2019 IL App (1st) 182676

No. 1-18-2676

Opinion filed December 3, 2019

SECOND DIVISION

IN THE

APPELLATE COURT OF ILLINOIS

FIRST DISTRICT

MONICA RIVERA, Individually and on Behalf of All Others Similarly Situated, Plaintiff-Appellant, v. COMMONWEALTH EDISON COMPANY and EXELON CORPORATION, Defendants-Appellees.	)	Appeal from the Circuit Court of Cook County No. 17-CH-07460 The Honorable Raymond W. Mitchell, Judge Presiding.

PRESIDING JUSTICE FITZGERALD SMITH delivered the judgment of the court, with opinion.

Justice Coghlan concurred in the judgment and opinion.

Justice Pucinski specially concurred, with opinion.

OPINION

¶ 1 The plaintiff, Monica Rivera, filed a class action complaint against the defendants, Commonwealth Edison Company (ComEd) and Exelon Corporation (Exelon), alleging that they violated her rights under the Employee Credit Privacy Act (820 ILCS 70/1 *et seq.* (West 2016)) by investigating her credit history in connection with a conditional offer of employment as a customer service representative (CSR) and ultimately refusing to hire her because of the results of that investigation. The trial court granted summary judgment in favor of the defendants on the

plaintiff's claim. The plaintiff now appeals. For the reasons that follow, we affirm the trial court's entry of summary judgment.

¶ 2 I. BACKGROUND

¶ 3 ComEd is a public utility company that provides electrical services to approximately 3.8 million customers in Illinois. It is a subsidiary of Exelon, which is an electric utility holding company. On May 9, 2017, the defendants extended to the plaintiff a conditional offer of employment for a temporary part-time position as a CSR with ComEd, with a starting wage of $31.42 per hour. This was an entry-level position that required a high school diploma or equivalent. The offer of employment was contingent upon the completion of a successful background check, credit check, and drug screen. As part of this, the defendants obtained a consumer report on the plaintiff that included certain information about her credit history. On May 23, 2017, a representative of the defendants sent an e-mail to the plaintiff, rescinding the conditional offer of employment. That e-mail stated that "due, in part, to information received from the consumer report previously provided to you, we are not able to offer you employment at this time."

¶ 4 The plaintiff filed a class action complaint alleging that, by inquiring into her credit history and obtaining her credit report in connection with her application for the CSR position and by ultimately refusing to hire her for that position because of information contained in the report, the defendants violated her rights under the Employee Credit Privacy Act. See *id.* § 10(a). The plaintiff alleged that she was bringing the case on behalf of herself and other similarly situated individuals who had applied for the same position or other similarly titled positions with the defendants and had been subjected to a credit inquiry or check as a condition of employment.

¶ 5 The defendants answered the complaint and later filed a motion for summary judgment. In general, they argued in the motion for summary judgment that the prohibition on an employer's

investigation into an applicant's credit history or use of that credit history in connection with hiring decisions did not apply to the customer service representative position for which the plaintiff had been a candidate. They argued that the possession of a satisfactory credit history was a *bona fide* occupational requirement of that position because it " 'involves access to personal or confidential information' " of the defendants' customers. See *id.* § 10(b)(5). After conducting discovery pertaining to the issues raised in the defendants' motion and supporting affidavits, the plaintiff filed a response supported by depositions and other evidence.

¶ 6 The affidavits, depositions, and other evidence in the summary judgment record demonstrate the facts as follows. For any residence, business, or other entity within ComEd's service territory to obtain electricity, an account must be established with ComEd. This is the case even for customers who purchase electricity from a different supplier, as ComEd still delivers it. Thus, as ComEd provides electrical services to 3.8 million customers, it receives and stores a significant amount of information about its customers.

