

[Cite as *Rebello v. Lender Processing Servs., Inc.*, 2015-Ohio-1380.]

# Court of Appeals of Ohio

EIGHTH APPELLATE DISTRICT  
COUNTY OF CUYAHOGA

---

JOURNAL ENTRY AND OPINION  
No. 101764

---

**CARRIE REBELLO**

PLAINTIFF-APPELLANT

vs.

**LENDER PROCESSING  
SERVICES, INC., ET AL.**

DEFENDANTS-APPELLEES

---

**JUDGMENT:  
REVERSED AND REMANDED**

---

Civil Appeal from the  
Cuyahoga County Court of Common Pleas  
Case No. 12-CV-785870

**BEFORE:** E.A. Gallagher, P.J., E.T. Gallagher, J., and Laster Mays, J.

**RELEASED AND JOURNALIZED:** April 9, 2015

**ATTORNEYS FOR APPELLANT**

Andrew A. Kabat  
Daniel M. Connell  
Haber Polk Kabat, L.L.P.  
737 Bolivar Rd. Suite 4400  
Cleveland, Ohio 44115

**ATTORNEYS FOR APPELLEES**

James E. Davidson  
Mary F. Geswein  
Ice Miller L.L.P.  
250 West Street, Suite 700  
Columbus, Ohio 43215

EILEEN A. GALLAGHER, P.J.:

{¶1} Plaintiff-appellant Carrie Rebello appeals from the trial court’s judgment entering a directed verdict on her claim for wrongful discharge in violation of public policy against defendants-appellees Lender Processing Services, Inc., et al. (collectively, “LPS”).<sup>1</sup> Rebello claims that she was wrongfully terminated in violation of public policy from her employment at LPS because she objected to, and threatened to, report LPS’s practice of password sharing among LPS employees when accessing the nonpublic customer information of one of its largest clients, JPMorgan Chase Bank, N.A. (“Chase”). For the reasons that follow, we reverse the trial court’s judgment.

### **Procedural and Factual Background**

{¶2} LPS is in the business of providing processing, technology and field services to clients, including mortgage lenders and financial institutions. The services provided by LPS include inspections, property validation for repairs and services and loss mitigation in connection with defaulted assets. From August 2009 until her termination on April 11, 2012, Rebello was employed by LPS as a supervisor in its property

---

<sup>1</sup> Rebello’s original complaint was filed against Lender Processing Services, Inc., LPS Field Services, Inc., FIS Field Services, Inc., LPS Management, L.L.C. and Lori Fryer. In June 2014, Rebello was granted leave to file an amended complaint adding Black Knight InfoServe, L.L.C., Black Knight Field Services, L.L.C., Black Knight Management Service, L.L.C., ServiceLink Field Services, Inc. and ServiceLink Management Company, L.L.C. as additional defendants due to various corporate name changes that had occurred. On July 11, 2014, the parties entered into a stipulation agreeing that the real parties in interest in the case were ServiceLink Field Services, Inc. (formerly known as FIS Field Services, Inc., LPS Field Services, Inc. and Black Knight Field Services), Black Knight InfoServe Inc. (formerly known as Lender Processing Services, Inc.), Black Knight Management Services, Inc. (formerly known as LPS Management, L.L.C.) and Lori Fryer. These entities are collectively referred to herein as “LPS.”

preservation department. She worked in LPS's Solon, Ohio office. Rebello supervised a team of employees who provided field services for properties owned by customers of Chase that were in default or foreclosure. In performing property preservation services for Chase, LPS employees used a secured, electronic database (the "MSP system") to access the nonpublic information of Chase's customers. Accessing the MSP system involved a two-step process: (1) Chase provided tokens to LPS employees that included random PIN numbers and (2) LPS employees were required to enter a username and password after using the token. All LPS employees were screened by both Chase and LPS before receiving log-in credentials. Chase, however, ultimately controlled who at LPS was authorized to access Chase's customer information on the MSP system. For LPS employees to be authorized to access Chase's customer information, they had to be both (1) authorized by LPS to work on the Chase account and (2) authorized by Chase to access Chase's account information through the MSP system. This process included training, a background check and a drug test. Once authorized by Chase, the LPS employee received a token and a unique username/password to access the MSP system.

{¶3} Over the course of the relationship between LPS and Chase, LPS employees encountered difficulties in accessing the MSP system due to delays in receiving the authorizations or tokens necessary to access the system. As a "work around" to the access problem, LPS employees began to share tokens, usernames and/or passwords ("password sharing").

{¶4} Both LPS and Chase had clear policies prohibiting password sharing among LPS employees. Section 10.3 of the Master Agreement governing the relationship between Chase and LPS (the “Master Agreement”) provided:

Login Ids for System Access

JPMC [Chase] will assign a login code (a “**Login ID**”) to each of the

Supplier [LPS] Personnel who will have access to the JPMC Systems.

Only the individual who was assigned a Login ID may use that Login ID.

Supplier will not permit any Login ID to be shared or used by any other

individual. Supplier will be responsible for all access to the JPMC

Systems by any person using a Login ID issued to any of the Supplier

Personnel.

Section 10.5 of the agreement further provided that LPS was to immediately notify Chase of any actual or threatened and confirmed security breach in or unauthorized access to Chase’s systems.

