CARR MALONEY PC

LEGALLY SPEAKING

Carr Maloney PC is a litigation firm providing comprehensive legal services throughout the mid-Atlantic region. Businesses and individuals use the firm as a single resource to meet all of their legal needs. Recognizing that each client's legal issue comes with its own specific complexities, **we simplify the complex.**

March 2014

In this issue:

To Have a Chance of Winning the Lottery, Employers Should Submit H-1B Petitions on April 1, 2014

By: Tina M. Maiolo, Esq. and Suzanne E. Derr, Esq.

The 113th Congress is considering legislation that would make extensive revisions to nonimmigrant categories for professional specialty workers (H-1B visas). The "Border Security, Economic Opportunity, and Immigration Modernization Act," or S.744, as passed by the Senate on June 27, 2013, would substantially revise the H-1B visa category by increasing the annual H-1B visa cap for highly skilled workers from 65,000 to 110,000 per year and by increasing the H1B cap for science, technology, engineering, and math (STEM) visas from 20,000 to 25,000 per year. In total, there would be 135,000 H-1B visas available the first year that the law is enacted. Because immigration reform legislation has not yet been passed, however, there are only 85,000 H-1B visas available for FY 2015.

The H-1B visa program applies to employers seeking to hire nonimmigrant aliens as workers in specialty occupations or as fashion models of distinguished merit and ability. A "specialty occupation" is one that requires the application of a body of highly specialized knowledge and the attainment of at least a bachelor's degree or its equivalent. 8 U.S.C. § 1184(i). "Specialty occupations" include but are not limited to positions in biotechnology, chemistry, architecture, engineering, mathematics, physical sciences, social sciences, medicine and health, education, law, accounting, business specialties, theology, and the arts. The intent of the H-1B visa provisions is to help employers who cannot otherwise obtain needed business skills and abilities from the U.S. workforce by authorizing the temporary employment of qualified individuals who are not otherwise authorized to work in the U.S.

In addition to the increase of available H-1B visas, the proposed legislation also contemplates protections for U.S. workers by modifying H-1B application requirements and procedures for investigating H-1B complaints. The legislation would amend the H-1B labor certification process to revise wage requirements based on Department of Labor (DOL) surveys, and would require employers to advertise for U.S. workers on a DOL website. The legislation also broadens the DOL's authority to investigate alleged employer violations, would require the DOL to conduct annual compliance audits of certain employers, and would increase the DOL's reporting requirements and information sharing between the DOL and the U.S. Citizenship and Immigration Services (USCIS).

Because Congress has not yet passed comprehensive immigration reform or legislation that reforms the H-1B visa program, for FY 2015, there are only 85,000 H-1B visas available. USCIS begins accepting H-1B visa applications for FY 2015 beginning on April 1, 2014. The H-1B visa cap remains in place until all of the available visas for the year's quota have been filed and issued. While there is no fixed or set cut-off date for filing an H-1B visa application, it is important to remember that the cap is quickly reached as H1-B visas are issued on a first come, first serve basis. H-1B visas can be applied for and filed towards the cap numbers until the date that all available visas have been issued.

The time it takes for the cap to be reached varies from year to year. For example, for FY 2013, visas were available for approximately 10 weeks after the petition period opened, while for FY 2014, all available visas were issued within the first 7 days after the petition period opened through a "lottery" system. When USCIS receives more petitions than it can accept (as it did for FY 2014, when 124,000 petitions were submitted during the first week), USCIS uses a lottery system to randomly select the number of petitions required to reach the numerical limit. The first lottery is limited to those applicants who hold advanced degrees from U.S. institutions. If an advanced degree petition is not selected in the advanced degree lottery, it is included in the lottery for the regular quota. Prior to FY 2014, the lottery for the H1-B cap had last been used in April 2008 for FY 2009. Because the H-1B cap was reached during the first week of the filing period last year, it is again expected that USCIS will receive more petitions than it can accept for FY 2015 and will therefore again need to utilize the lottery system. Accordingly, employers should ensure that their petitions are ready to be filed on April 1, 2014.

Navigating the Minefields of Local Data Breach Notification Laws

By: Nat P. Calamis, Esq.