¶ 7 The primary database that ComEd uses to store information about its customers is its Customer Information Management System (CIMS). Access to CIMS is restricted to those ComEd employees who hold positions requiring them to use it in the course of their job duties. Over 2000 ComEd employees have some access to CIMS. Among those who have access, employees have varying levels of access to the information in the database, depending on what information they require to perform their job duties. ComEd denotes part of the information within CIMS as "personal identifiable information," which includes information such as a customer's Social Security number, tax ID number, driver's license number, credit card number, and bank account number. Access to such personal identifiable information is restricted to those positions and groups that are required to gather and use this information in the performance of their job duties. This

includes the customer care, billing, security, new business, and claims departments. CSR is one of the positions with access to the part of CIMS where customers' personal identifiable information can be entered into the database.

¶ 8 The job of ComEd's CSRs involves communicating by telephone with new and existing customers seeking to establish or transfer electrical service or making other inquiries concerning their service or account with ComEd. In certain situations, CSRs obtain or are able to view customers' full Social Security numbers. One situation in which CSRs obtain a customer's full Social Security number is when a new customer calls ComEd to establish service. As part of that process, CSRs validate the new customer's identity by requesting the customer's name and full Social Security number and entering that information into the CIMS database, where it is validated by Equifax. After that occurs, CSRs request additional information, including the new customer's date of birth and driver's license number, and enter that information into CIMS. After the appropriate information is obtained about the new customer and entered into CIMS, CSRs are no longer able to view the customer's full Social Security number in CIMS. Rather, only the last four digits of the number are visible to the customer service representative. The same occurs with customers' full driver's license numbers. Only the last several digits of these can be viewed in CIMS by a CSR after being entered.

¶ 9 Two additional situations in which CSRs obtain or can view a customer's full Social Security number are when a new customer's Social Security number is found to exist in another customer's record, and when a customer calls to inform ComEd that he or she has filed for bankruptcy and is entitled to have his or her electricity restored. In cases involving the duplication of a Social Security number, CSRs send an electronic communication to the revenue management department to resolve the issue. That communication typically includes the full Social Security number given

by the new customer. CSRs have the continued ability to view that communication, including the full Social Security number, until it is resolved by the revenue department, which can take up to 12 days. In cases where a customer reports declaring bankruptcy, CSRs ask the customer to provide either a full Social Security number or a bankruptcy case number. CSRs then send that information in an electronic communication to the bankruptcy or legal department. CSRs have the continued ability to view that communication, including the full Social Security number, until the customer's electricity is restored, which can take up to 30 days.

¶ 10 CSRs also obtain customers' bank account numbers and credit card information when customers call ComEd and provide this information to pay a bill or an overdue balance. After these numbers are initially inputted into CIMS, CSRs can no longer view the full bank account numbers or credit card numbers.

¶ 11 After ComEd initially obtains personal identifiable information from customers, its CSRs have the continued ability to view certain information in CIMS to perform their job duties and assist customers. This includes the ability to view partially redacted Social Security numbers, driver's license numbers, matricula numbers, bank account information, dates of birth, and address history for all current and former ComEd customers.

¶ 12 Eric Leslie, one of ComEd's senior trainers who provides training to CSRs in the performance of their duties, was questioned in his deposition about ComEd's "new business" department. This is a different department than the customer care department, in which CSRs work. Leslie testified that the new business department handles calls concerning newly constructed buildings or houses that require electrical infrastructure to be installed for ComEd to deliver electricity. He testified that those calls are not handled by CSRs. He testified that where the infrastructure already exists at a premises and a customer calls to put their name on the service there, such calls are handled by

CSRs in the manner described above.

¶ 13 ComEd employs approximately 500 CSRs, who work on two floors of an office building in Oak Brook, Illinois. They work in individual cubicles with two computer monitors and a pad of paper on which they can take notes during calls. Each CSR handles about 100 calls from customers each workday. The calls that CSRs handle are recorded and stored electronically in a database. CSRs' supervisors can listen during or after these calls, and they can also monitor the computer screens of the CSRs. ComEd also uses a third-party vendor, Clear Metrics, to monitor calls handled by CSRs for quality assurance purposes. Fewer than 1% of the calls handled by CSRs are actually monitored.