{¶5} Jack Evans, Chase’s vice president in property preservation and the Chase relationship manager or “point person” for LPS, testified that Chase’s password policy was designed to prevent unauthorized use and disclosure of nonpublic information belonging to Chase’s customers. LPS’s management similarly acknowledged that Chase’s and LPS’s anti-sharing policies were designed, at least in part, to help prevent unauthorized persons from accessing Chase’s customers’ nonpublic information. For example, Curtis Larson, Rebello’s supervisor from 2009 to October 11, 2011, testified that “the concept” of prohibiting password sharing was “to help protect those who were

not authorized and did not have the ability to otherwise access a consumer's [nonpublic information]." Lori Fryer, Rebello's supervisor from October 2011 until her termination in April 2012, similarly acknowledged that if passwords were shared among LPS employees, the confidentiality of Chase's customers' nonpublic information could be jeopardized. Notwithstanding their knowledge of the policies prohibiting password sharing, LPS's property preservation supervisors and managers did not stop the practice because they felt they needed to share passwords in order to handle the volume of business that Chase was assigning to LPS. Evans testified that, other than a couple of days in February 2010, when LPS employees were having problems logging onto the MSP system and Chase granted LPS employees permission to share passwords, he was not aware that LPS employees were sharing passwords. Evans further testified that he believed the subsequent password sharing he later learned was occurring among LPS employees violated the master agreement because "when passwords were being shared, that meant somebody had unauthorized access to personal customer information that they were not entitled to" but that he was not aware of "any unauthorized disclosure of any non-public information by LPS" or "any individuals who somehow suffered any kind of damage" as a result of password sharing by LPS.

{¶6} Rebello testified that she first learned that LPS employees were sharing passwords in January 2010. She testified that she thereafter had several discussions with her then supervisor, Larson, regarding the issue. She testified that Larson responded that password sharing was "a temporary fix." Larson acknowledged that Rebello had raised

concerns regarding password sharing with him. Although he did not recall specifically what was said, he testified that he recalled telling Rebello something to the effect of “[m]anagement is working on the issue. Continue to focus on your job.” Larson further testified that upper management was aware that password sharing was occurring and that although he knew LPS had an obligation under its contract with Chase to immediately notify Chase of any unauthorized access to the MSP system and to inform Chase that its employees were sharing passwords, LPS did not inform Chase that its employees were sharing passwords, deciding instead “to handle the matter internally.” Despite her concerns regarding password sharing, Rebello testified that she was aware that other LPS employees were using her password to work on the Chase account.

{¶7} Password sharing intensified in October 2011, when Chase began to “dramatically increase” the volume of work being handled by LPS. At that time, Lori Fryer took over management of the Chase account. To handle the increased workload, LPS hired additional employees and requested additional authorizations from Chase for those employees to access the MSP system. LPS was unable to get Chase to promptly assign passwords and grant access to all the LPS employees who were hired to work on the Chase account. As a result, LPS’s employees did not have sufficient access to the MSP system and resorted to password sharing to perform the work LPS was receiving from Chase.

{¶8} Rebello testified that shortly after Fryer took over management of the Chase account in October 2011, Rebello had discussions with her regarding password sharing.

Rebello testified that she told Fryer that there was a problem with password sharing and that they needed to address it and get additional access from Chase. Fryer told her to “[s]tay the course” and that she was handling the issue. Fryer testified that at the time, she knew that password sharing was prohibited by Chase’s and LPS’s policies, put the nonpublic information of Chase’s customer’s at risk and exposed both Chase and LPS to potential violations of the law. She further testified that although she knew she had an obligation to inform Chase that passwords were being shared, she did not disclose the practice to Chase because she knew it was prohibited and did not want to risk losing the Chase account. Fryer did not inform her supervisors that passwords were being shared. Instead, Fryer testified, she contacted Chase executives and requested that they become more involved in acquiring the number of tokens LPS employees needed to access the MSP system.

{¶9} In February 2012, an employee who had worked in LPS’s Denver office reported to human resources, in connection with her resignation from the company, that her group had been sharing passwords. In response to the incident, a conference call was held with all of the property preservation department supervisors (including Rebello), Fryer, Fryer’s supervisor, Tim Guertin and Guertin’s supervisor, Pat Gluesing. During the call, upper management stated that password sharing “must stop.”

{¶10} After the call, Rebello became “animated” about password sharing, expressing her concern to Fryer that everyone was going to be fired. Fryer testified that she told Rebello to “calm down,” “stay the course” and “to focus on her team and



production.” Fryer testified that Rebello asked who was going to tell Chase about LPS’s password sharing. Fryer responded that it was not their responsibility to communicate that information to Chase and that it would be handled through appropriate channels in the Information Security Office (“ISO”). Although Fryer testified that it was her “expectation” that no one in her department was sharing passwords after the call, LaSheen Farley, another supervisor working on the Chase account who reported to Fryer testified that Fryer allowed password sharing to continue in their department until July 2012.

{¶11} On February 29, 2012, Rebello and other LPS employees received an email from LPS’s Human Resource Manager addressing password security, which stated in relevant part:

Please read the attached reminder about password security. As LPS employees we are all responsible for maintaining the integrity and security of our systems and or clients['] systems that we have access to. Do NOT share your passwords with anyone for any reason. Violations of our Company policies, including security policies, may lead to disciplinary action up to and including termination.

The attachment provided information regarding the creation of strong passwords and protecting passwords and also provided:

It is important all LPS employees understand the importance of using a strong password and not sharing logins/passwords for any purpose as outlined in the below excerpt from the LPS Employee Handbook. This policy applies to all systems/electronic equipment requiring a user name and/or password that you have access to including clients, suppliers, etc.

If you receive an assignment that requires access to a system that either you or one of your direct reports do not have, please let your supervisor know so \* \* \* other arrangements can be made \* \* \* until needed access has been obtained.

## **In the LPS Employee Handbook under Electronic Communications**

**System Integrity and Security:** Employees may not use any personal login and/or password that have been assigned to anyone other than the Employee.

**Consequences of Policy Violations:** Violations of this Policy may result in disciplinary action up to and including **immediate termination of an employee's employment as well as possible civil liabilities or criminal prosecution.** Where appropriate, the Company may advise legal officials or appropriate third parties of policy violations and cooperate with official investigations. We will not, of course, retaliate against anyone who reports possible policy violations or assists with investigations.