With recent high-profile data breach incidents such as those at Target and Neiman Marcus shining a spotlight on data security issues, it is critical for businesses, both large and small, to understand their obligations in the event of a data breach. It is, however, often complicated for businesses to get a definitive answer as to exactly what their obligations are. While there has been a strong push since the Target and Neiman Marcus breaches for the passage of federal legislation to govern the response of businesses to data breaches,[1] to date no such federal law exists. Instead, businesses are governed by a patchwork of state laws[2] and industry-specific requirements[3], many of which vary significantly.

The differences in local data breach notification laws create uncertainty about potential liability exposure in the wake of a data breach, and can also place onerous burdens on businesses to determine the exact notification procedures that need to be followed in a given situation. This is particularly true for entities who store personal information of individuals from multiple jurisdictions. To demonstrate the difficulties these differing local statutes can create, this article will summarize the state data breach notification laws in the District of Columbia, Maryland, and Virginia, and explain the potential exposure and notification requirements that would be faced by an entity conducting business in all three jurisdictions.

The District of Columbia's data breach notification law is codified at D.C. Code, §28-3851, *et seq*. Pursuant to this statute, "personal information" is defined as an individual's name combined with any one or more of the following elements: (I) social security number; (II) driver's license or District of Columbia Identification Card number; (III) credit or debit card number; or (IV) any other number or code or combination of numbers or codes such as account number, security code, access code, or password, that allows access to or use of an individual's financial or credit account. *See* D.C. Code, §28-3851(3)(A). The statute further defines "breach of the security of the system" as the unauthorized acquisition of computerized or other electronic data, or any equipment or device storing such data, that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. *Id.* at §28-3851(1).

The District of Columbia statute requires any person or entity conducting business in the District and that owns or licenses computerized or electronic data that includes personal information, and who discovers a breach of the security of the system to "promptly" notify any District of Columbia resident whose personal information was included in the breach. *Id.* at §28-3852(a). The statute requires that the notification "be made in the most expedient time possible and without unreasonable delay . . .". *Id.* If the breach involves the personal information of more than 1000 individuals, the statute also requires the business or entity to notify, "without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide

[1] *See, e.g.* The Washington Post, February 18, 2014, "Calls grow for law on data breaches", by Hayley Tsukayama.
[2] 46 states and the District of Columbia have adopted their own data breach notification laws.
[3] For example, the Health Information Privacy and Accountability Act ("HIPAA") has its own requirements for reporting the mishandling of medical records. *See, e.g.* 45 CFR §164.400-414.

basis . . .". *Id.* at §28-3852(c). The notification required under the District of Columbia statute may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. *Id.* at §28-3852(c).

District of Columbia residents injured by a violation of the breach notification statute may institute a civil action to recover actual damages, the costs of the action, and reasonable attorneys' fees. *Id.* at §28-3853(a).[4]

In Maryland, businesses are governed by the Maryland Personal Information Protection Act ("PIPA"), codified at Md. Code, Ann. Comm. Law §14-3501, *et seq*. PIPA defines "personal information" as an individual's name in combination with any one or more of the following data elements: (i) a social security number; (ii) a driver's license number; (iii) a financial account number, including a credit card number or debit card number; or (iv) an Individual Taxpayer Identification Number. PIPA requires businesses that own or license personal information of individuals residing in the State to maintain "reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations." *Id.* at §14-3503(a).

PIPA also requires businesses to take various actions if a "breach of the security of a system" occurs, defined as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business." *Id.* at §14-3504(a)(1). Specifically, when businesses that own or license personal data discover a breach of the security of a system, they are required to "conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach." *Id.* at §14-3504(b)(1). If a business concludes after that the misuse of an individual's personal information has occurred or is reasonably likely to occur, the business is required to notify the individual of the breach "as soon as reasonably practicable". However, this notification requirement may be delayed if a law enforcement agency determines that the notification would impede a criminal investigation; or if the delay is required to determine the scope of the breach, identify the individuals affected, or restore the integrity of the system. *Id.* at §14-3504(d). Pursuant to PIPA, the notification must include a description of the categories of information that are reasonably believed to have been acquired by an unauthorized person, the contact information of the business making the notification, the contact information for the major consumer reporting agencies, and the contact information for the Federal Trade Commission and the Office of the Attorney General. *Id.* at §14-3504(g). In addition, PIPA requires businesses who discover a breach of the security of a system to notify the Office of the Attorney General. *Id.* at §14-3504(j).

