WHITE-COLLAR CRIME COMMITTEE NEWSLETTER

Winter 2017

In This Issue

Important Dates

Business Law Section Spring Meeting
April 6-8, 2017
New Orleans, LA

Editorial Board

DOJ wants your U.S. export controls and sanctions disclosures: what's the impact

By David Ring

This article is reprinted from the November 2016 issue of WorldECR, the journal of export controls and sanctions.
www.worldecr.com

The U.S. Department of Justice, National Security Division recently published guidance which encourages companies to voluntarily self-disclose directly to it possible wilful violations of U.S. export controls and sanctions. David A. Ring examines the pros and cons of self-disclosure of what are, essentially, criminal violations.

Read more...

The Lanham Act and the Food, Drug, and Cosmetic Act: When Private Pharmaceutical Litigation Complements FDA Regulatory Enforcement

By Thomas A. Capezza

This article addresses the interplay between two federal statutes that complement one another; the interplay between private litigants, whose expertise lies in understanding market dynamics, and the Food and Drug Administration ("FDA"), whose expertise lies in public health and safety. The article focuses on the U.S. Supreme Court's decision in POM Wonderful and the pharmaceutical cases following that decision.

Read more...

Innocent Password Sharing: A Prosecutable Offense?

By Gregory J. O'Connell & Peter J. Sluka

In a decision published this summer, the U.S. Court of Appeals for the Ninth Circuit affirmed the conviction under the Computer Fraud and Abuse Act ("CFAA") of an individual who used his former colleague's login and password to reach a proprietary portion of his former employer's network.1 While the case involves the theft of corporate proprietary information, it also illustrates the potential for broader application of the CFAA to more benign cases of "password sharing"-using credentials freely provided by a friend or colleague to access a protected website, such as a video streaming service.2 To make matters worse, a CFAA charge could lead to an additional charge of aggravated identity theft-a crime which is itself broadening and which imposes a mandatory two-year consecutive sentence.3 As discussed below, broad interpretations of both the computer fraud and aggravated identity theft statutes have caused these crimes to overlap in the area of password sharing, and a creative prosecutor could join

these charges to seriously raise the stakes for even the most benign password sharers. In light of these trends, individuals and corporations would be wise to take a fresh look at their practices and policies regarding shared computer access credentials.

Read more...

Possible Outcomes for the Financial Sector in the Trump Era

By Patty P. Tehrani

The General Counsel calls you to prepare a summary of possible outcomes for the financial services industry following Donald Trump's unexpected victory. She has a meeting with your company's CEO to advise her on what to expect in the coming years. You don't have much to work with. The recent market surge would suggest that a Trump victory could be a huge win for the financial industry. On the other hand, the lack of specific proposals has resulted in more questions than answers.

Read more...

DOJ wants your U.S. export controls and sanctions disclosures: what's the impact?

The U.S. Department of Justice, National Security Division recently published guidance which encourages companies to voluntarily self-disclose directly to it possible wilful violations of U.S. export controls and sanctions. David A. Ring examines the pros and cons of self-disclosure of what are, essentially, criminal violations.

On 2 October 2016, the U.S. Department of Justice ('DOJ'), National Security Division ('NSD') published guidance[1] encouraging organisations to voluntarily self-disclose possible wilful – and therefore criminal – violations of U.S. export controls and sanctions directly to NSD. This guidance is applicable not only to U.S. companies, but to non-U.S. companies that are subject to the extraterritorial reach of U.S. export and sanctions laws. Because this policy marks an extension of the U.S. government's efforts to hold individuals criminally liable for corporate wrongdoing, companies everywhere should take notice.

