is not generally available to the public that relates to the Company or the Company's . . . employees," "personally-identifiable information (Personal Data). Personal Data includes names, home and office contact information. . . ."

The test under *Lutheran Heritage,* is whether employees could reasonably construe these rules as prohibiting, or limiting their protected activities. In evaluating contested rules of conduct, the Board attempts to work out ". . . an adjustment between the undisputed right of self-organization assured to employees under the Wagner Act and the equally undisputed right of employers to maintain discipline in their establishments." *Republic Aviation v. NLRB,* 324 U.S. 793, 797–798 (1945). In other words, while employees have a right to engage in union and concerted activities, employers have "a substantial and legitimate interest in maintaining the confidentiality of private information." *Lafayette Park Hotel*, 326 NLRB 824, 826 (1998). However, in formulating its privacy and confidentiality rules, the employer must tread carefully and not venture into its employees' Section 7 rights.

In *Triana Industries*, 245 NLRB 1258 (1979), the Board held that Section 7 "encompasses the right of employees to ascertain what wages are paid by their employer, as wages are a vital term and condition of employment." *Aroostook County Regional Opthamology Center,* 317 NLRB 218, 220 (1995), enfd. in part 81 F.3d 209 (D.C. Cir 1996) held that wage discussions among employees are considered to be at the core of Section 7 rights because wages, "probably the most critical element in employment," are "the gist on which concerted activity feeds."

In *Parexel International, LLC,* 356 NLRB 516 (2011), the Board stated: "But whether such discussions lead to union activity or not, our precedents provide that restrictions on wage discussions are violations of Section 8(a)(1)."

As stated above, the ultimate issue herein is whether employees reading these rules, would reasonably construe them as restricting their Section 7 rights. In *Lafayette Park Hotel*, supra, the provision stated that the following conduct is unacceptable: "Divulging Hotel-private information to employees or other individuals or entities that are not authorized to receive that information." The Board dismissed this allegation saying that employees would not read it as prohibiting the discussion of wages among fellow employees or with a union:

> Clearly, businesses have a substantial and legitimate interest in maintaining the confidentiality of private information, including guest information, trade secrets, contracts with suppliers, and a range of other proprietary information. Although the term "Hotel-private" is not defined in the rule, employees in our view reasonably would understand that the rule is designed to protect that interest rather than to prohibit the discussion of their wages.

Similarly, in *Ark Las Vegas Restaurant Corp.,* 335 NLRB 1284, 1290–1291 (2001), the challenged rule stated:

> It is our policy to ensure that the operations, activities and affairs of Ark Las Vegas and our clients are kept confidential to the greatest extent. If, during their employment, employees acquire confidential or proprietary information about Ark Las Vegas or its clients, such information is to be handled in strict confidence and not to be discussed.

Citing *Lafayette Park,* supra*,* the Board dismissed this allegation finding that employees would not read this provision as restricting their right to discuss wages and other conditions of employment with fellow employees or a union. As neither *Lafayette Park* nor *Ark* specifically restrict the flow of employee information, they can easily be differentiated from the instant matter.

In *Cintas Corp.,* 344 NLRB 943 (2005), the challenged provision stated: "We honor confidentiality. We recognize and protect the confidentiality of any information concerning the company, its business plans, its partners[2], new business efforts, customers, accounting and financial matters." The Board found this provision unlawful due to the unqualified prohibition of the release of any information about "partners"-employees, finding that employees would reasonably construe this to restrict discussions of their terms of employment. Similarly, in *Double Eagle Hotel & Casino*, 341 NLRB 112, 114 (2004), the restrictive provision stated: "You are not, under any circumstances, permitted to communicate any confidential or sensitive information concerning the Company or any of its employees to any non-employee without approval from the General Manager or the President." In finding that this provision violated the Act, the Board found that employees could reasonably read this as chilling their Section 7 rights: "It is hard to imagine a rule that more explicitly restricts discussion of terms and conditions of employment more than the Confidential Information rule herein." Similarly, the restrictions on the release of personal information of the Respondent's employees, including their names and home and office contacts, obviously restricts employees in their Section 7 rights to discuss their terms and conditions of employment with fellow employees, as well as their ability to notify a union of other employees of the Respondent who might be interested in participating in the union movement. The fact that this restriction was repeated so many times in the Handbook further enforces the belief that employees could reasonably believe that it interferes with their Section 7 rights. I therefore find that these restrictions violate Section 8(a)(1) of the Act. *Flamingo Hilton-Laughlin*, 330 NLRB 287 (1999).

Counsel for the General Counsel also 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, and Counsel for the General Counsel argues that these restrictions are also unlawful. In *Trinity Protection Services, Inc.*, 357 NLRB 1382 (2011), the Board stated, ". . . employees' concerted communications regarding matters affecting their employment with their employer's customers or with other third parties, such as governmental agencies, are protected by Section 7 and, with some exceptions not applicable here, cannot lawfully be banned." I therefore find that this restriction violates Section 8(a)(1) as well. *Kinder-Care Learning Centers,* 299 NLRB 1171 (1990); *Boch Imports, Inc.*, 362 NLRB No. 83, slip op. 1 fn. 4 (2015).