Businesses that violate PIPA are deemed to have engaged in unfair or deceptive trade practices in violation of the Maryland Consumer Protection Act. *Id.* at §14-3504. The Maryland Consumer Protection Act allows the Office of the Attorney General to seek injunctive relief and civil penalties. It also permits consumers to assert private causes of action for the recovery of actual damages and attorneys' fees. *See, e.g.* Maryland Code, Commercial Law, §13-408.

Virginia's data breach notification law is set forth at Virginia Code, §18.2-186.6. This statute defines "personal information" as an individual's name in combination with any one or more of the

[4] Pursuant to the statute, actual damages do not include dignitary damages, including pain and suffering.

following data elements: (1) social security number; (2) driver's license number or state identification card number; (3) financial account number, or credit or debit card number in combination with any security code, access code, or password that would permit access to a resident's financial accounts. It further defines "breach of the security of the system" as "the unauthorized access and acquisition of unencrypted and un-redacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity . . . that causes, or the individual or entity reasonably believes will cause identity theft or fraud to any resident of the Commonwealth."

The Virginia statute requires individuals or entities that learn of a breach of the security of the system to provide notification of the breach to the Office of the Attorney General and any affected resident of the Commonwealth "without unreasonable delay". Pursuant to the statute, the notice must describe: (1) the incident in general terms; (2) the type of personal information that was subject to unauthorized access; (3) the acts the entity has taken to protect the information from further unauthorized access; (4) a telephone number that the person may call for further information or assistance; (5) advice that directs the person to remain vigilant by reviewing accounting statements and monitoring free credit reports. This notification requirement "may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system." The notification requirement may also be delayed if a law enforcement agency advises that the notification would impede an investigation. The Virginia statute permits the Office of the Attorney General to bring an action to address violations of the statute, and the Office of the Attorney General may impose a civil penalty not to exceed $150,000 per breach of the security of the system. The statute also permits individuals to recover direct economic damages for violations.

While there is no doubt that the data breach notification laws of the District of Columbia, Maryland, and Virginia have substantial similarities, there are also significant differences between the laws that an entity conducting business in all three jurisdictions would need to be aware of in the event of a data breach situation. For example, suppose there is a large retailer located in the District of Columbia that sells goods to thousands of customers, who are primarily residents of the District of Columbia, Maryland, and Virginia. The retailer learns that hackers have breached its computer system and been able to access the names, credit card numbers, and security codes for thousands of its customers.

In all three jurisdictions, this incident would constitute a "breach of a security system" which would require some type of action on behalf of the retailer. However, the specific action required by the retailer differs depending on the applicable statute. The retailer would have to provide notice of the breach to all District of Columbia, Maryland, and Virginia residents whose personal information may have been accessed, and the notice would have to be provided in a "reasonably" prompt fashion.[5] The retailer would have to provide notice of the breach to the Office of the Attorney General in Maryland and Virginia, but it would not be required to provide notice to the Office of the Attorney General in the District of Columbia. The retailer would have to determine if the breach

[5] All three jurisdictions reference "reasonableness" in terms of the timing of the notification requirements. This is obviously a nebulous term, and it would require a fact-specific inquiry to determine what would constitute "reasonable" behavior in a given circumstance. It is possible that different states will develop different definitions of reasonableness as case law interpreting these data breach notification statutes develops.

involved personal information of more than 1000 District of Columbia, Maryland, and/or Virginia residents. If it did, the retailer would also have to provide notice to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. The notice that the retailer is required to provide to Maryland residents would have to be more detailed than the notice to District of Columbia and Virginia residents, in that it would have to include a description of the information accessed, contact information for the business whose data was compromised, as well as contact information for the Federal Trade Commission, the Office of the Attorney General, and the major consumer reporting agencies.

Perhaps the most onerous requirement that the retailer would face is determining whether the breach led to the unauthorized access of personal information from residents of any other jurisdictions. For each jurisdiction implicated, the retailer would have to determine the requirements of the applicable state notification law (assuming one exists), and adhere to those requirements.

In terms of liability, the retailer could face enforcement actions from the Office of the Attorney General of all three jurisdictions that could seek to recover civil penalties, with the Virginia statute allowing for civil penalties of up to $150,000 per breach. Consumers impacted by the breach could also pursue private causes of action in all three jurisdictions where they can seek to recover any direct damages caused by the breach. In the District of Columbia and Maryland, the consumers could also recover the reasonable attorneys' fees incurred in pursuing these claims.