NSD's newly announced guidance, at its core, encourages companies to disclose possible criminal violations of export control and sanctions laws, and offers leniency and benefits to companies that do so and, then, cooperate with law enforcement. This guidance aligns NSD with other DOJ components that have promulgated disclosure guidelines in an attempt to bolster DOJ's efforts to hold companies and – especially – individuals criminally responsible for regulatory wrongdoing. Consistent with the Yates Memo[2] issued late last year, NSD's guidance makes clear that its primary purposes include encouraging companies to implement stronger efforts to 'prevent and detect' violations, and increasing NSD's ability '*to prosecute individual wrongdoers whose conduct might otherwise have gone undiscovered or been impossible to prove*' [emphasis added].

Of interest to non-U.S. businesses headquartered in the U.S., the new guidance explicitly offers leniency to U.S.-parent companies that make available evidence and witnesses from their overseas subsidiaries, especially when such evidence and witnesses otherwise would not be available under international treaties. Similarly, leniency would be extended to non-U.S. companies that voluntarily disclose to NSD criminal violations of U.S. laws by their non-U.S. employees. While DOJ recognises that, in some instances, non-U.S. law may prohibit disclosure, it places the burden on companies to prove that a disclosure was prohibited, and nonetheless encourages companies to 'identify all available legal bases' for cooperating with the DOJ.

Leniency would be extended to non-U.S. companies that voluntarily disclose to NSD criminal violations of U.S. laws by their non-U.S. employees.

NSD's new guidance marks a significant departure from the long-established practice of encouraging companies to voluntarily disclose export and sanctions violations to the pertinent regulatory agencies (i.e., the Department of State's Directorate of Defense Trade Controls, the Department of Commerce's Bureau of Industry and Security, the Treasury Department's Office of Foreign Assets Control), and then relying on law enforcement liaisons within those agencies to determine which disclosures warrant additional scrutiny. Now, companies are expected to determine whether a violation is wilful (and therefore criminal), and, if so, whether to disclose the violation to both the regulatory agency and NSD.

Not only does this mark a change in DOJ's expectations regarding where a disclosure should go, it marks a change in what is said in disclosures and how they are investigated, as well. Under current regulations, companies are instructed to disclose (among other things) whether any individual acted 'intentionally'. That analysis is largely factual and straightforward: Did the employee act purposefully to accomplish what was done, or not? But NSD's newly released guidance requires another level of legal analysis: whether any employee acted 'wilfully,' which NSD defines as 'done with the knowledge that it is illegal'.

NSD's 'wilfulness' analysis raises a number of questions and challenges. First, it's by no means settled that a criminal violation of export laws requires only general knowledge of illegality, rather than specific knowledge of the underlying regulatory requirements. Compare *U.S. v. Pulungan*, 569 F3d 326 (7th Cir. 2009) (defendant cannot be convicted of wilfully attempting to export a defence article unless he knew the item was a 'defence article') with *U.S. v. Bishop*, 740 F3d 927 (4th Cir. 2014) (upholding conviction of wilfully attempting to export a defence article where the defendant believed the export was illegal, but did not know the items were 'defence articles'). The new guidance, therefore, may put companies in the uncomfortable position of disclosing 'wilful' conduct to NSD in order to obtain leniency, while still maintaining that the conduct was not wilful under applicable law. Moreover, and perhaps more problematic, compliance personnel who typically draft and submit disclosures may be ill-suited to make the delicate determination of

Links and notes

[1] https://www.justice.gov/nsd/file/902491/download
[2] https://www.justice.gov/dag/file/769036/download

whether a fellow employee may have known his or her actions were illegal. Typically, criminality turns on circumstantial evidence and inference, which require a type of analysis not normally made by in-house personnel. The consequences for disclosing a wilful violation to NSD can be extreme, and the decision to do so should not be made lightly by those who are not well versed with the intricacies of U.S. criminal law.

