EMPLOYMENT LAW NEWS

Summer 2012

IN THIS ISSUE

Seward & Kissel is pleased to announce the addition of two new partners, Michael Considine, a former supervisory federal prosecutor from the United States Attorney's Office for the Eastern District of New York, and Rita Glavin, a former federal prosecutor for the Southern District of New York who served as the head of the United States Department of Justice's Criminal Division. Mr. Considine and Ms. Glavin have extensive experience with governmental investigations, regulatory enforcement and compliance matters, including, but not limited to, internal investigations relating to allegations of an employee's wrongdoing. To welcome our new partners, we devote this edition of the Employment Law Newsletter to recent cases involving employment and white collar legal issues.

Former FrontPoint and Morgan Stanley Employee Ordered to Disgorge Wages as Restitution to Employer for Insider Trading

- *Summary:* On March 20, 2012, the U.S. District Court for the Southern District of New York ordered a hedge fund manager to pay his former employer, Morgan Stanley, $10.2 million in restitution in connection with his conviction for insider trading. The Court found that Morgan Stanley was a "victim" for purposes of restitution under the Mandatory Victims Restitution Act, and that the manager's illegal conduct deprived Morgan Stanley of his honest services and caused it injury. The Court made clear that, under appropriate circumstances involving employee criminal wrongdoing, companies may be able to recover certain sums relating to that employee's dishonest services, as well as its internal investigations and related interactions with law enforcement and regulated entities.

Full article on page 2.

Second Circuit Releases Former Goldman Sachs Programmer From Prison, Ruling That He Did Not Commit A Crime When He Took Goldman Sachs' Trading Code

- *Summary:* The United States Court of Appeals for the Second Circuit, in an April 11, 2012 opinion, explained the rationale for its summary order in February of this year overturning the conviction of a former Goldman Sachs programmer for violations of the National Stolen Property Act ("NSPA") and the Economic Espionage Act ("EEA"). The Second Circuit, narrowly interpreting the two statutes, held that the programmer's upload of Goldman Sachs' internal trading code to an overseas server did not violate the EEA because it did not involve a product in "interstate or foreign commerce," and did not violate the NSPA because the code was not "tangible property." The Court's reasoning highlights the limits of certain criminal statutes in the digital age with respect to actions taken by departing employees.

Full article on page 4.

Ninth Circuit's Decision in *U.S v. Nosal* Creates Circuit Split Over Scope of Computer Fraud and Abuse Act

- *Summary:* On April 10, 2012, the *en banc* United States Court of Appeals for the Ninth Circuit limited the applicability of the Computer Fraud and Abuse Act (the "CFAA") by holding that gaining authorized access to, and subsequently using information for a purpose prohibited by a computer-use agreement, even for a fraudulent purpose, did not violate the CFAA. In so holding, the Ninth Circuit created a circuit split with earlier interpretations of the CFAA by the Fifth, Seventh and Eleventh Circuits.

Full article on page 5.

Employment Law Practice Group

If you have any questions or comments about this Newsletter, please feel free to contact any of the attorneys in our Litigation Group listed below via telephone at (212) 574-1200 or via e-mail generally by typing in the attorney's last name @sewkis.com.

Partners:
M. William Munno
Michael J. McNamara
Mark D. Kotwick
Anne C. Patin

Associates:
Jennifer J. Pearson
Julia C. Spivack
Benay L. Josselson

SEWARD & KISSEL LLP

One Battery Park Plaza, NY, NY 10004
Tel: (212) 574-1200 | Fax: (212) 480-8421
sknyc@sewkis.com
www.sewkis.com

Former FrontPoint and Morgan Stanley Employee Ordered to Disgorge Wages as Restitution to Employer for Insider Trading