As the above analysis demonstrates, businesses who suffer data breaches are currently forced to navigate an extremely complex array of requirements and potential exposure under the existing legal framework. Unless and until federal legislation is passed that pre-empts these local statues, it will be extremely costly and difficult for businesses to respond to data breaches in a manner that is compliant with all applicable laws. This is particularly true for data breaches impacting consumers in multiple jurisdictions.

Disgruntled Former Employees Disrupting Your Business? Options for DC Employers Following an Involuntary Termination

By: Kristine M. Ellison, Esq.

While terminating an employee is never an easy or painless task for an employer, the aftermath of that termination can sometimes seem worse than it would have been to continue employing the person. Some former employees harass their former coworkers and supervisors with incessant phone calls and emails, while some may even go as far as to come back to their former offices and/or the employer's main office and demand to speak with the CEO or similarly high-ranking official.

While many employers end up on the defense side of post-termination lawsuits or charges of discrimination with the EEOC or the Office of Human Rights, some employers may need to "play offense" to stop a former employee from disrupting business operations. This article explains two approaches available to employers under D.C. law. An employer may either seek a permanent injunction or a civil protection order. Although a civil protection order (CPO) is usually reserved for domestic violence issues, anyone who is the victim of stalking may seek a CPO. If the former employee is doing something other than stalking, the employer should seek a permanent injunction. Regardless, once either a CPO or an injunction is obtained, we strongly recommend that the employer pursue violations of the order through the criminal process. If the employer fails to pursue the violations and the former employee commits an act of violence, the employer can count on that failure counting against it in a subsequent personal injury case. The remainder of this article discusses the procedures for each approach along with the positives and negatives of each.

Permanent Injunction Approach

If stalking is not an issue but the former employee is harassing, threatening via telephone or email, or trespassing on the employer's property, the employer may pursue a permanent injunction. This process requires drafting a complaint, a motion for a temporary restraining order, a motion for a preliminary injunction and a proposed order specifying the conduct to be restrained. The D.C. Superior Court Clerk's office now requires that all three of these pleadings be filed at the time the case is opened. After filing, the Clerk will direct the employer to judge-in-chambers to obtain a hearing date on the motion for the temporary restraining order. Usually, the hearing date is within one week of the filing date, so we recommend that an employer confirm availability of its witness to the former employee's conduct. Once the hearing date and time for the temporary restraining order is set, the employer needs to have the former employee served. If the employer is unable to get the employee served in the interim, the judge-in-chambers is unlikely to grant the motion unless 1) the employer can show by affidavit or verified complaint "that immediate and irreparable injury, loss, or damage will result to the applicant" before another hearing; and 2) the Court finds that the employer has "made all reasonable efforts under the circumstances" to give the former employee (or his attorney) actual notice of the hearing and copies of all pleadings filed to date in the case. D.C. Superior Court Rule of Civil Procedure 65(b). As a best practice, we recommend using a private process server to ensure that the former employee is served with notice of the hearing and all filings.

Once the former employee has been served, she is likely to attend the hearing. The hearing takes place with the judge-in-chambers on the fourth floor of the Superior Court and is usually less formal than other court hearings. The parties remain seated even when addressing the judge, and the rules of evidence are not strictly enforced. During these proceedings, the judge usually attempts to find some common ground between the parties so a consent order may be entered. The hearing is much less adversarial, and some of the judges will choose not to hear from witnesses when an attorney is present and representing the party. One of the benefits of this approach is that a former employee who is rational is more likely to abide by an order when the judge's approach makes her feel as if the order is more of an agreement as opposed to a directive coming from the employer. Consequently, the former employee is less likely to violate the order. Unfortunately this does not hold true in our experience when the former employee is irrational or suffering from mental illness.