Disclosure dilemmas

So what of the beleaguered business manager who authorises IT access to a new non-U.S. employee knowing that company policy – and presumably the underlying regulations – doesn't allow access to a portion of the data contained in the system? Surely the violation (if there was one) would be 'knowing' under the ITAR, but is it 'wilful'? What if the new employee was Chinese? What if, unknown to the manager, technical data were actually accessed by the new employee for no known business reason? In the highly technical realm of export and sanctions compliance – where violations can occur in a myriad of ways – a decision to disclose to NSD will involve a calculation of numerous factors beyond whether an employee acted with knowledge that a regulatory violation would occur. For instance, consideration should be given to the seriousness of the conduct, the potential for harm, the employee's underlying motivations, and the subjective determination of whether a law enforcement agency might care. As a practical matter, companies will now be asked to make a law enforcement assessment for the government, and must face the risks inherent to this determination: under-disclosure may deprive the company of significant benefits, whereas over-disclosure might lead to absurd results, including criminal referrals for pedestrian conduct.

Companies need to proceed with caution before deciding whether to disclose potential wilful conduct to NSD.

At bottom, it remains to be seen what tangible benefits will be bestowed on companies that make disclosures under NSD's new policy. If recent FCPA cases are any indicator, the benefits may be substantial. But companies need to proceed with caution before deciding whether to disclose potential wilful conduct to NSD. And at the very least, NSD's new guidelines should make clear that DOJ expects companies to do more to detect possible criminal violations, and that DOJ itself intends to do more to hold individuals criminally responsible for trade compliance violations.

David Ring, a partner at Wiggin and Dana LLP, serves as a U.S. State Department appointed monitor for a global aerospace company. He also conducts corporate investigations on a variety of legal and regulatory issues, provides compliance and ethics counseling, and defends individuals and companies accused of crime.

dring@wiggin.com

This article is reprinted from the November 2016 issue of *WorldECR*, the journal of export controls and sanctions.

www.worldecr.com

The Lanham Act and the Food, Drug, and Cosmetic Act: When Private Pharmaceutical Litigation Complements FDA Regulatory Enforcement

by Thomas A. Capezza[*]

This article addresses the interplay between two federal statutes that complement one another; the interplay between private litigants, whose expertise lies in understanding market dynamics, and the Food and Drug Administration ("FDA"), whose expertise lies in public health and safety. The article focuses on the U.S. Supreme Court's decision in *POM Wonderful* and the pharmaceutical cases following that decision.

The Lanham Act creates a cause of action against any person who "uses in commerce any . . . false or misleading description of fact, or false or misleading representation of fact, which . . . misrepresents the nature, characteristics [or] qualities . . . of his or her or another person's goods, or services, or commercial activities." 15 U.S.C. § 1125(a)(1). The purpose of the Lanham Act is "to protect persons engaged in such commerce against unfair competition" and "to prevent fraud and deception." 15 U.S.C. § 1127. To that end, the Lanham Act affords private litigants damages and injunctive relief. The Food, Drug, and Cosmetic Act ("FDCA"), by contrast, is enforced by the FDA and intended to protect the health and safety of the public at large. 21 U.S.C. §§ 301-399f.

POM Wonderful LLC v. Coca-Cola Co.

In *POM Wonderful LLC v. Coca-Cola Co.*, 134 S. Ct. 2228 (2014), the U.S. Supreme Court considered whether a private party may bring a Lanham Act claim challenging a food label that is regulated by the Food, Drug, and Cosmetic Act (FDCA). Specifically, POM Wonderful LLC made and sold pomegranate juice products, including a pomegranate-blueberry juice blend. Its competitor, the Coca-Cola Company, made a juice blend containing only 0.3% pomegranate juice and 0.2% blueberry juice. Yet, the words "pomegranate blueberry" were prominently displayed on the Coca-Cola label. *Id.* at 2235.