It is further alleged that the Respondent violated the Act by prohibiting the use of the Respondent's "logo or other intellectual property" by others. Although not as obvious as prohibiting the use or release of information about its employees, this prohibition could also be reasonably understood to limit its employees, or a union, from publicizing a dispute with the Respondent by employing its logo in its distributed information. This could be an effective means of publicizing a dispute as the Respondent's logo is well known and easily recognized. In addition, the Respondent cannot defend that it has a legitimate business concern for forbidding the use of its logo; there is no confidentiality issue with the logo and I can see no valid business reason for this rule. I therefore find that the maintenance of this rule violates Section 8(a)(1) of the Act. *Boch Imports, Inc.*, supra at slip op. 2; *Pepsi Cola Bottling Co.*, 301 NLRB 1008 (1991).

The final allegation relates to the Respondent's Handbook policy regarding Government Investigations. After stating that it is the Respondent's policy to cooperate with appropriate governmental requests or investigations, it states, inter alia:

> If we are asked to provide information- verbal or written- for a government investigation, or if a government representative appears at our workplace, we must promptly notify our Human Resources representative or the Law Department and obtain approval for the release of any information. We must not obstruct, influence, mislead or impede the investigation.

Even though this provision states that it is the Respondent's policy to cooperate with governmental investigations, and that they will not obstruct or impede investigations, I believe that it

[2] The company refers to its employees as "partners."

is reasonable to conclude that employees who are asked to give a statement to a Board agent, or an agent of any other governmental agency, would be hesitant to participate in such a process knowing that they would first have to notify Respondent's representatives of their participation. In *Direc*TV, 359 NLRB 545, 546 (2013), the rule stated: "If law enforcement wants to interview or obtain information regarding a DIRECTV employee . . . the employee should contact the security department . . who will handle contact with law enforcement agencies . . . The Board found that this rule violated the Act because it would lead reasonable employees to conclude that they had to contact the company's security department before cooperating with the Board when the issue might involve their wages, hours and working conditions. In *Cellular Sales of Missouri, LLC*, 362 NLRB No. 27, slip op. 1 fn. 2 (2015), the Board stated that a rule violates the Act, "if employees would reasonably believe the rule or policy interferes with their ability to file a Board charge or access to the Board's processes, even if the rule does not expressly prohibit access to the Board." I therefore find that by requiring employees to notify Respondent's representatives prior to participating in a governmental investigation, the Respondent violated Section 8(a)(1) of the Act. *Trinity Protection services,* supra.

The final issue is whether the savings clause that Respondent sent to its employees on April 1, 2014 neutralizes these unlawful provisions. The Board has strict policies for employers attempting to repudiate unlawful rules. In *DirecTV,* 359 NLRB 545, 548 (2013), the Board stated:

> In order for a repudiation to serve as a defense to an unfair labor practice finding, it must be timely, unambiguous, specific in nature to the coercive conduct, and untainted by other unlawful conduct. There must be adequate publication of the repudiation to the employees involved, and the repudiation must assure employees that, going forward, the employer will not interfere with the exercise of their Section 7 rights.

In *First Transit, Inc.*, 360 NLRB 619, 622, 623 (2014), the Board stated:

> We agree that an employer's express notice to employees advising them of their rights under the Act may, in certain circumstances, clarify the scope of an otherwise ambiguous and unlawful rule. In our view, however, inclusion of the FOA policy in the handbook under the circumstances presented here does little to ensure that employees would not read otherwise overbroad rules as restricting their Section 7 rights. First, the policy is too narrow, focusing solely on union organizational rights. An effective "safe harbor" provision of this kind, also referred to as a "savings clause," should adequately address the broad panoply of rights protected by Section 7 of the Act . . . The policy does not expressly reference these rules and the rules do not expressly reference the policy.

The principal shortcoming of the Respondent's attempted savings clause is that it is written in a "generic" manner, while the unlawful restrictions are very specific. While the Respondent's Handbook provisions unlawfully restrict its employees use of "confidential information," and the use of the Respondent's logo, as well as cooperating with governmental investigations, the savings clause simply tells them that nothing contained in the handbook is intended to limit them from engaging in their rights protected by the Act, including protected concerted activities. This is far from language that is "specific in nature to the coercive conduct" and "does not expressly reference those rules," as required by *DirecTV* and *First Transit,* supra. I would further note that the Respondent did not notify its employees of its safe harbor rule until approximately seven months after it began maintaining the rules found to be unlawful in its Employee Handbook. I therefore find that the Respondent's attempt to repudiate the unlawful rules described herein is ineffective.