On March 20, 2012, Judge Denise Cote of the U.S. District Court for the Southern District of New York, in a case entitled *U.S. v. Skowron*, No. 11 Cr. 699, ordered former FrontPoint Partners LLC ("FrontPoint") hedge fund manager Joseph F. Skowron III to pay Morgan Stanley $10.2 million in restitution in connection with his conviction for an insider trading scheme he perpetrated while employed as a Managing Director at Morgan Stanley. The Court held that Morgan Stanley was a "victim" for purposes of restitution under the Mandatory Victims Restitution Act ("MVRA"), and that Skowron's actions deprived Morgan Stanley of his honest services and caused it injury. The Court concluded that Morgan Stanley could recover from Skowron its legal fees and a portion of the compensation it paid to him in restitution, making clear that, under appropriate circumstances involving employee criminal misconduct, companies may be able to recover certain sums from that employee relating to his dishonest services, as well as its resulting internal investigations and related interactions with law enforcement and regulated entities.

Background

Skowron is a former portfolio manager at FrontPoint, a health care focused hedge fund acquired by Morgan Stanley in 2006 and spun off in 2011. In the criminal action before Judge Cote, Skowron pled guilty to insider trading related to his trading on tips from a former advisor for Human Genome Sciences Inc. ("HGSI") relating to certain of HGSI's drug trials. He was sentenced to five years in prison and ordered to pay restitution to five counterparties of the FrontPoint funds with whom Skowron had traded relying on the inside information.

Skowron's guilty plea in the criminal action coincided with an August 2011 settlement of an action brought against FrontPoint and Skowron by the SEC in which the SEC, among other things, required that FrontPoint disgorge $30 million (the amount of trading losses it avoided), plus prejudgment interest, and Skowron pay a civil penalty of $2.72 million. Ultimately, Morgan Stanley paid the SEC approximately $33 million in settlement of the SEC's claims against FrontPoint and Skowron.

Morgan Stanley Seeks Restitution From Skowron

Morgan Stanley subsequently sought restitution in the amount of $45 million from Skowron under the MVRA, which provides that victims may seek restitution against a wrongdoer in sentencing proceedings for convictions of any offense resulting in, among other things, the victims' pecuniary loss. Morgan Stanley explained that the amount it sought reflected the $33 million settlement it paid to the SEC, $3.8 million in legal fees and costs it incurred in connection with the SEC investigation, plus an additional $8 million that Morgan Stanley paid to Skowron from 2007 to 2010 while he had been perpetrating his scheme, which was equivalent to 25% of Skowron's total compensation during that period.

Is Morgan Stanley A Victim?

Morgan Stanley argued that it was a "victim" of Skowron under the terms of the MVRA. The MVRA defines a "victim" as "a person directly and proximately harmed as a result of the commission of an offense for which restitution may be ordered including, in the case of an offense that involves as an element a scheme… any person directly harmed by the defendant's criminal conduct in the course of the scheme…" 18 U.S.C. § 3663A(a)(2).

The Court determined there was a causal nexus between Skowron's securities fraud, insider trading and obstruction of the resulting SEC investigation, and the harm suffered by Morgan Stanley. The Court observed that Skowron's crimes "deprived Morgan Stanley of the honest services of its employee, diverted valuable corporate time and energy in the defense of Skowron and FrontPoint, and injured Morgan Stanley's reputation." Order at 10. The Court also determined that Skowron caused further damage to Morgan Stanley when, in an attempt to conceal his insider trading scheme, he lied to Morgan Stanley's attorneys during the course of its internal investigation, and later to the SEC. *Id*. For these reasons, the Court concluded Morgan Stanley was a "victim" under the MVRA, and thus eligible for restitution from Skowron.

Morgan Stanley Is Entitled to Some, But Not All, Of The Requested Restitution

Despite the Court's determination that Morgan Stanley was a victim of Skowron under the MVRA, the Court determined that it was not entitled to restitution of the entire $45 million it sought from the Court.