¶ 14 After a new customer establishes an account, ComEd sends a letter to the customer. The letter, a sample of which is included in the record, invites customers to visit the defendants' website. The letter does not specifically direct customers to the website for the purpose of accessing the defendants' privacy policy, nor does the record on appeal contain any other evidence of the defendants specifically directing customers to their website for the specific purpose of accessing the privacy policy. However, the privacy policy is generally available on the defendants' website and is included in the record on appeal. It states in part, "Through your use of our *** Services we may collect Personal Information ('PI'), which is information that identifies you as an individual or relates to you as an identifiable individual," including "your first and last name, home or business address, email address, and telephone number." It further states that the defendants "must collect certain PI and [personally identifiable information (PII)] if you choose to use our Services. PII includes information where your name is combined with your Social Security number, driver's license number, state identification card number, bank account number, credit card or debit card number, or unique biometric data."

¶ 15 The trial court granted the defendants' motion for summary judgment. The trial court concluded that the undisputed facts established that a satisfactory credit history was a *bona fide* occupational requirement of the CSR position that the plaintiff sought because the position " 'involves access to personal or confidential information.' " See *id.* As such, the trial court determined that the prohibition on an employer's investigating and considering a job applicant's credit history in making hiring decisions did not apply in this case. The plaintiff then filed a timely notice of appeal.

¶ 16 II. ANALYSIS

¶ 17 This case is before us on the trial court's granting of summary judgment in favor of the defendants, and thus, our standard of review is *de novo*. *Williams v. Manchester*, 228 Ill. 2d 404, 417 (2008). Summary judgment is proper where, when viewed in the light most favorable to the nonmoving party, the pleadings, depositions, admissions, and affidavits on file reveal that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law. *Hall v. Henn*, 208 Ill. 2d 325, 328 (2003); 735 ILCS 5/2-1005(c) (West 2018). The purpose of summary judgment is not to try a question of fact but to determine whether one exists. *Thompson v. Gordon*, 241 Ill. 2d 428, 438 (2011). If a dispute exists about a material fact, or if reasonable observers could draw divergent inferences from the undisputed material facts, then summary judgment should be denied. *Forsythe v. Clark USA, Inc.*, 224 Ill. 2d 274, 280 (2007).

¶ 18 The plaintiff's claim in this case was that the defendants' actions of investigating of her credit history in connection with the conditional offer of employment and ultimately refusing to hire her because of the results of that investigation violated section 10(a) of the Employee Credit Privacy Act, which provides as follows:

"(a) Except as provided in this Section, an employer shall not do any of the following:

> (1) Fail or refuse to hire or recruit, discharge, or otherwise discriminate against an individual with respect to employment, compensation, or a term, condition, or privilege of employment because of the individual's credit history or credit report.
>
> (2) Inquire about an applicant's or employee's credit history.
>
> (3) Order or obtain an applicant's or employee's credit report from a consumer reporting agency." 820 ILCS 70/10(a) (West 2016).

The defendants contended that the above prohibition on an employer's investigation into a job applicant's credit history or use of that credit history in connection with hiring decisions did not apply to the position for which the plaintiff had been a candidate. They argued that the CSR position at issue involved access to personal or confidential information of ComEd's customers, and therefore, it qualified for an exception under section 10(b)(5) of the Employee Credit Privacy Act. *Id.* § 10(b)(5). Section 10(b)(5) provides in pertinent part:

> "(b) The prohibition in subsection (a) of this Section does not prevent an inquiry or employment action if a satisfactory credit history is an established bona fide occupational requirement of a particular position or a particular group of an employer's employees. A satisfactory credit history is not a bona fide occupational requirement unless at least one of the following circumstances is present:
>
> * * *
>
> (5) The position involves access to personal or confidential information, financial information, trade secrets, or State or national security information." *Id.*

"Personal or confidential information" is a defined term in the Employee Credit Privacy Act, and it means "sensitive information that a customer or client of the employing organization gives explicit authorization for the organization to obtain, process, and keep; that the employer entrusts

only to managers and a select few employees; or that is stored in secure repositories not accessible by the public or low-level employees." *Id.* § 5.