{¶12} Rebello testified that after the conference call and February 29, 2012 email, she determined that the practice of password sharing “must stop” as it related to her team because she did not want to subject her team to a risk of termination, civil liability or criminal prosecution as set forth in the February 29, 2012 email. She testified that approximately two weeks after receiving the email, she again spoke with Fryer regarding her concerns about password sharing. Rebello testified that she told Fryer “it had to absolutely stop” and that she was going to instruct her team not to share passwords anymore “even if it meant our volume was going to plummet.” She further testified she told Fryer that Chase needed to be advised that they had been previously sharing passwords, that they were not sharing passwords any longer and that, as a result, their production was going to “decrease considerably.” Rebello testified that she told Fryer that if the issue was not resolved, she was going to raise the issue with upper management or Chase. Rebello testified that Fryer told her that “ISO would handle it.”

{¶13} Rebello testified that she then instructed her assistant supervisors that password sharing would no longer be permitted on her team. Rebello claimed that, before she could raise her concerns regarding password sharing to “the next level,” she was terminated.

{¶14} LPS denied that Rebello was terminated due to her threats to disclose LPS’s practice of sharing passwords and claimed that she was terminated due to an “outburst of profanity on the production floor” and other performance issues. Fryer testified that in early March she raised concerns regarding Rebello’s tardiness and attendance with human resources. A coworker thereafter complained to Fryer regarding an incident that occurred on April 2, 2012, in which Rebello used profanity during a personal telephone call. The coworker claimed the incident was disruptive and made him uncomfortable. Fryer reported the incident to human resources that investigated the complaint. Lisa Miles, the human resources representative who conducted the investigation, testified that she learned that this was not the first time such an incident had occurred involving Rebello and that other coworkers had been similarly bothered by Rebello’s disruptive personal telephone calls. Miles testified that based on her investigation, human resources recommended that Rebello be terminated.

{¶15} LPS thereafter decided to terminate Rebello’s employment. Rebello’s “termination document” indicated that she was terminated for disrupting the work environment, unsatisfactory performance, violation of policies and procedures, challenges with supervisory execution and challenges with attendance, punctuality and time off.

Rebello denied that her April 2, 2012 telephone call was disruptive. She also denied that she had attendance issues and claimed that she was not told about any alleged performance issues prior to her termination and, therefore, could not state whether the specific concerns raised with regard to her performance were accurate.

{¶16} On June 27, 2012, Rebello filed a complaint against LPS, alleging that her employment was wrongfully terminated in violation of public policy. Rebello claimed that she was terminated because she told the employees she supervised that they were not to share passwords or access Chase customer information from unsecured locations under any circumstances and advised her supervisor that Chase “must be told of the past, and ongoing, violations relating to customer, non-public personal information.” Rebello alleged that the termination of her employment, shortly after these discussions, “implicated” and “was motivated by and causally connected to” “several clear public policies,” including, but not limited to, policies prohibiting the unauthorized disclosure of nonpublic confidential information found in the Gramm-Leach-Bliley Act, 15 U.S.C. 6801, et seq. and its implementing regulations, the Fair Credit Reporting Act, 15 U.S.C. 1681, et seq., the Fair Debt Collection Practices Act, 15 U.S.C. 1692 et seq., and R.C. 1349.19. Rebello sought to recover compensatory and punitive damages from LPS as a result of her alleged wrongful termination.

{¶17} On August 1, 2012, LPS filed a motion to dismiss Rebello’s complaint pursuant to Civ.R. 12(B)(6), asserting that none of the statutes or regulations Rebello had identified in her complaint “involves public policy concerns as a matter of law” and that,

as such, Rebello had failed to state a claim for wrongful discharge in violation of public policy. LPS argued that Rebello's allegations "did not implicate public policy concerns" and that the statutes and regulations identified in Rebello's complaint either did not apply to LPS or were not triggered by any conduct alleged by Rebello. Rebello opposed the motion, asserting that the laws and regulations she had identified require entities such as LPS to maintain the security of nonpublic personal information and that she had alleged sufficient facts in her complaint demonstrating the applicability of these public policies in this case. The trial court denied LPS's motion to dismiss, concluding that "the statutes relied upon by plaintiff in her complaint implicate public policy concerns." LPS thereafter filed its answer, denying the material allegations of the complaint and asserting various affirmative defenses.

{¶18} After nearly a year-and-a-half of discovery, LPS filed a motion for summary judgment arguing, once again, that Rebello could not establish her claim for wrongful termination in violation of public policy as a matter of law. LPS argued that it was not subject to any of the four statutes Rebello relied on in support of her claim, that the objections that Rebello contended led to her termination were limited to "password sharing" and that there was nothing in any of the statutes cited by Rebello that prohibited "password sharing." Rebello opposed the motion. The trial court denied the motion, concluding that Rebello had satisfied the clarity and jeopardy elements of her claim and that genuine issues of material existed for trial regarding the causation and business justification elements of her claim.

{¶19} The case was then transferred to a visiting judge for trial. Trial commenced on July 14, 2014.

{¶20} At the close of the plaintiff's case, LPS moved for a directed verdict, arguing that Rebello had failed to establish the clarity and jeopardy elements of her claim because (1) she had complained only about "password sharing" (and never raised a concern regarding the disclosure of nonpublic information); (2) there was no law or public policy that prohibited "password sharing" in and of itself and (3) Rebello's concern regarding password sharing was based on a fear that she or others on her team would lose their jobs if they were found to have violated company policies prohibiting password sharing, not a concern that nonpublic information would be disclosed.<sup>2</sup> In response, Rebello argued that LPS's anti-password sharing policy was based on its obligations to maintain the security of nonpublic information under the Gramm-Leach-Bliley Act and that by objecting to password sharing as a policy violation, she was also implicitly objecting to LPS's failure to comply with its legal obligations under the act and its implementing regulations. Rebello further argued that she had presented evidence establishing that it was her threat to go to Chase "to vindicate her concern" that led to her termination. The trial court agreed with LPS. After hearing argument on the issue, the trial court granted the motion, concluding that Rebello had

---

<sup>2</sup> LPS also argued that Rebello had failed to satisfy the requirements for a statutory whistleblower claim. However, Rebello had not brought a statutory whistleblower claim and did not dispute that she had not satisfied the requirements for bringing such a claim.

failed to establish the clarity and jeopardy elements of her wrongful termination claim.