Regardless of whether the temporary restraining order is by consent or not, the judge will enter it and set a future date for a hearing on the motion for a preliminary injunction. The judge may refer to this hearing as a "status hearing." Because the restraining order is meant to be temporary, this hearing will usually be set for two weeks after the date of the first hearing. The order itself may also include language indicating that it expires on the date of the next hearing. If the former employee does not appear at the status hearing, the court may extend the temporary restraining order for additional time, depending on the reason why the former employee has failed to appear. Counsel must remember to orally request a renewed restraining order, especially if the initial order contained an expiration date. If the former employee does appear, the court may conduct an evidentiary hearing. The employer should be prepared with witnesses and exhibits regardless of what it may anticipate about the former employee's attendance. At the conclusion of that hearing, the Court will either grant or deny the motion, and the case will proceed as any other civil matter proceeds in the Superior Court. The parties may conduct discovery, and the employer is likely to dispose of the issue by filing a motion for summary judgment at the close of discovery. The employer should disseminate both the temporary restraining order and the order granting the preliminary injunction as necessary to ensure that violations of the order will be reported. As noted above, if a violation occurs, we strongly recommend that employers report the violation to the police, file a motion for civil contempt and follow through until the former employee is held responsible for the violation. If the employer declines to pursue contempt for the violation, the former employee may later use that as evidence that the alleged threat or disruption is not serious enough to warrant further court action. In the worst case scenario, the former employee may commit an act of violence on the employer's property and/or against a current employee who will seek compensation from the employer.

Civil Protection Order (CPO)

If a person is threatening to commit a crime against an individual and/or stalking is occurring, the employer may choose to seek a CPO. If the situation is a true emergency, we recommend filing for a temporary CPO in person at the Domestic Violence Intake Unit in Room 4550 at the Superior Court. The process may take a few hours, but if the judge finds that the employer has proven that the former employee committed a crime or threatened to commit a crime, an order may be entered the same day even without the former employee present. D.C. Code § 16-1004(b)(1). Employers may view a sample of the temporary protection order on the Superior Court's website.[1] Once granted, a temporary order lasts only fourteen days with a few exceptions,[2] and another hearing will be scheduled.

When the situation is urgent, but not a true emergency, we recommend filing a petition and affidavit for a CPO. The Superior Court has a form available on its website[3] that the employer may fill out in advance and bring to the courthouse. Legal representation is not required for filing the petition and affidavit, but we recommend employing counsel for the hearing on the petition. The hearing will require presentation of evidence, and the judge will not grant the petition unless she determines that good cause exists to believe the former employee has committed or threatened to commit a criminal offense against the employer. D.C. Code § 16-1005(c). If the judge makes this finding, he may issue an order directing the former employee to refrain from committing or threatening to commit a criminal offense against specific individuals; requiring the former employee to stay away from and have no contact with the employer and current employees, or some combination of the two. *Id.* The order may also require payment of attorneys' fees and costs and will normally direct the police to enforce the order. *Id.*

One advantage of this approach is that the police and prosecutor are involved from the beginning which will make pursuing violations more efficient. On the other hand, this approach has a couple of drawbacks. First, a CPO lasts only for one year from the date of issuance. D.C. Code § 16-1005(d). If the former employee is patient but persistent, as we have seen in some cases, the employer will have to seek an extension of the order after the year expires. *Id.* Employers may also want to consider that they cannot pursue discovery through this procedure without first filing a motion and obtaining a court order.

Ultimately, each situation is different, even if the same employer is involved. Employers should consult with counsel and carefully weigh their options before pursuing either approach against a disruptive former employee.

---

[1] http://www.dccourts.gov/internet/documents/tpo.pdf
[2]D.C. Code § 16-1004 provides in pertinent part:

(2) An initial temporary protection order shall not exceed 14 days except, if the last day falls on a Saturday, Sunday, a day observed as a holiday by the court, or a day on which weather or other conditions cause the court to be closed, the temporary protection order shall extend until the end of the next day on which the court is open. The court may extend a temporary protection order in additional 14 day increments, or longer increments with the consent of the parties, as necessary until a hearing on the petition is completed.

(3) If a respondent fails to appear for a hearing on a petition for civil protection after having been served in accordance with the Rules of the Superior Court of the District of Columbia, and a civil protection order is entered in accordance with § 16-1005, the temporary protection order shall remain in effect until the respondent is served with the civil protection order or the civil protection order expires, whichever occurs first.

[3] http://www.dccourts.gov/internet/documents/petition.pdf

Taxes on Severance Payments: Supreme Court to Resolve Split among Circuit Courts

By: Ali Khorsand, Esq.