Under the MVRA, a victim is entitled to a return of its property, or restitution equal to the value of his property. The victim must have a legal entitlement to the money or property in order to make a claim for restitution. Order at 13. With respect to Morgan Stanley's request for restitution of the approximately $33 million it paid to the SEC in settlement of the claims against Skowron and FrontPoint, the Court determined that it was not money FrontPoint could have legally retained

because the payment represented losses that FrontPoint avoided as a result of Skowron's illegal actions, and not money to which Frontpoint or Morgan Stanley had a legal entitlement On the other hand, Morgan Stanley was entitled to restitution for the legal fees it incurred in connection with the SEC investigation because it was legally and contractually obligated to pay for Skowron and other FrontPoint employees' legal fees in connection with the investigation.

Lastly, the Court determined that Morgan Stanley was entitled to restitution in the amount of $6,420,801, an amount equal to 20% (not the 25% requested) of the compensation it paid to Skowron from 2007 through 2010. As the Court explained, "[m]oney paid in salary is property… a portion of an individual's salary can be subject to forfeiture where, as here, an employer pays for honest services but receives something less." Order at 21 (quoting *U.S. v. Bahel*, 662 F.3d 610, 649 (2d Cir. 2011)). Skowron acted dishonestly when he executed his scheme between December 2007 and January 2008, prolonged the SEC investigation by almost two years due to his deception and extended "the period during which Skowron received generous compensation from Morgan Stanley; if Morgan Stanley had learned at an earlier date that Skowron had engaged in insider trading, it would have terminated his employment then." *Id.* at 23.

The Court reasoned that the amount represented "a conservative estimate of the cost of the fraud with respect to his compensation." *Id.* at 20 (internal quotation omitted). As such, that percentage approximated the difference between "the honest services for which Morgan Stanley paid and what it received as a result of Skowron's offense." *Id.* at 27.

The Court expressly disagreed with Skowron's argument that allowing Morgan Stanley to recover a portion of his compensation would "create an extremely broad rule… allow[ing] restitution to an employer in any case in which a defendant's fraud against another would have been grounds for termination by that employer." *Id.* at 26. Reiterating "the scale of Skowron's fraud, the severity and length of his deception, and the impact on Morgan Stanley," in addition to the applicability of the MVRA to Skowron's actions, the Court determined restitution in the amount of $6,420,801 to be appropriate.

Conclusion

The Court's decision in *Skowron* makes clear that, under appropriate circumstances, a company may be eligible to recover restitution from an employee convicted of certain federal crimes. The amount of restitution could include a portion of the compensation the company paid to the employee during the period of misconduct, along with the legal costs associated with the company's internal investigation of, and response to, governmental inquiries into the misconduct.

Second Circuit Releases Former Goldman Sachs Programmer From Prison, Ruling That He Did Not Commit A Crime When He Took Goldman Sachs' Trading Code

On April 11, 2012, the United States Court of Appeals for the Second Circuit, in an opinion written by Chief Judge Dennis Jacobs, explained why the Second Circuit in February summarily overturned the conviction of Sergey Aleynikov, a former Goldman Sachs Group Inc. programmer who had served eleven months in prison for violations of the National Stolen Property Act (the "NSPA") and the Economic Espionage Act (the "EEA"). *U.S. v. Aleynikov*, 676 F.3d 71 (2d Cir. 2012). The Second Circuit explained that Aleynikov's upload of Goldman Sachs' internal trading code to an overseas server did not violate the EEA because it did not involve "interstate commerce," and did not violate the NSPA because the code was not "tangible property." The Second Circuit's reasoning underscores the difficulties involved in applying the plain wording of certain criminal statutes to actions taken by departing employees in the digital age.

Background

In June 2009, prior to leaving Goldman Sachs to begin a new job with Teza Technologies LLC, a start-up trading company, Aleynikov uploaded source code from Goldman Sachs' high-frequency trading system to an overseas server. He later downloaded the code to a thumb drive. Goldman Sachs, upon discovering what it considered to be Aleynikov's theft of its highly valuable property, reported Aleynikov to the authorities. Aleynikov was arrested and, in December 2010, convicted for violating the NSPA and the EEA and sentenced to an eight year prison term. On February 17, 2012, barely hours after his attorneys argued to the Second Circuit that Aleynilov's conviction should be reversed, his conviction was overturned by the Court in a summary order and he was freed from prison. The Second Circuit's April 11, 2012 written decision provided the reasoning for this rare move.