¶ 19 The plaintiff raises several principal arguments on appeal that the CSR position at issue does not qualify for the exemption under section 10(b)(5). She argues that genuine issues of material fact exist about whether the information handled by ComEd's CSRs satisfied the statutory definition of "personal or confidential information." She also argues that a genuine issue of material fact exists about whether CSRs have "access" to such information, as opposed to merely serving as "conduits" who receive the information initially and then distribute it to other employees within ComEd. The plaintiff correctly notes that the defendants bear the burden of proving that an exemption applies to the position at issue. *Ohle v. The Neiman Marcus Group*, 2016 IL App (1st) 141994, ¶ 47.

¶ 20 A. Personal or Confidential Information

¶ 21 We first address the plaintiff's arguments concerning whether the information at issue satisfies the statutory definition of "personal or confidential information." In doing so, we note that the plaintiff does not challenge the fact that the information received by ComEd's CSRs constitutes "sensitive information." 820 ILCS 70/5 (West 2016). We agree that information such as Social Security numbers, driver's license numbers, bank account information, credit card numbers, and other similar information obtained by ComEd's CSRs meets this aspect of the statutory definition.

¶ 22 The plaintiff contends that the information at issue does not satisfy any of the three aspects of the statutory definition of "personal or confidential information." First, she argues that a genuine issue of material fact exists about whether CSRs themselves are "low-level employees," such as to show an issue of fact about whether the sensitive information at issue "is stored in secure

repositories not accessible by the public or low-level employees." See *id.* Second, she argues that a question exists about whether the number of CSRs employed by ComEd (approximately 500), as well as the total number of ComEd employees who have some level of access to the information in the CIMS database (approximately 2000), constitutes a "select few" employees, such as to raise an issue of fact about whether the defendants entrust the sensitive information at issue "only to managers and a select few employees." See *id.* Third, she argues that the defendants did not make a sufficient showing that customers gave "explicit authorization" for ComEd to "obtain, process, and keep" the sensitive information at issue. See *id.*

¶ 23 In support of her argument that CSRs are themselves low-level employees, the plaintiff relies on the fact that the position she was offered was a temporary, part-time position. She points out that it was an entry-level position, for which the educational requirements were a high school diploma or equivalent. She would have been paid hourly and not on a salary basis. Although the record does not appear to contain any evidence about the number of hours that the plaintiff would have worked in this position, she argues that, at a wage of $31.42 per hour, she would have earned "at most half" of the $65,000 earned by CSRs working full time. Additionally, she cites the fact that all of the phone calls that CSRs handle are recorded and stored in a database, where they can be monitored by supervisors or by Clear Metrics. She argues that "low-level employees" refers to employees without managerial control or authority over business operations, and the fact that CSRs are highly monitored, closely managed employees raises an issue of fact about whether they qualify as low-level employees.

¶ 24 By contrast, the defendants argue that ComEd's CSRs are not low-level employees. They argue that CSRs have a much higher level of responsibility for handling the sensitive information of customers than nearly all other employees of ComEd. They argue that the position is "highly

paid." They argue that, given that it is undisputed that part-time CSRs perform the same job, receive the same customer information, and are paid the same hourly wage as full-time CSRs, the fact that the plaintiff sought a part-time position did not make her a "low-level employee." They argue that the fact that the position was entry level is immaterial, given the level of responsibility that a CSR has for handling information about customers. They argue that the question of whether an employee is "low-level" does not hinge on whether the employee has managerial or supervisory responsibilities.