As the trial court explained:

This court finds that the plaintiff failed to articulate a specific, clear public policy and failed to prove that any public policy was jeopardized by her termination. The mere assertion relative to sharing passwords is insufficient to satisfy the clarity element of a wrongful termination action. There is no evidence before this court that anyone's confidential information or identity was compromised in any fashion. There is no evidence that the plaintiff's termination jeopardized any public policy.

The plaintiff failed to assert and prove a clear public policy derived from the state or federal constitution, a statute or administrative regulation or the common law. \* \* \* The complaint alleges but on[e] cause of action, that being a wrongful discharge in violation of public policy. Having failed as to the elements of clarity and causation [sic], this court will not address causation or whether or not the employer lacked a legitimate business justification for termination.

{¶21} Rebello timely appealed the trial court's judgment, raising the following assignment of error for review:

The trial court erred by granting Defendants-Appellees' motion for directed verdict on the grounds that Plaintiff failed to establish the clarity and jeopardy elements of her claim for wrongful discharge in violation of public policy.

## **Law and Analysis**

{¶22} As an initial matter, we first address the issue of whether the trial court erred in entering a directed verdict in favor of LPS based on Rebello's failure to satisfy the clarity and jeopardy elements of her claim, given its prior contrary ruling in favor of Rebello addressing the same issues. Rebello contends that because the original trial judge had ruled in her favor on LPS's motion for summary judgment, concluding that "plaintiff has satisfied the clarity and jeopardy elements of her claim," the visiting judge

lacked authority to direct a verdict in favor of LPS based on Rebello's failure to satisfy the clarity and jeopardy elements of her claim. We disagree.

{¶23} A trial court has plenary power to review its own interlocutory rulings before entering final judgment. *Tablack v. Wellman*, 7th Dist. Mahoning No. 04-MA-218, 2006-Ohio-4688, ¶ 38. Pursuant to Civ.R. 54(B), any order that adjudicates fewer than all of the claims between parties is subject to revision at any time before the entry of judgment adjudicating all the claims and the rights and liabilities of all the parties. The trial court's order on summary judgment was interlocutory in nature; it did not fully adjudicate Rebello's claim and, therefore, was not a final order. Accordingly, it was within the trial court's discretion to reconsider its prior summary judgment ruling at trial. *Tablack*, 2006-Ohio-4688 at ¶ 39, citing *State ex rel. Overmeyer v. Walinski*, 8 Ohio St.2d 23, 222 N.E.2d 312 (1966); *Frazier v. Rodgers Builders*, 8th Dist. Cuyahoga No. 91987, 2010-Ohio-3058, ¶ 64-67; *see also Gracetech Inc. v. Perez*, 8th Dist. Cuyahoga No. 96913, 2012-Ohio-700, ¶ 29.

{¶24} The fact that the visiting judge reconsidered the previous judge's ruling is of no consequence. "[V]isiting judges may, in their discretion, defer to the rulings of the original judge, but are also not prohibited from exercising discretion to revisit prior rulings." *Zappola v. Rock Capital Sound Corp.*, 8th Dist. Cuyahoga No. 100055, 2014-Ohio-2261, ¶ 35, citing *O'Connor v. Fairview Hosp.*, 8th Dist. Cuyahoga No. 98721, 2013-Ohio-1794, citing *Schultz v. Duffy*, 8th Dist. Cuyahoga No. 93215, 2010-Ohio-1750. Both decisions here were decisions of the Cuyahoga County Common



Pleas Court. “We should not look at them as decisions of particular judges.” *Tablack* at ¶ 40. Accordingly, the visiting trial judge was not precluded from reconsidering the assigned trial judge’s decision on summary judgment in ruling on LPS’s motion for directed verdict.

{¶25} We now turn to the merits of Rebello’s appeal.

### **Standard of Review**

{¶26} In her sole assignment of error, Rebello argues that the trial court erred when it granted LPS’s motion for a directed verdict. We review the grant or denial of a motion for directed verdict pursuant to a de novo standard of review. *Loreta v. Allstate Ins. Co.*, 8th Dist. Cuyahoga No. 97921, 2012-Ohio-3375, ¶ 5, citing *Grau v. Kleinschmidt*, 31 Ohio St.3d 84, 90, 509 N.E.2d 399 (1987). We construe the evidence presented most strongly in favor of the nonmoving party and determine whether reasonable minds could only reach a conclusion that is against the nonmoving party. *Sivit v. Vill. Green of Beachwood*, 8th Dist. Cuyahoga No. 98401, 2013-Ohio-103, ¶ 11, citing *Titanium Industries v. S.E.A. Inc.*, 118 Ohio App.3d 39, 691 N.E.2d 1087 (7th Dist.1997), citing *Byrley v. Nationwide Ins. Co.*, 94 Ohio App.3d 1, 640 N.E.2d 187 (6th Dist.1993). In considering whether a trial court properly granted a motion for directed verdict, we do not weigh the evidence or test the credibility of the witnesses. *Sivit* at ¶ 12. We assume the truth of the evidence supporting the facts essential to the claim of the party against whom the motion is directed and give that party the benefit of all reasonable inferences from that evidence. *Id.*, citing *Becker v. Lake Cty. Mem. Hosp. W.*,

53 Ohio St.3d 202, 206, 560 N.E.2d 165 (1990), citing *Ruta v. Breckenridge-Remy Co.*, 69 Ohio St.2d 66, 68, 430 N.E.2d 935 (1982).

{¶27} In Ohio, the common-law doctrine of employment at-will governs employment relationships. As such, an employer's termination of an at-will employee's employment relationship with the employer does not generally give rise to an action for damages. *Dohme v. Eurand Am., Inc.*, 130 Ohio St.3d 168, 2011-Ohio-4609, 956 N.E.2d 825, ¶ 11, citing *Collins v. Rizkana*, 73 Ohio St.3d 65, 67, 652 N.E.2d 653 (1995). If, however, an employee is terminated in contravention of a clear public policy articulated in the Ohio or United States Constitution, federal or state statutes, administrative rules and regulations or the common law, a cause of action for wrongful termination in violation of public policy may exist as an exception to the general rule. *Painter v. Graley*, 70 Ohio St.3d 377, 639 N.E.2d 51 (1994), paragraphs two and three of the syllabus.