Aleynikov Did Not Violate the NSPA or the EEA

The Court's April 11 decision set forth the simple reasons for Aleynikov's February release — his conviction for stealing Goldman Sach's computer code was improperly premised on violations of the NSPA and the EEA, neither of which applied to his actions.

The NSPA criminalizes the transportation, transmittal or transfer "in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud." 18 U.S.C. § 2314. In the absence of a statutory definition of "goods, wares [and] merchandise," courts have generally interpreted the terms to mean types of *tangible* property ordinarily a subject of commerce, and that "the theft and subsequent interstate transmission of purely *intangible* property is beyond the scope of the NSPA." 676 F.3d at 77 (emphasis added).

Declining "to stretch or update statutory words of plain and ordinary meaning in order to better accommodate the digital age," the Court determined that by uploading Goldman Sach's proprietary source code, "Aleynikov stole purely intangible property embodied in a purely intangible format." *Id*. at 78. The Court found unpersuasive the argument that Aleynikov's subsequent transfer of the code to a thumb drive altered the nature of the intangible property such that it should be considered a stolen "good" as defined in the NSPA. *Id.* "Because Aleynikov did not 'assume physical control' over anything when he took the source code, and because he did not thereby 'deprive [Goldman] of its use,' Aleynikov did not violate the NSPA." *Id.* at 78-79.

The EEA, on the other hand, is violated by anyone who, "with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other that the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly…without authorization…downloads, uploads,…transmits …or conveys such information." 18 U.S.C. § 1832(a). Analyzing the legislative history of the statute and applying doctrines of statutory interpretation, the Court concluded that the district court incorrectly determined, for purposes of the EEA, that "a product is 'produced for' interstate or foreign commerce if its purpose is to facilitate or engage in such commerce." 676 F.3d at 80. The Second Circuit found that the district court's broad interpretation would cover every product and, if that were the case, there would be no reason for Congress to have included in the statute the alternative phrase of "or placed in" interstate or foreign commerce. *Id.* at 80-81.

The Second Circuit concluded that Goldman Sach's confidential and proprietary trading system and source code was neither "produced for" nor "placed in" interstate or foreign commerce because it was an internal product that Goldman Sachs had no intention of selling or licensing to others. "Because the [trading system] was not designed to enter or pass in commerce, or to make something that does, Aleynikov's theft of source code relating to that system was not an offense under the EEA." *Id.* at 82.

What This Decision Means for Companies

By interpreting the NSPA and EEA narrowly, the Second Circuit sent companies a message that the plain wording of criminal statutes will continue to apply, despite changing technology. Absent Congressional action to revise the NSPA and the EEA, where an employee steals a company's proprietary, but solely internal intangible property, the company likely will be limited to seeking civil remedies against the offending employee.

Ninth Circuit's Decision Creates Circuit Split Over Scope of Computer Fraud and Abuse Act

On April 10, 2012, the *en banc* United States Court of Appeals for the Ninth Circuit in *U.S. v. Nosal*, in an opinion authored by Chief Judge Alex Kozinski, limited the applicability of the Computer Fraud and Abuse Act (the "CFAA"). 676 F.3d 854 (9th Cir. 2012). The Ninth Circuit held that gaining authorized access to, and subsequently using, information for a purpose prohibited by a computer-use agreement, even for a fraudulent purpose, did not constitute "exceeding authorized access," and therefore did not violate the CFAA. The Ninth Circuit decision created a circuit split with earlier interpretations of the CFAA by the Fifth, Seventh and Eleventh Circuits.