Alleging that the use of that label was deceptive and misleading, POM sued Coca-Cola under section 43 of the Lanham Act, which allows one competitor to sue another if it alleges unfair competition arising from false or misleading product descriptions. *Id.* The District Court granted partial summary judgment to Coca-Cola on POM's Lanham Act claim, reasoning that the FDCA and its regulations preclude challenges to the name and label. 727 F. Supp.2d 849, 871-73 (C.D. Cal. 2010). The Court of Appeals for the Ninth Circuit affirmed in relevant part. 679 F.3d 1170, 1178 (9th Cir. 2012).

[*] Thomas A. Capezza is a Director at Carter, Conboy, Case, Blackmore, Maloney & Laird, P.C., specializing in white collar litigation and government investigations.

The Supreme Court reversed reasoning that this was a "preclusion" (federal-federal) case, not a "pre-emption" (state-federal) case. *Id.* at 2236-37. Looking next to the statutory text, the Court concluded that neither the Lanham Act nor the FDCA forbids or limits Lanham Act claims challenging labels that are regulated by the FDCA. Next, the Court looked to the purpose of each statute reasoning that: "The Lanham Act and the FDCA complement each other in major respects, for each has its own scope and purpose. Although both statutes touch on food and beverage labeling, the Lanham Act protects commercial interests against unfair competition, while the FDCA protects public health and safety." *Id.* at 2238. Finally, the Court also took note of the functional aspects of each statute and the expertise of the relevant parties. Specifically, the Court considered FDA's enforcement of the FDCA, and "detailed prescriptions of its implementing regulations," and the "expertise in assessing market dynamics that day-to-day competitors possess." *Id.* at 2238-39.

Lanham Act Cases Following POM Wonderful

Private plaintiffs since *POM Wonderful* have brought Lanham Act claims in the context of a variety of labels beyond food and beverage; defendants, conversely, have steadfastly argued preclusion and challenged the sufficiency of pleadings and the merits, all to contain the reach of the Lanham Act following *POM Wonderful*. This article focuses on those issues as they relate to pharmaceutical cases. Two Second Circuit cases figure prominently in the Post-*POM Wonderful* dialogue.

Preclusion Challenges

Fact-based claims in promotional material that do not invoke the expertise of the FDA have survived preclusion challenges. For example, preclusion arguments regarding representations that a given drug was FDA-approved have been largely unsuccessful. *See JHP Pharms., LLC v. Hospira, Inc.*, 52 F. Supp.3d 992, 999-1000 (C.D. Cal. 2014) (because obtaining FDA approval is costly, "representations that a drug is approved when it is not undermine the Lanham Act's public policy goals both by confusing consumers and by enabling unfair competition by producers who have not bothered to get FDA approval"); *Par Sterile Prods., LLC v. Fresenius Kabi USA LLC*, 2015 U.S. Dist. LEXIS 32409 (N.D. Ill., March 17, 2015). The reasoning, in such cases, is that FDA-approval is a specific and particularized claim, the imprimatur of FDA approval, and not whether a product is safe and effective enough to be approved by the FDA. *Id. at *10*. Likewise, other fact-based representations, including whether a test was conducted or not, have not been precluded. *See Catheter Connections, Inc. v. Ivera Med. Corp.*, 2014 U.S. Dist LEXIS 98206 (D. Utah, July 17, 2014).

Separately, preclusion arguments have arisen in the context of FDA review of labeling and promotional materials. Specifically, certain "medical devices" are subject to premarket FDA review pursuant to a "§ 510(k) process" (21 U.S.C. § 360(k)) to determine whether a given device is "substantially equivalent" to an existing authorized device. *See Medtronic, Inc. v. Lohr*, 518 U.S. 470, 478-79 (1996). A determination of substantial equivalence is essentially a finding that the new device is as safe and

effective as the preexisting device and may, therefore, be marketed. *Id.* Notwithstanding such a finding, under § 513(i)(1)(E) of the FCDA, the FDA may nevertheless require changes to the product's labeling or promotional materials. 21 U.S.C. § 360c(i)(1)(E). In *Church & Dwight Co. v. SPD Swiss Precision Diagnostics, GmbH*, 836 F.3d 153 (2d Cir, 2016), the Second Circuit, applying *POM Wonderful*, rejected defendant's preclusion argument holding that FDA's "§ 510(k) process" does not categorically immunize product labeling from Lanham Act claims. *Id.* at 166. Consistent with *POM Wonderful*, the Second Circuit noted, among other things, that FDA is not charged with protecting the interests of its subject's competitors. *Id.* at 166-67.