¶ 25 No definition of "low-level" employee is contained in the Employee Credit Privacy Act. Thus, we are presented with an issue of statutory interpretation, in which our role is to ascertain and give effect to the intent of the legislature. *General Motors Corp. v. State of Illinois Motor Vehicle Review Board*, 224 Ill. 2d 1, 13 (2007). The best evidence of legislative intent is the language used in the statute itself, which must be given its plain and ordinary meaning. *Paris v. Feder*, 179 Ill. 2d 173, 177 (1997). Words and phrases should not be considered in isolation but, rather, they must be interpreted in light of other relevant provisions and the statute as a whole. *County of Du Page v. Illinois Labor Relations Board*, 231 Ill. 2d 593, 604 (2008). In addition to the statutory language, the court may consider the purpose behind the law, the evils sought to be remedied, and the consequences that would result from interpreting the law one way or the other. *Id.*

¶ 26 Here, the plain and ordinary meaning of "low-level," as defined in the dictionary, is "being of low importance or rank." Merriam-Webster's Collegiate Dictionary 691 (10th ed. 1998). If we considered this phrase in isolation, we might conclude that, because there is no indication of how "low" in importance or rank the employees must be, the plaintiff proposes a reasonable interpretation that low-level employees "refers to employees without managerial control or

authority over business operations." However, we must interpret the term in the context of the statute as a whole. It appears in the aspect of the statute describing "sensitive information *** that is stored in secure repositories not accessible by the public or low-level employees." 820 ILCS 70/5 (West 2016). The term "low-level employees" is used in conjunction with "the public." This indicates a level of employee whose need or ability to access sensitive information stored in secure repositories is of a level similar to that of the public in general. ComEd's CSRs would not fall within this category of employees, because it is undisputed that their need and ability to obtain and use the information of ComEd's customers to perform their job duties is much greater than that of the general public. Therefore, they are not "low-level employees" within the meaning of the statute.

¶ 27 Further, there is no genuine issue of material fact that ComEd stores the sensitive information it possesses about its customers in a secure repository, the CIMS database. This database is not accessible to the public, and ComEd restricts access to the database to those of its employees who hold positions requiring them to use it. Thus, although approximately 2000 ComEd employees have some access to CIMS, there are many employees of ComEd who cannot access it because their job duties do not require it. These would include the "low-level employees" referred to in the statute, whose need or ability to access the information in CIMS is no greater than that of the public in general.

¶ 28 We therefore hold that no genuine issue of material fact exists about whether the information at issue satisfies the statutory definition of "personal or confidential information" because it is "sensitive information *** that is stored in secure repositories not accessible by the public or low-level employees." *Id.* As the satisfaction of any one aspect of the definition is sufficient, we do not need to consider the plaintiff's alternative arguments that the number of ComEd employees who

can access the information indicates that it is not entrusted "only to managers and a select few employees," or that there is no evidence that customers gave "explicit authorization" for ComEd to "obtain, process, and keep" the information at issue. To the extent that the plaintiff's argument suggests that all three aspects of the statutory definition must be satisfied, we reject this argument. The use of the word "or" in the statute indicates that these are three different alternatives and establishing any one of the three alternatives is sufficient to satisfy the statutory definition of "personal or confidential information." See *Elementary School District 159 v. Schiller*, 221 Ill. 2d 130, 145 (2006).

¶ 29 B. "Access" to Personal or Confidential Information

¶ 30 The plaintiff next argues that a genuine issue of material fact exists about whether CSRs have "access" to personal or confidential information within the meaning of section 10(b)(5) of the Employee Credit Privacy Act. 820 ILCS 70/10(b)(5) (West 2016). She argues that ComEd's CSRs are merely "conduits" whose role is merely to receive customers' information initially and pass it on to the other responsible departments within ComEd, and not thereafter to process, keep, or access customers' information. She also argues that the ability to view the redacted information of customers in CIMS is insufficient to amount to "access" under section 10(b)(5). Both parties argue that their respective positions are supported by this court's decision in *Ohle*, 2016 IL App (1st) 141994, which analyzed the meaning of the word "access" as used in section 10(b)(5).