On January 14, 2014, the Supreme Court heard oral arguments in *United States v. Quality Stores, Inc.*, a case on appeal from the Sixth Circuit Court of Appeals. A split between the Sixth Circuit and the Federal Circuit of the U.S. Court of Appeals prompted the Supreme Court to hear the case and to decide whether severance payments made to employees whose employment was involuntarily terminated are taxable under the Federal Insurance Contributions Act (FICA). FICA is a federal payroll tax imposed on both employees and employers to fund Social Security and Medicare. The taxes imposed are withheld by the employer under Internal Revenue Code

(IRC) Section 3102. The withholding mechanism is similar to income tax withholding, where Congress requires employers to withhold income taxes from wages under IRC Section 3402. Although the term "wage" is defined slightly differently in the FICA and income tax-withholding chapters, the Supreme Court has previously held that the two terms should be read similarly.

The central issue of the case currently in front of the Court began in the 1950's, when, as result of an accord reached between various companies and labor unions, supplemental unemployment benefits (SUB) payments paid to laid-off workers were not characterized as wages since workers in some states could not receive both unemployment payments and supplemental benefit payments, normally classified as wages. The Internal Revenue Service (IRS) went along with the agreement and ruled that severance payments were not wages, if certain tests were met, most notably the SUB payments were made along with state unemployment payments. The severance payments which met the IRS criteria were termed as supplemental unemployment benefit (IRS SUB) payments.

To subject the SUB payments, not defined as wages, to income tax withholdings, Congress enacted IRC Section 3402(o), "Extension of withholding to certain payments other than wages." Pursuant to Section 3402(o), "any supplemental unemployment compensation benefit paid to an individual . . . shall be treated as if it were a payment of wages." The Section does not require the person receiving the payment to receive it in connection with state unemployment payments, in contrast to the main requirement of IRS SUB. Consequently, because many severance payments do not depend on an employee's receipt of state unemployment payments, they will meet the 3402(o) definition for wages for income tax withholding purposes, but not the IRS SUB definition.

In 2008, the U.S. Court of Appeals, the Federal Circuit, in *CSX Corp. v. United States*, held that payments made to union employees to leave the company, not in conjunction with state unemployment payments, were wages subject to FICA withholdings. After paying the FICA taxes and suing the government for a refund, CSX unsuccessfully argued the payments met the criteria of 3402(o) IRS SUB payments and, therefore, were not wages and were only treated "as if" wages for income tax holding.

The next time this issue arose, the Sixth Circuit ruled the SUB payments were not wages and not subject to the FICA withholding. In 2001, Quality Stores closed all of its stores and terminated the employment of all its employees. Prior to its closure, Quality Stores was one of the nation's largest agricultural implement retailers in the United States, which served farmers and hobby gardeners alike. Quality Stores made severance payments to the employees whose employment was involuntarily terminated. These severance payments were not tied to the receipt of state unemployment compensation, and they were not attributable to the provision of any particular services by the employees. The company withheld FICA taxes from the severance payments and forwarded the withholdings to the government. Because the severance payments constituted gross income to the employees for federal income tax purposes, Quality Stores reported the payments as wages on W-2 forms and withheld federal income tax.

Although Quality Stores collected and paid the FICA tax, it did not agree with the IRS's position that the severance payments constituted wages for FICA purposes. Quality Stores contended that

the severance payments were not wages but instead constituted SUB payments that were not taxable under FICA. In September 2002, Quality Stores filed fifteen 843 Forms with the IRS seeking the refund of $1,000,125.00 in FICA tax. After the IRS did not allow or deny the refund claims, Quality Stores filed an action in the US Bankruptcy Court in June 2005. The bankruptcy court granted the refund request and the US District Court upheld the decision.

On appeal, the Sixth Circuit upheld the US District Court's decision to issue the refund of approximately One Million Dollars in taxes paid under FICA. In doing so, the Sixth Circuit upheld the District Court's holding that payments Quality Stores made to its employees upon the involuntary termination of their employment constituted SUB payments that are not taxable as wages under FICA. Reflecting upon the title and legislative history of Section 3402(o), the court reasoned that Congress clearly expressed its intent to not treat SUB payments as wages for FICA tax purposes, but were to be only treated as if they were "wages" for purposes of federal income tax withholding.

Although the amount of the refund at issue is small, the potential effects of the Supreme Court's upholding of the Sixth Circuit's decision could be significant. The Obama administration, in the government's filings, has argued that the Court's possible upholding of the Sixth Circuit's decision could trigger a wave of tax refund claims that could drain over $1 billion from Social Security and Medicare, programs already facing major financial difficulties for the years ahead. A decision in this closely watched decision is expected late this summer.