By contrast, representations that require FDA expertise have been precluded. For example, a representation that a medical device did not need FDA clearance independent of the 510(k) process was held to be precluded by the FDCA. *See Catheter Connections, Inc.*, 2014 U.S. Dist LEXIS 98206 (D. Utah, July 17, 2014), at *15; *see also Cottrell, Ltd. v. Biotrol Int'l, Inc.,* 191 F.3d 1248, 1256 (10th Cir. 1999) ("[if] the circumstances 'inherently require' court interpretation of the FDCA and implementing regulations, the area of inquiry is precluded.").

The Merits of Lanham Act Claims

In the context of promotional claims made in interstate commerce, private plaintiffs are required to establish falsity, materiality and the cause of actual or likely injury to the plaintiff.

Falsity may be established in two ways. First, a plaintiff may demonstrate that an advertising claim is literally false or false on its face. *Apotex Inc. v. Acorda Therapeutics, Inc.*, 823 F.3d 51, 63 (2d Cir. 2016) (citations omitted) (affirming a district court's decision to grant summary judgment in defendant's favor regarding advertising that merely *repeated* labeling that had been approved by FDA; falsity requires advertising claims that are *inconsistent* with FDA label.). In such a case, consumer deception is presumed and the court may grant relief without reference to the impact on the buying public. *Id.* Literal falsity is considered in full context and extrinsic evidence of consumer confusion is not necessary. *Id.* (relevant context of an advertisement is the advertising brochure, not external marketing documents). Literal falsity must also be unambiguously false; a promotional claim that is capable of more than one interpretation cannot be literally false. *Id.* One example of literal falsity is the claim of test-proven superiority. Specifically, literal falsity of a test-proven superiority claim is established when a plaintiff meets his or her burden and proves that the tests did not establish defendant's product as superior. *Id.*

When a promotional claim is not literally false, falsity may nevertheless exist because a promotional claim is likely to mislead or confuse customers. *Id.* at 63. In such instances, implicit falsity is established by comparing the *impression* left by the statement with the *truth*, not (as in the case of literal falsity) by comparing the statement itself with the truth. *Id.* Unlike literal falsity, implicit falsity requires extrinsic evidence of

consumer deception or confusion. *Id.* Alternatively, implicit falsity has been supported by evidence that the defendant intended to deceive the public through deliberate, egregious, conduct creating a rebuttable presumption of consumer confusion. *See Church & Dwight Co.*, 836 F.3d at 168-69 (citations omitted).

The false promotional claim must also involve the *separate* element that the claim involves an inherent or material quality of the product. *Apotex Inc.*, 823 F.3d at 63-64. Materiality, in these circumstances, is generally accepted as "likely to influence purchasing decisions." *Id.* (citations omitted). In this context, promotional claims that are fully consistent with FDA-approved labels generally have not supported Lanham Act liability. *Id.* (citations omitted). The justification for such a decision is rooted in deference to the expertise of the FDA and First Amendment protections. *Id.* Literally false claims, in light of the presumption that makes consideration on the buying public unnecessary for purposes of falsity, nevertheless require a showing that the claim involves an inherent or material quality of the product ("likely to influence purchasing decisions"), for purposes of the separate element of materiality. *Id.* (affirming district court's decision to grant summary judgment; while the statement in question was deemed to be false, plaintiff failed to cite a material issue as to the representation's impact on the decision to purchase for purposes of materiality).