¶ 31 In *Ohle*, the plaintiff was a candidate for an entry-level position as a dress-collection sales associate at one of the defendant's retail stores. *Id.* ¶ 2. The defendant obtained a credit check of the plaintiff in conjunction with a potential job offer and elected not to hire her after she failed it. *Id.* ¶¶ 2, 5. The issue on appeal in the plaintiff's ensuing lawsuit was whether the sales associate position involved "access" to personal or confidential information of customers within the

meaning of section 10(b)(5). *Id.* ¶ 22. The evidence in the case demonstrated that sales associates' jobs were to sell the defendant's merchandise to the public. *Id.* ¶ 6. Sales associates were heavily supervised, both by store managers and by the loss prevention teams using surveillance cameras. *Id.* Part of their jobs included encouraging customers to open store credit cards. *Id.* ¶ 8. They could accept customers' applications for such cards, and these applications would contain the customer's date of birth, Social Security number, driver's license number, and income information. *Id.* It was disputed whether the sales associates would input some or all of this information into an encrypted database in the point-of-sale (POS) register, or whether they merely received the applications, placed them in a locked drawer in the POS register, and delivered them to the cash department at the end of the day. *Id.* ¶¶ 8, 23, 32, 34-35. They were prohibited from keeping or accessing any personal customer information from the POS terminals or through any other means. *Id.* ¶¶ 8, 32, 36.

¶ 32 In its analysis, the court considered that the legislature's intent in enacting the Employee Credit Privacy Act was to protect employees and prospective employees from having their credit histories used in employment decisions for jobs in which credit history was not relevant. *Id.* ¶¶ 17, 29. The court rejected the defendant's argument that the facts above demonstrated that its sales associates had "access" to personal or confidential information within the meaning of section 10(b)(5). *Id.* ¶¶ 37-40. In doing so, the court explained part of its reasoning as follows:

> "Neiman Marcus requires the sales associates keep the applications locked in their cash drawer until the end of the work day or immediately give them to a manager. Only managers and credit office and loss prevention employees can see the customer information in the computer database and can obtain, keep, or process that information. In sum, Neiman Marcus does not permit sales associates to do any of the above. A sales associate essentially

> acts as a conduit by (1) receiving the application from the customer, ensuring it gets to Neiman Marcus manager or trusted employee, or (2) entering the information into the POS system for immediate credit approval, which is a task no more sensitive in nature than entering credit card numbers into a credit card machine or taking down driver's license information to accept a personal check in order to complete a sales transaction. *** Therefore, we find it is Neiman Marcus managers and select few employees (credit office personnel and loss prevention), who have 'access' to personal and confidential customer information as contemplated by section 10(b)(5) and not Neiman Marcus dress collection sales associates." *Id.* ¶ 37.

The court recognized that if "access" were interpreted so broadly as to exempt employees who simply received a credit card application and placed it in a drawer for processing at a later time by a different department, the Employee Credit Privacy Act "would in effect accomplish nothing." *Id.* ¶ 39. The court went on to state:

> "In the context of this case, 'access' to credit application information would pertain to the employees that process the credit application, receive the customer's credit report, analyze the customer's detailed financial history and make the decision on whether to extend credit. *** Only a select group of Neiman Marcus employees in the loss prevention, customer service, and the credit department have access to credit card applications after they were submitted, and only employees in those departments can access the encrypted customer information obtained from further processing of the customer's credit history. Those are the types of positions that the legislature contemplated as having 'access' to personal or confidential information subject to section 10(b)(5) of the Act, not the type of position plaintiff sought." *Id.* ¶ 40.