{¶28} To prevail on a claim of wrongful discharge in violation of public policy, a plaintiff must establish four elements: (1) that there exists a clear public policy that is manifested in a state or federal constitution, statute or administrative regulation or in the common law (the "clarity element"); (2) that dismissing employees under circumstances like those involved in the plaintiff's dismissal would jeopardize the public policy (the "jeopardy element"); (3) that the plaintiff's dismissal was motivated by conduct related to the public policy (the "causation element"); and (4) that the employer lacked an

overriding legitimate business justification for the dismissal (the “overriding justification element”).

*Collins*, 73 Ohio St.3d at 69-70. The clarity and jeopardy elements are questions of law to be decided by the court, and the causation and overriding justification elements are questions of fact to be decided by the factfinder. *Id.* at 70. At issue in this appeal are the clarity and jeopardy elements of Rebello’s claim.

### **Clarity**

{¶29} To satisfy the clarity element of a claim of wrongful discharge in violation of public policy, a terminated employee “must articulate a clear public policy by citation to specific provisions in the federal or state constitution, federal or state statutes, administrative rules and regulations, or common law.” *Dohme* at syllabus. “[A] public policy sufficient to overcome the presumption in favor of employment at will is not limited to instances in [which] the statute expressly forbids termination, but may be discerned from legislation generally, or from other sources of law.” *Jacobs v. Highland Cty. Bd.*, 4th Dist. Highland No. 13CA20, 2014-Ohio-4194, ¶ 16, citing *Powers v. Springfield City Schools*, 2d Dist. Clark No. 98-CA-10, 1998 Ohio App. LEXIS 2827 (June 26, 1998), citing *Painter* at 384; *Zajc v. Hycomp*, 172 Ohio App.3d 117, 2007-Ohio-2637, 873 N.E.2d 337, ¶ 27 (8th Dist.) (“[T]he wrongful-discharge tort \* \* \* is not limited to situations where the discharge violates a statute. \* \* \* [C]ase law demonstrates that the cited policy need not prohibit discharge per se.”).<sup>3</sup>

---

<sup>3</sup> LPS cites *Greeley v. Miami Valley Maint. Contrs.*, 49 Ohio St.3d 228, 234, 551 N.E.2d

{¶30} Rebello contends that there is a public policy against terminating employees for objecting to and refusing to participate in the unauthorized access and disclosure of nonpublic consumer information. Rebello contends that she identified “several clear public policies” manifested in the (1) the Fair Credit Reporting Act, 15 U.S.C. 1681, et seq. (“FCRA”), (2) R.C. 1349.19 (disclosure of breach of security system) and (3) the Gramm-Leach-Bliley Act, 15 U.S.C. 6801, et seq.<sup>4</sup> and its implementing regulations (“GLBA”) that were “implicated by her termination” and that the trial court, therefore, erred in granting a directed verdict based on her failure to satisfy this element of her claim.

{¶31} In response, LPS contends that the trial court properly entered a directed verdict in its favor because (1) Rebello’s complaints were limited to “password sharing”; (2) none of the statutes upon which Rebello relies prohibits “password sharing”; (3) none of the statutes upon which Rebello relies applies to LPS and (4) there is no public policy against “password sharing.”

---

981 (1990), for the proposition that “an employee must be discharged for a reason prohibited by statute” to satisfy the clarity element. Although *Greeley* held that “public policy *warrants* an exception to the employment-at-will doctrine” when an employee is discharged for a reason which is specifically prohibited by statute,” it is not the only basis upon which Ohio courts have recognized an employee’s termination violates public policy. (Emphasis added.) *Greeley* at paragraph one of the syllabus.

<sup>4</sup> Rebello has apparently abandoned her claim that her termination violated a public policy implicated by the Fair Debt Collection Practices Act.

{¶32} The stated purpose of FCRA is “to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of [the act].” 15 U.S.C. 1681(b). A “consumer reporting agency” is defined as “any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.” 15 U.S.C. 1681a(f). Rebello has not established that LPS is a “consumer reporting agency,” is involved in preparing or furnishing “consumer reports” within the meaning of FCRA or that her concerns regarding password sharing in any way implicated any of the specific policies or purposes FCRA was enacted to address. 15 U.S.C. 1681(b), 1681a(d), (f). To the extent FCRA seeks to protect the “confidentiality” of consumer information, Rebello has not established a “clear public policy” under FCRA sufficient to support a wrongful termination claim under the facts and circumstances at issue here.

{¶33} R.C. 1349.19(B)(1) imposes a disclosure obligation on a person who discovers that the security of a system containing certain personal information of Ohio residents has been breached. The disclosure is required only if “unauthorized access

and acquisition” of the personal information “causes or reasonably is believed will cause a material risk of identity theft or other fraud.” That provision states, in relevant part:

Any person that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system, following its discovery or notification of the breach of the security of the system, to any resident of this state whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. \* \* \*

{¶34} Rebello has made no showing that this provision applies here or was in any way implicated by her concerns related to password sharing. In this case, there was no evidence that, as a result of password sharing, LPS’s or Chase’s security systems were “breached” as defined in the statute or that any unauthorized “access and acquisition” of personal information occurred (or was likely to occur) that “cause[d] or reasonably is believed will cause a material risk of identity theft or other fraud.” Rebello presented no evidence that any of the Chase customers whose information was accessed by LPS employees through password sharing was at any material risk of identity theft, fraud or any other financial harm as a result of that practice.

{¶35} Accordingly, we agree with the trial court that Rebello failed to establish a “clear public policy” manifested in FCRA or R.C. 1349.19 that was implicated by

Rebello’s objections to password sharing or jeopardized by her termination in this case. However, we reach a contrary conclusion with respect to Rebello’s claims relating to the GLBA.