Background

The CFAA is primarily a criminal statute, focused chiefly on deterring and punishing third party computer hacking. However, the CFAA also authorizes companies to bring civil suits against individuals who access a protected computer "without authorization" or while "exceed[ing] authorized access." These civil remedies have led to an increase in lawsuits brought by employers against former employees who have misappropriated for their own use confidential or proprietary data from company computers.

That is precisely what happened in the *Nosal* case. Defendant David Nosal, a former executive at Korn/Ferry, a search firm, resigned his position at Korn/Ferry to form a competing business. He convinced several of his former Korn/Ferry co-workers to do likewise. Prior to the other employees' resignations, however, they used their authorization to access Korn/Ferry's computers to download confidential information from Korn/Ferry's network – including source lists, names and contact information – and, despite a policy prohibiting them from disclosing confidential information, provided the source data to Nosal in order to compete against Korn/Ferry.

The Government indicted Nosal for, among other things, aiding and abetting violations of the CFAA. The District Court for the Northern District of California dismissed the CFAA claims, finding that Nosal's actions did not fall within the scope of the CFAA. A Ninth Circuit panel, however, reversed that decision, reinstating the CFAA claims, but the *en banc* Court overturned the panel decision and dismissed the claims.

Nosal Did Not Violate the CFAA

At issue in this case was whether the CFAA criminalizes an employee's removal of confidential information from a computer in violation of company non-disclosure policies where the employer had placed no restrictions on the employee's access to such information. In determining the answer to be "no," the Ninth Circuit drew a distinction between access and use restrictions.

The CFAA defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to so obtain or alter." 18 U.S.C. § 1030(e)(6). The Government argued, and the Court ultimately rejected, that this definition includes a person who has unlimited *access* to a computer, but is limited in his ability to use the information to which he has access. Instead, the Court adopted the District Court's more narrow view of the definition, relating to a person who has authorized access to some parts of a computer but "hacks" into unauthorized sections. The Court looked to principles of statutory construction to reach this conclusion, such as the plain language of the statute and the practice of narrowly construing ambiguous criminal statutes to avoid judicial creation of a criminal law.

The Ninth Circuit's *en banc* decision cautioned against turning the CFAA "from an anti-hacking statute into an expansive misappropriation statute" or "sweeping Internet-policing mandate." 676 F.3d at 857. Citing numerous examples of potential employer-employee and consumer disputes that would be encompassed by such a broad interpretation of the CFAA, the Court warned that "[b]asing criminal liability on violations of private computer use policies can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved." *Id.* at 860.

In declining to interpret the CFAA broadly to cover violations of corporate computer use policies and/or an employee's duty of loyalty, and thereby creating a circuit split on what is proving to be frequent source of litigation, the Ninth Circuit pointedly declined to "follow our sister circuits and urge them to reconsider instead." *Id.* at 863. The Court criticized the Fifth, Seventh and Eleventh Circuits for failing to consider the effects of their decisions on everyday people, and for failing to follow basic principles of statutory construction.

A strongly worded dissenting opinion criticized the majority for its reading of the statute and focusing on a "parade of horribles" that could occur under the CFAA generally, as opposed to the specific section of the CFAA at issue in the case.

Conclusion

In rejecting the more expansive reading of the CFAA adopted by the Fifth, Seventh and Eleventh Circuits, as well as a number of District Courts, the Ninth Circuit decision in *U.S. v. Nosal* creates a circuit split. The Government has asked for and received an extension of time through August 8, 2012 to appeal the decision to the U.S. Supreme Court. While the Second Circuit has not had the opportunity to weigh in on this issue, several New York District Court opinions have adopted the more narrow view set out in the Ninth Circuit's *en banc* decision that an employee's authority to access information is not defined by what the employee does with the information, but rather is defined by whether they had permission to access the information in the first place. Thus, until the Second Circuit or the Supreme Court provides further guidance, employers in New York should expect that the CFAA will be applied narrowly to employee data theft situations.