CONCLUSIONS OF LAW

1. The Respondent has been an employer engaged in commerce within the meaning of Section 2(2), (6), and (7) of the Act.

2. The Union has been a labor organization within the meaning of Section 2(5) of the Act.

3. The Respondent violated Section 8(a)(1) of the Act by unlawfully restricting its employees' use of information regarding their fellow employees and the Respondent's customers, the use of the Respondent's logo, and requiring the employees to notify Respondent's human resources representative prior to providing information for a government investigation.

THE REMEDY

Having found that the Respondent has unlawfully maintained rules restricting its employees use of what it considers confidential information regarding other employees and its customers, the use of Respondent's logo and the participation in governmental investigations without prior notice to the Respondent's human resources department, I recommend that the Respondent be required to rescind these provisions and notify all of its employees, nationwide that it has done so and that these provisions are no longer in effect and that it post a notice to its employees to this effect.

On the foregoing stipulated record, conclusions of law and the entire record, I hereby issue the following recommended[3]

ORDER

The Respondent, Macy's, Inc., its officers, agents, successors and assigns, shall

1. Cease and desist from

(a) Maintaining overly broad rules in its Employee Handbook that restrict its employees use of information regarding fellow employees and, but to a lesser extent, the Respondent's customers.

(b) Maintaining an overly broad rule in its employee handbook that restricts the use of the Respondent's logo.

(c) Maintaining an overly broad rule in its employee handbook that requires employees to notify the Respondent's human resources department prior to participating in a government

[3] If no exceptions are filed as provided by Sec. 102.46 of the Board's Rules and Regulations, the findings, conclusions, and recommended Order shall, as provided in Sec. 102.48 of the Rules, be adopted by the Board and all objections to them shall be deemed waived for all purposes.

investigation.

(d) In any like or related manner interfering with, restraining or coercing employees in the exercise of their rights guaranteed them by Section 7 of the Act.

2. Take the following affirmative action necessary to effectuate the policies of the Act.

(a) Within 14 days, rescind and/or revise all the rules referred to in paragraphs 1(a) through 1(c) above.

(b) Furnish all employees at all of the Respondent's facilities nationwide with (1) inserts for the current employee handbook that advise that the unlawful rules have been rescinded, or (2) the language of lawful rules on adhesive backing that will cover or correct the unlawful rules; or (3) publish and distribute a revised employee handbook that does not contain the unlawful rules.

(c) Within 14 days after service by the Region, post at all of its facilities nationwide copies of the attached notice marked "Appendix."[4] Copies of the notice, on forms provided by the Regional Director for Region 1, after being signed by the Respondent's authorized representative, shall be posted by the Respondent and maintained for 60 consecutive days in conspicuous places including all places where notices to employees are customarily posted. Reasonable steps shall be taken by the Respondent to ensure that the notices are not altered, defaced, or covered by any other material. In the event that, during the pendency of these proceedings, the Respondent has gone out of business or closed the facility involved in these proceedings, the Respondent shall duplicate and mail, at its own expense, a copy of the notice to all current employees and former employees employed by the Respondent at any time since September 5, 2013.

(d) Within 21 days after service by the Region, file with the Regional Director a sworn certification of a responsible official on a form provided by the Region attesting to the steps that the Respondent has taken to comply.

Dated, Washington, D.C. May 12, 2015

APPENDIX

NOTICE TO EMPLOYEES
Posted by Order of the
National Labor Relations Board
An Agency of the United States Government

The National Labor Relations Board has found that we violated Federal labor law and has ordered us to post and obey this notice.

FEDERAL LAW GIVES YOU THE RIGHT TO

Form, join, or assist a union

Choose representatives to bargain with us on your behalf

Act together with other employees for your benefit and protection

Choose not to engage in any of these protected activities.

WE WILL NOT maintain any rules in our Employee Handbook or elsewhere which restrict your right to discuss your wages and other terms or conditions of employment, or our customers or vendors, with your fellow employees and others;

WE WILL NOT maintain any rules in our employee handbook which restrict your right to talk to governmental agencies;

WE WILL NOT unlawfully restrict the right of others to use our logo in conjunction with your protected concerted activities; and

WE WILL NOT in any like or related manner interfere with, restrain or coerce you in the exercise of the rights listed above.

WE WILL, within 14 days, rescind and/or revise the overly broad rules described above; and

WE WILL furnish all employees with (1) inserts for the current employee handbook that advise that the unlawful rules have been rescinded, or (2) the language of lawful rules on adhesive backing that will cover or correct the unlawful rules, or (3) publish and distribute revised handbooks that do not contain the unlawful rules.

MACY'S, INC.

The Administrative Law Judge's decision can be found at www.nlrb.gov/case/01–CA–123640 or by using the QR code below. Alternatively, you can obtain a copy of the decision from the Executive Secretary, National Labor Relations Board, 1099 14th Street, N.W., Washington, D.C. 20570, or by calling (202) 273-1940.

[4] If this Order is enforced by a judgment of a United States court of appeals, the words in the notice reading "Posted by Order of the National Labor Relations Board" shall read "Posted Pursuant to a Judgment of the United States Court of Appeals Enforcing an Order of the National Labor Relations Board."