{¶36} The GLBA requires financial institutions to take steps to ensure the security and confidentiality of the nonpublic information of its customers. 15 U.S.C. 6801, entitled “Protection of nonpublic personal information,” provides in relevant part:

(a) Privacy obligation policy. It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information.

{¶37} The GLBA also provides that, in furtherance of this policy, that certain specified government agencies and authorities

shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards —

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

15 U.S.C. 6801(b).

{¶38} In addition to the provisions of the GLBA itself, Rebello also cites certain guidelines promulgated under the GLBA — the Interagency Guidelines Establishing Information Security Standards (“guidelines”), 12 C.F.R. part 30, Appx. B — which she

contends manifest a clear public policy in protecting nonpublic customer information from unauthorized access and disclosure. The guidelines “address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.” *Id.* at (I). The guidelines apply to “customer information maintained by or on behalf of entities over which the office of the Comptroller of the Currency has authority.” *Id.* at (I)(A). “Customer information” includes “any record containing nonpublic personal information, as defined in 12 C.F.R. 1016.3(p), about a customer, whether in paper, electronic, or other form, that is maintained by or on behalf of the national bank.” *Id.* at (I)(C)(2)(e). The guidelines require banks to “implement a comprehensive written information security program that includes administrative, technical, and physical safeguards,” which must be designed to, among other things: (1) ensure the security and confidentiality of customer information; (2) protect against any anticipated threats or hazards to the security or integrity of such information and (3) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. *Id.* at (II)(A)-(B). The guidelines also require banks to consider whether other security measures, such as controls to authenticate and permit access only to authorized individuals, controls to prevent employees from providing customer information to unauthorized individuals, and encryption of electronic customer information to which unauthorized individuals may have access, are appropriate and, if so, adopt those measures. *Id.* at (III)(C)(1). The guidelines also require banks to “[r]equire its service



providers by contract to implement appropriate measures designed to meet the objectives” of the guidelines. *Id.* at (III)(D)(2). “Service providers” include “any person or entity that maintains, processes, or otherwise is permitted access to customer information or consumer information through its provision of services directly to the [bank].” *Id.* at (I)(C)(2)(g).

{¶39} We agree with Rebello that a clear public policy exists, based on the provisions of the GLBA, to prevent unauthorized access to and disclosure of nonpublic personal information of consumer customers, such as that at issue here.

{¶40} LPS does not dispute that the GLBA and its regulations apply to Chase and the nonpublic customer information accessed by LPS in the MSP system. Nevertheless, LPS contends that GLBA does not support the clarity element of Rebello’s claim because (1) the GLBA does not apply to LPS, (2) Rebello complained only about “password sharing” and (3) Rebello’s complaints regarding “password sharing” were based on concerns that company policies were being violated, not that nonpublic information was being disclosed. We do not find these arguments to be persuasive.

{¶41} LPS first argues that because the GLBA requires banks to take steps “by contract” to ensure that its service providers comply with the requirements of the GLBA and does not directly regulate service providers, LPS “is not subject to the GLBA” and “cannot be liable for violating a public policy in a statute by which it is not governed.” We disagree. LPS cites no authority in support of its contention that an employer must be found to have violated and subject to liability under the specific statute that serves as

the source of the public policy before we may conclude that a clear public policy exists that has been compromised by the employer's conduct.

{¶42} Moreover, LPS repeatedly acknowledged in its own documents that its activities were subject to the GLBA and that it had an obligation under the GLBA to protect and maintain the security and confidentiality of Chase's nonpublic customer information.

{¶43} For example, LPS's Code of Business Conduct and Ethics states:

Employees also must ensure that they do not misuse the \* \* \* confidential information of any other parties. There are several U.S. federal and state laws that require the Company to protect and maintain the security and confidentiality of customer data. Regulators of financial institutions have also implemented numerous regulations dealing with data security in the outsourcing of data processing that involves personally identifiable financial information about a customer. If your job involves the providing of services to domestic financial institutions or you have access to customer data, you should be aware of the Company's obligations to protect certain customer data under the Gramm-Leach-Bliley Act.

\* \* \*

The Company has established corporate policies to protect and secure sensitive consumer and employee data. Each employee must strictly adhere to these policies and take seriously our shared responsibilities to ensure the safety and confidentiality of consumer information we access while performing our jobs.

{¶44} Further, Section 11 of the Master Agreement between LPS and Chase expressly provided, in relevant part, as follows:

If Supplier receives, has access to or process nonpublic personal information protected by the Privacy Regulations ("NPI") from JP Morgan Chase & Co., Supplier will be subject to application Laws restricting

collection, use, disclosure, processing and free movement of personal data (collectively, the “**Privacy Regulations**”). The Privacy Regulations include the Federal “Privacy of Consumer Financial Information” Regulation (12 CFR Part 30), as amended from time to time, issued pursuant to Section 504 of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. §6801, *et seq.*) \* \* \*.

{¶45} LPS also argues that because Rebello’s complaints were limited to “password sharing” and the GLBA does not prohibit “password sharing,” it cannot be said that any public policy manifested by the GLBA was implicated by Rebello’s objections to and threats to disclose LPS’s practice of sharing passwords to Chase. Once again, we disagree. Rebello does not contend that there is a public policy against “password sharing” under the GLBA or any other state or federal law. Instead, she argues that her objections to password sharing and threats to report LPS’s practice of password sharing to Chase implicated public policy because they related to concerns over the unauthorized access and disclosure of nonpublic personal information of Chase’s customers. Rebello contends that “by objecting to sharing passwords, she [was] objecting to a practice that threatened the confidentiality and allowed unauthorized access of individuals to confidential nonpublic customer information. ” She argues that even though there is no public policy against password sharing per se, there is a public policy manifested in the GLBA to protect against the unauthorized access and disclosure of nonpublic personal information and that because LPS’s and Chase’s anti-password

sharing policies were implemented (at least in part) to prevent the unauthorized access and disclosure of this information, dismissing employees under circumstances like those allegedly involved in her dismissal, i.e., for refusing to continue sharing passwords and threatening to report password sharing among LPS employees to Chase, would jeopardize that public policy.