Plaintiffs are also required to establish that the false, material, promotional claim caused actual or likely injury to the plaintiff. *See Church & Dwight Co.*, 836 F.3d at 173-75 (citation omitted). The standard is whether it is likely that the defendant's advertising has caused or will cause a loss to plaintiff's sales. *Id.* (affirming trial court's finding of liability following bench trial; standard for liability stage is reasonable basis that plaintiff is likely to be damaged because of false advertising). Typically, the actual or likely injury element is satisfied when plaintiff establishes that plaintiff and defendant are competitors in a relevant market, and plaintiff demonstrates a logical causal connection between defendant's false advertising and its own sales. *Id.* Finally, while the materiality of the falsity and likelihood of injury to the plaintiff resulting from the defendant's falsity are separate elements, a finding by a court that a plaintiff has been injured or is likely to be injured, will satisfy the materiality standard, particularly where the defendant and plaintiff are competitors in the relevant market, and the falsity of the defendant's advertising is likely to lead customers to prefer the defendant's product over the plaintiff's. *Id.* (citations omitted).

Looking Ahead

The preference favoring Lanham Act claims shows no signs of abating. Indeed, as we potentially enter a period wherein public policy favors less federal government regulation and less enforcement in favor of allowing the markets to regulate themselves, presumably, Lanham Act claims by private litigants and business competitors will only increase.

Innocent Password Sharing: A Prosecutable Offense?

Gregory J. O'Connell & Peter J. Sluka[†]

In a decision published this summer, the U.S. Court of Appeals for the Ninth Circuit affirmed the conviction under the Computer Fraud and Abuse Act ("CFAA") of an individual who used his former colleague's login and password to reach a proprietary portion of his former employer's network.[1] While the case involves the theft of corporate proprietary information, it also illustrates the potential for broader application of the CFAA to more benign cases of "password sharing"—using credentials freely provided by a friend or colleague to access a protected website, such as a video streaming service.[2] To make matters worse, a CFAA charge could lead to an additional charge of aggravated identity theft—a crime which is itself broadening and which imposes a mandatory two-year consecutive sentence.[3] As discussed below, broad interpretations of both the computer fraud and aggravated identity theft statutes have caused these crimes to overlap in the area of password sharing, and a creative prosecutor could join these charges to seriously raise the stakes for even the most benign password sharers. In light of these trends, individuals and corporations would be wise to take a fresh look at their practices and policies regarding shared computer access credentials.

U.S. v. Nosal considers a case of unauthorized access to corporate proprietary information. In 2004, David Nosal agreed to serve a one-year term as an independent contractor for his former employer, Korn/Ferry Executive Recruiting Services.[4] Soon after, he and two colleagues began covertly developing their own recruiting company, which would compete with Korn/Ferry when Nosal's contract ended.[5] When Korn/Ferry learned of the trio's plans, the company revoked their access to its computer network.[6] By revoking their access, the company deprived the trio of a critical tool in the development of their new company: Korn/Ferry's proprietary database of executives, resumes, compensation data, and the like.[7] On three occasions after their access was revoked, Nosal's colleagues used a login and password provided by his former executive assistant, who was still employed at Korn/Ferry, to access the company's proprietary database.[8]

[†] Gregory J. O'Connell is a partner and Peter J. Sluka is an associate at De Feis O'Connell & Rose, P.C., a firm specializing in white collar defense.

[1] *United States v. Nosal*, Nos. 14-10037, 14-10275, 2016 U.S. App. LEXIS 12382 (9th Cir. July 5, 2016).

[2] *See, e.g.*, Allan Yu, *How a "Nightmare" Law Could Make Sharing Passwords Illegal*, NPR, July 14, 2016, http://www.npr.org/sections/alltechconsidered/2016/07/14/485735920/how-a-nightmare-law-could-make-sharing-passwords-illegal; Jacob Gershman, *Appeals Court: Using Shared Password to Steal Company Secrets is Hacking*, WSJ, July 5, 2016, http://blogs.wsj.com/law/2016/07/05/appeals-court-using-shared-password-to-steal-company-secrets-is-hacking.