¶ 33 Here, the plaintiff argues that ComEd's CSR position is similar to the sales associate position in *Ohle*. The plaintiff points out that the CSR position is an entry-level position requiring only a high-school diploma or equivalent.[1] She also points out that CSRs are subject to having their telephone calls or computer activity monitored by supervisors, the quality assurance department, and Clear Metrics. She argues that CSRs "are admittedly mere conduits entering information into the ComEd database and nothing more." She contends that, when customers call to set up a new account, CSRs input the customers' Social Security numbers, driver's license numbers, and bank account numbers into CIMS "for processing by the new business department." She contends that CSRs "indisputably do not process the information," and after inputting it into CIMS, they are prohibited from accessing the full Social Security numbers or other information.

¶ 34 We reject the plaintiff's argument that the access of ComEd's CSRs to customers' personal or confidential information is similar to that of the dress-collection sales associate in *Ohle*. In that case, the evidence demonstrated that after a sales associate received credit card applications and either entered information into the POS system for immediate credit approval or placed them in a locked drawer in the POS register until they could be delivered to the responsible department for processing, the sales associate had no further ability to "see the customer information in the computer database" or to "obtain, keep or process that information." *Id.* ¶ 37. Here, by contrast, the evidence shows that CSRs, after initially inputting the information into CIMS, continue throughout their employment to have the ability to view at least partial Social Security numbers, driver's license numbers, bank account numbers, and credit card numbers, in addition to customers' names, address histories, dates of birth, and other identifying information. Moreover,

[1]*Ohle* did not involve the issue, addressed above, of whether the defendants' sales associates were "low-level employees."

the evidence shows that CSRs use this customer information routinely to assist customers as part of their job duties.

¶ 35 We do not find any relevance in the fact that the CSR position sought by the plaintiff was entry-level or temporary. As explained above, the evidence demonstrates that regardless of its entry-level or temporary nature, it involves access to personal or confidential information. Also, the plaintiff contends that ComEd's CSRs are subjected to a level of surveillance or monitoring in their jobs that is comparable to that of the sales associate in *Ohle*. We disagree. Although the evidence demonstrates that CSRs are subjected to having their telephone calls or computer activity recorded or monitored, the evidence further shows that less than one percent of the calls handled by CSRs are actually monitored. Therefore, we conclude that nothing about the level of monitoring or surveillance experienced by ComEd's CSRs affects whether that position involves access to the personal or confidential information of customers.

¶ 36 We find that the plaintiff incorrectly characterizes the evidence when she states that CSRs merely input customer information into CIMS "for processing by the new business department." As Eric Leslie testified in his deposition, ComEd's new business department handles calls concerning newly constructed premises that require the installation of electrical infrastructure to receive electricity. He testified that CSRs do not handle those calls but, rather, they handle calls in situations when the infrastructure already exists and customers need their names added to the accounts. The evidence cited by the plaintiff does not establish that the new business department "processes" the information collected by the CSRs, or that any other department processes that information to the exclusion of the CSRs themselves.

¶ 37 Furthermore, we reject the plaintiff's contention that the defendants' own witnesses agree that the CSRs are "merely conduits" who " 'just put all the information into the system' " but do

not process it. The testimony that the plaintiff cites for this proposition, which is from the deposition of ComEd employee Juan Rivera, is as follows:

> "MR. STEPHAN [(PLAINTIFF'S ATTORNEY)]: Would you agree that [CSRs are] sort of a conduit between the customers and the field?
>
> MS. ARGENTIERI [(DEFENDANTS' ATTORNEY)]: Object to form. Vague.
>
> MR. RIVERA: In a sense, I mean, I guess they can be.
>
> MR. STEPHAN: In other words, they collect information from the customers about outages, service calls, whatever, and they communicate that, and it goes up the chain to the technicians in the field who perform the service?
>
> MR. RIVERA: Correct. Yeah, they just put all the information into the system. Right."

The only information that Juan Rivera was questioned about in this exchange involved outages and service calls. This exchange had nothing to with CSRs' responsibilities with regard to the kind of personal or confidential information of customers that is at issue in this case. It does not support the proposition for which it is cited by the plaintiff.