{¶46} Password sharing can occur in one of two ways: (1) passwords can be shared among authorized users or (2) passwords can be shared among authorized users and unauthorized users. There is no public policy against the disclosure of nonpublic customer information to those who have been authorized to access or use the information, provided the scope of the authorization has not been exceeded. Where a password is shared with someone who has authority to access the system for which the password is being used and the information is not leaving the boundaries of the persons authorized to access it, password sharing among such individuals would not threaten the public policy against the unauthorized disclosure of nonpublic customer information. Where, however, a password that permits access to nonpublic customer information is shared with a person who does not have authority to access that information and the password is, in fact, used by the person with whom it is shared to access nonpublic consumer information, password sharing results in the unauthorized disclosure of that information, thereby implicating the public policy against unauthorized access and disclosure of nonpublic personal information of consumers. Thus, the issue in this case is whether Rebello's objections to password sharing were akin to a complaint regarding the

unauthorized access and disclosure of nonpublic consumer information. Viewing the evidence in the light most favorable to Rebello and drawing all reasonable inferences from the evidence in her favor — as we must do in reviewing a trial court’s decision on a motion for directed verdict — we find that under the particular facts and circumstances in this case, it was.

{¶47} There was conflicting evidence at trial as to whether the LPS employees who had not yet received their own tokens to access the MSP system from Chase and were using the passwords of other LPS employees to access that system (1) had been authorized by Chase to access its customers’ nonpublic information but were just awaiting the means to access the MSP system or (2) had not yet been authorized by Chase to access its customers’ nonpublic information. Curtis Larson, who managed the Chase account from 2009 to October 2011, testified that password sharing was not a problem of getting the necessary authorizations from Chase for LPS employees, but simply one of connectivity:

- Q. LPS believed that it didn’t have enough employees who were authorized by Chase and given a password to do all of the volume of work that had come in; correct?
- A. Not exactly. They had authorization. They didn’t have connectivity. They didn’t have – they weren’t able to sign on.
- Q. They didn’t have passwords.
- A. They had passwords.
- Q. So if everybody had passwords, why were they sharing?

A. Because we couldn't establish sign-on through their new protocols. So they weren't able to access MSP to do their job.

Q. So it's your testimony that each and every person who shared a password was authorized by Chase to be on that account?

A. To my knowledge, the people that accessed MSP had been given, at some point, authorization through a password or user id to access MSP.

Q. So why was there a need to share at all?

A. Like I say, we weren't able to get through their sign-on protocols to successfully get access for everybody that needed it.

{¶48} LaSheen Farley, another supervisor working on the Chase account, offered similar testimony — i.e., that password sharing resulted from delays in employees receiving the tokens necessary to access the MSP system and not a failure to receive the necessary authorization to access customer information from Chase:

Q. Those employees who were sharing were not authorized to access the MSP database; true?

A. There were authorized to access MSP. They did not have authorization at that time. They didn't have the actual token, but they had already been authorized, meaning they went through their background checks, both from LPS and Chase. They did not have the physical token in which to access the system.

Q. Do you remember I took your deposition, ma'am?

A. Yes, sir.

Q. \* \* \* I asked you the following question: And in essence, by sharing passwords, LPS was able to bypass the authorization process with Chase and get more people into the MSP system and allowed more people to use the non-public private information of Chase's clients; correct? And what was your answer?

A. Yes.

{¶49} Others offered contrary testimony. Rebello testified that the LPS employees who were sharing passwords had been authorized and approved by LPS to work on the Chase account and were “in line” to receive authorization from Chase but that Chase had not yet “approve[d] them to be in their system.” Evans testified that when passwords were being shared among LPS employees “that meant somebody had unauthorized access” to Chase’s nonpublic customer information.

{¶50} Rebello testified that although her objections were phrased in terms of “password sharing” — and not the unauthorized access and disclosure of nonpublic customer information — in her mind, under the circumstances, there was little difference between the two:

Q. \* \* \* Now you claim in this case that LPS’s decision to terminate your employment was unlawful; do you understand that?

A. Yes.

Q. And you claim that the reason it was unlawful is because you complained about password sharing; is that right?

A. Yes.

\* \* \*

Q. You understand that there’s a difference between sharing a password and disclosing private non-public information?

A. *I understand one results from the other. I don’t understand the difference.*

Q. Well, one doesn’t always result from the other, does it?

A. No, of course not.

Q. We could share passwords, you and I, all day long and nothing bad could happen from that; right?

A. Not necessarily. I think you're [sic] confusion – you're confusing the situation though. *This e-mail is very specific to not sharing passwords.* Not about — says nothing about NPI. *The next step would be NPI.* But in this it says, do not share passwords.

Q. I just want to understand then what your claim is in the case. Your claim in this case is that you complained about password sharing; right?

A. Yes.

Q. You didn't complain about a specific concern that Carrie Rebello had that non-public private information would be disclosed?

A. You're absolutely correct, I complained about password sharing.

(Emphasis added.)

{¶51} In this case, based on the evidence presented by Rebello that LPS was regularly and systemically disregarding the password system established by Chase and allowing LPS employees who had not yet been authorized by Chase to access its nonpublic customer information, a reasonable jury could have found that there was, in fact, no difference between Rebello objecting to password sharing and Rebello objecting specifically to the results of that password sharing, i.e., the unauthorized access and disclosure of nonpublic information to LPS employees. The trial court erred in taking that determination away from the jury and concluding as a matter of law that “[t]he mere assertion relative to sharing passwords is insufficient to satisfy the clarity element of a wrongful termination action.”