[3] 18 U.S.C. § 1028A.

[4] *Nosal*, 2016 U.S. App. LEXIS 12382, at *8-9.

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] *Id.* at *10-12.

Nosal was charged with three counts of violating the CFAA's prohibition on obtaining information by means of unauthorized access to a protected computer. Specifically, the CFAA provides:

> Whoever . . . knowingly and with intent to defraud, accesses a protected computer *without authorization*, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value . . . shall be punished as provided in subsection (c) of this section.[9]

At trial, the jury was instructed that the statute's phrase "without authorization," referred only to permission granted or revoked by Korn/Ferry, not Nosal's former assistant.[10] Nosal was convicted even though his former assistant consented to the use of her credentials.

On appeal, Nosal argued that the trial court improperly defined the "without authorization" element of the statute. He insisted that his accessing Korn/Ferry's database after the company had revoked his credentials was not access without authorization because his former assistant granted permission to use her credentials.[11] Though Nosal's former assistant could not formally restore the authorization revoked by the company, Nosal urged that "authorization" as the term is used in the CFAA must also include permission granted by a password sharer. Holding otherwise, Nosal insisted, would criminalize even the most common and innocuous instances of password sharing.[12] Nosal spun a host of hypotheticals where a shared password is used without the permission of the website's owner: A wife's accessing her husband's email account to forward a document, a mother's logging into her daughter's Facebook profile to check her postings, or a student's borrowing his roommate's ESPN streaming access to watch a game.[13] The CFAA, he argued, could not be so broad as to criminalize these instances.

The Ninth Circuit affirmed Nosal's conviction. The Court held, consistent with a plain reading of the statute, that Nosal's using another employee's credentials to access the company database after their credentials were revoked was access "without authorization" under the CFAA.[14] Because the company had revoked Nosal's authorization, his former assistant's permission was immaterial.[15] The Court rejected Nosal's insistence that his case must rise and fall with all cases of password sharing; his conduct, the Court remarked, was a far cry from a wife's logging on to her husband's email account to print a boarding pass.[16]

---

[9] 18 U.S.C § 1030(a)(4) (emphasis added).
[10] *Nosal*, 2016 U.S. App. LEXIS 12382, at *30-31.
[11] Opening Brief of Appellant at 18-19, *United States v. Nosal*, Nos. 14-10037, 14-10275, 2016 U.S. App. LEXIS 12382 (9th Cir. July 5, 2016).
[12] *Id.* at 22, 24-25.
[13] *Id.* at 19.
[14] *Nosal*, 2016 U.S. App. LEXIS 12382, at *20-21.
[15] *Id.*
[16] *Id.* at *29-30.

The *Nosal* Court was careful to avoid opining on a more innocent case of password sharing, but the case nonetheless raises the potential that a prosecutor could apply its core holding—that the "without authorization" element of the CFAA refers to authorization granted by the website's owner and not other password holders—to more benign facts. If only the owner of the password-protected content can provide authorization, then arguably *any* use of another's credentials without the owner's consent is punishable under the CFAA. Because a video streaming service does not authorize the subscriber's roommate to view its content, for example, the roommate's use of those credentials on his own device, even with the subscriber's consent, could run afoul of the CFAA's prohibition on access without authorization.