¶ 38 Finally, the plaintiff argues that the fact that CSRs can only view partial Social Security numbers, driver's license numbers, and the like, as opposed to the full numbers, should not trigger the exception at issue. She contends that in *Ohle*, the sales associates "had the ability to view encrypted or redacted information as part of their job duties." We believe that the plaintiff is misreading the facts of *Ohle* and downplaying the amount of customer information that the record discloses that ComEd's CSRs can actually view. As stated above, in that case, the sales associates, after initially processing the credit card applications, had no further ability to see any sensitive information of customers in the computer database or to obtain, keep, or process that information.

Id. Only employees in the defendant's loss prevention, customer service, and credit departments had access to credit card applications after they were submitted or "can access the encrypted customer information obtained from further processing of the customer's credit history." *Id.* ¶ 40. Here, by contrast, the uncontested evidence shows that ComEd's CSRs have the ongoing ability to view in CIMS customers' partial Social Security numbers, driver's license numbers, bank account numbers, and credit card numbers, in conjunction with customers' names, address histories, dates of birth, and other identifying information. With the ongoing ability to view this information and use it as part of their jobs, their position is closer to that of the employees in the loss prevention, customer service, and credit departments of the defendant in *Ohle* than that of the sales associate. The fact that these numbers are only partially visible to CSR does not mean that the position does not involve "access to personal or confidential information" of the customers of ComEd.

¶ 39 III. CONCLUSION

¶ 40 For the foregoing reasons, we affirm the trial court's entry of summary judgment in favor of the defendants and against the plaintiff.

¶ 41 Affirmed.

¶ 42 JUSTICE PUCINSKI, specially concurring:

¶ 43 I agree with the analysis and result in this matter; however, I write specially to point out that since the legislature did not define the word "access," we are left to decide if some job applicants will or will not have "access" to confidential information.

¶ 44 Here the CSRs at Commonwealth Edison clearly had access to customers' confidential information because the CSR first had to get that information verbally from the customer over the phone, certainly for all new customers, and sometimes for existing customers to resolve a problem.

¶ 45 Getting that information gives any CSR immediate access to confidential information that they keyboard onto a screen. That information is not secured until the next step, actually pushing it into the encrypted data system. Old fashioned pencil and paper and certainly the glitzier cell phones with cameras and recorders give any CSR gathering that information the opportunity to hijack it. While we hope that the vast majority of CSRs will not hijack information, and thus, customer identities, it is becoming more and more apparent that limiting access to such information is a fundamental security issue.

¶ 46 That being said, and with the greatest respect to the author and my colleagues who decided *Ohle*, it appears to me that the case was wrongly decided. The salespersons at Neiman Marcus had firsthand access to the confidential information their customers were providing to apply for a store credit card. It would only take a few seconds to voice record the information, take a photograph of it on a cell phone camera, or just plain write it down before hitting the "enter" key to push it into the secure part of the system. If the information was written by the customer on an actual paper application, the same opportunity for mischief exists.

¶ 47 While I am sympathetic to the idea that the exemption should not swallow the rule, where we must protect the right of people to apply for a job, we must also protect the right of people to the security of their confidential information.

¶ 48 I would find that "access" exists from the moment confidential information is given to any employee for the purpose of furthering that employer's ability to provide service to a customer. Without more significant security protocols in place, applicants for those positions are expected to conform to the employer's hiring security policies.

No. 1-18-2676

Cite as:	*Rivera v. Commonwealth Edison Co.*, 2019 IL App (1st) 182676
Decision Under Review:	Appeal from the Circuit Court of Cook County, No. 17-CH-07460; the Hon. Raymond W. Mitchell, Judge, presiding.
Attorneys for Appellant:	Ryan F. Stephan, James B. Zouras, Andrew C. Ficzko, and Anna M. Ceragioli, of Stephan Zouras, LLP, of Chicago, for appellant.
Attorneys for Appellee:	Neil H. Dishman, Julia P. Argentieri, and Nicholas A. Simpson, of Jackson Lewis P.C., of Chicago, for appellees.