{¶52} Although the trial court stated, as a basis for granting LPS’s motion for directed verdict, that “[t]here is no evidence \* \* \* that anyone’s confidential information or identity was compromised in any fashion,” Rebello was not required to show that any consumer identity theft had occurred or that any consumer’s confidential information had otherwise been misappropriated to establish the clarity and jeopardy elements of her claim. A plaintiff asserting a claim of wrongful termination in violation of public policy is not required to show that the conduct to which the employee objected actually resulted in the type of harm that the public policy seeks to prevent. Furthermore, even if such a showing were required, the unauthorized access of Chase’s customers’ nonpublic information by LPS employees in and of itself caused a harm to the privacy interests of those customers — one of the interests the GLBA seeks to protect.

{¶53} Because we find that the GLBA manifests a clear public policy against the unauthorized access and disclosure of the nonpublic personal information of consumers that was (1) applicable to LPS in connection with the work it performed on behalf of Chase and (2) allegedly implicated in Rebello’s termination in this case, we conclude that Rebello presented sufficient evidence to satisfy the clarity element of her claim for wrongful termination in violation of public policy. *See, e.g., Collins*, 73 Ohio St.3d at 71, 652 N.E.2d 653 (recognizing that even where “no actual crime” has been committed, it is “nevertheless a violation of public policy to compel an employee to forgo his or her legal protections or to do an act ordinarily proscribed by law”); *Blackburn v. American Dental Ctrs.*, 10th Dist. Franklin No. 13AP-619, 2014-Ohio-5329 (trial court erred in

entering summary judgment in favor of defendant employers, a dentist and corporation that owned several dental offices, on employees' claims for wrongful discharge in violation of public policy based on public policy prohibiting retaliation against employees who reported workplace conditions that jeopardized staff and dental patient safety); *Anders v. Specialty Chem. Resources*, 121 Ohio App.3d 348, 700 N.E.2d 39 (8th Dist.1997) (plaintiff stated a claim for wrongful termination in violation of public policy where he alleged that employer terminated his employment because he refused to participate in insurance fraud or falsification of insurance claims); *Zajc*, 172 Ohio App.3d 117, 2007-Ohio-2637, 873 N.E.2d 337 (employee allegedly terminated for refusing to ship defective aircraft parts could maintain a claim for wrongful discharge in violation of public policy).

### **Jeopardy**

{¶54} Having found a clear public policy sufficient to justify an exception to the employment-at-will doctrine, we must now determine whether the termination of an employee for raising objections to, refusing to participate in and threatening to disclose her employer's unauthorized access and disclosure of nonpublic information would jeopardize that public policy (the jeopardy element). This requires a showing "not just that a policy may have been violated [as to the plaintiff] but also that the policy itself is at risk if the discharge of the employee is allowed to continue." *Zwiebel v. Plastipak Packaging, Inc.*, 3d Dist. Shelby No. 17-12-20, 2013-Ohio-3785, ¶ 32, citing *Langley v. Daimler Chrysler Corp.*, 407 F.Supp.2d 897, 909 (N.D.Ohio 2005).

{¶55} Analysis of the jeopardy element involves an inquiry into the existence of any alternative means of promoting the particular public policy to be vindicated by a common-law wrongful discharge claim. As the Ohio Supreme Court explained in *Wiles v. Medina Auto Parts*, 96 Ohio St.3d 240, 2002-Ohio-3994, 773 N.E.2d 526:

“If the statute that establishes the public policy contains its own remedies, it is less likely that tort liability is necessary to prevent dismissals from interfering with realizing the statutory policy.” 2 Perritt at 71, Section 7.26. Simply put, there is no need to recognize a common-law action for wrongful discharge if there already exists a statutory remedy that adequately protects society’s interests. \* \* \* In that situation, the public policy expressed in the statute would not be jeopardized by the absence of a common-law wrongful-discharge action in tort because an aggrieved employee has an alternate means of vindicating his or her statutory rights and thereby discouraging an employer from engaging in the unlawful conduct.

*Id.* at ¶ 15. In other words, “it is unnecessary to recognize a common-law claim when remedy provisions are an essential part of the statutes upon which the plaintiff depends for the public policy claim and when those remedies adequately protect society’s interest by discouraging the wrongful conduct.” *Leininger v. Pioneer Natl. Latex*, 115 Ohio St.3d 311, 2007-Ohio-4921, 875 N.E.2d 36, ¶ 27.

{¶56} The GLBA contains no statutory remedies protecting employees who complain about, refuse to participate in and threaten to disclose an employer's unauthorized access and disclosure of nonpublic consumer information. Thus, there is no existing statutory remedy that "adequately protect[s] society's interest [in] discouraging this wrongful conduct." *Id.* If employers were allowed to terminate employees for objecting to, refusing to participate in and threatening to disclose the unauthorized access and disclosure of nonpublic consumer information, such retaliatory practices could deter employees from reporting or taking other steps to protect nonpublic consumer information from unauthorized access and disclosure. We find that without a common-law tort for wrongful discharge under these circumstances, the clear public policy against unauthorized access and disclosure of nonpublic consumer information would be compromised. *See, e.g., Armstrong v. Trans-Service Logistics Inc.*, 5th Dist. Coshocton No. 04CA015, 2005-Ohio-2723, ¶ 62. Accordingly, Rebello satisfied the jeopardy element of her claim for wrongful termination in violation of public policy.

{¶57} For the reasons set forth above, the trial court erred in granting a directed verdict in favor of LPS on Rebello's claim for wrongful discharge in violation of public policy. Rebello's assignment of error is sustained. This case is remanded to the trial court for further proceedings consistent with this opinion.

{¶58} Judgment reversed; case remanded to the trial court.

It is ordered that appellant recover from appellees the costs herein taxed.

The court finds there were reasonable grounds for this appeal.

It is ordered that a special mandate be sent to said court to carry this judgment into execution.

A certified copy of this entry shall constitute the mandate pursuant to Rule 27 of the Rules of Appellate Procedure.

---

EILEEN A. GALLAGHER, PRESIDING JUDGE

EILEEN T. GALLAGHER, J., and  
ANITA LASTER MAYS, J., CONCUR