While *Nosal* raises the concern that seemingly innocent cases of password sharing might violate the letter of the CFAA, the aggravated identity theft statute also threatens to apply. A person commits aggravated identity theft where she, "during and in relation to [certain enumerated felonies, including CFAA violations], knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person."[17]

Just like the CFAA, the aggravated identity theft statute contains no carve-out for cases where an individual consents to another's use of his identity, and courts have generally refused to read one into the statute. As a consequence, a person can be guilty of aggravated identity theft where the identity used in the underlying crime is not stolen, but freely provided. For instance, a son who used his father's social security number with his father's consent was held guilty of aggravated identity theft.[18] Similarly, an individual who, with his friend's permission, used his friend's name and address on fraudulent warranty submissions,[19] a Medicare fraudster who submitted claims for fictitious treatments of real patients who had freely provided him their Medicare information,[20] and an individual who used his half-brother's name on a passport application[21] all faced the added charge of aggravated identity theft (and consequentially, the threat of an additional two-year prison term) even though none of the identities used were stolen.[22]

Paradoxically then, although using a login and password shared by a friend or colleague involves neither hacking nor identity theft, the conduct potentially runs afoul of statutes aimed at

---

[17] 18 U.S.C. § 1028A(a)(1).
[18] *See United States v. Retana*, 641 F.3d 272, 275 (8th Cir. 2011).
[19] *See United States v. Kuc*, 737 F.3d 129, 134 (1st Cir. 2013).
[20] *See United States v. Cwibeker*, No. 12-CR-0632 (JS), 2015 U.S. Dist. LEXIS 12432 (E.D.N.Y. Feb. 2, 2015).
[21] *See United States v. Roberts-Rahim*, No. 15-CR-243 (DLI), 2015 U.S. Dist. LEXIS 143827, at *2 (E.D.N.Y. Oct. 22, 2015).
[22] The Seventh Circuit has read the aggravated identity theft statute to require the non-consent of the individual whose identity was used, but such a reading has not been adopted by its sister circuits. In *United States v. Spears*, the defendant created a counterfeit handgun permit for a client who, due to her criminal history, could not obtain a legitimate permit. 729 F.3d 753 (7th Cir. 2013). The counterfeit permit contained the client's own name and birthdate. *Id.* at 754. The defendant was convicted of Aggravated Identity Theft in violation of 18 U.S.C. § 1028A. On Appeal the defendant argued that he did not transfer the means of identification "of another person," because he transferred the information of the client, who had obviously consented to the transfer. *Id.* The court agreed, stating that while "[p]roviding a client with a bogus credential containing the client's own information is identity fraud," it was not identity theft; "no one's identity has been stolen or misappropriated." *Id.* at 756. In the majority of jurisdictions, however, the *theft* of the identity used is not required; a conviction will stand even in cases like *Spears*, where the individual willingly offered her identity for use in the predicate crimes.

preventing both. Even the most well-intentioned user of a shared password accesses content without the authorization of the content's owner, and the user therefore could be charged under the CFAA, as defined by *Nosal*. Similarly, under recent caselaw, the user may also be charged with aggravated identity theft for assuming the identity of the password sharer—by entering their login and password—during the commission of the CFAA violation. These are high-stakes charges. Both are felonies, and a conviction for aggravated identity theft imposes a mandatory two-year prison sentence that must run consecutive to any sentence imposed for the underlying CFAA violation.[23] While perhaps appropriate in cases like *Nosal*, the potential for these charges in cases of innocent password sharing is less palatable.

As the computer fraud and aggravated identity theft statutes threaten to apply to even the most benign cases of password sharing, the legislature might consider intervening. One legislative fix would be installing a threshold value that the content accessed must exceed in order to trigger a CFAA violation. The CFAA already employs a similar value threshold where the unauthorized access results only in the use of the computer.[24] A vestige of a time where computers were so scarce that their owners would rent their hourly use, the CFAA does not criminalize unauthorized access where the use of the computer was the only thing obtained and the value of that unauthorized use does not exceed $5,000 in any one year period.[25] Expanding this value threshold to all cases of unauthorized access would ensure that common and benign uses of a shared password—to access an email or stream a game—are not be punishable under the CFAA, while conduct like Nosal's—using a shared password to steal valuable corporate proprietary information—is.

Until further legislative action, however, and as long as the courts continue to adopt broad readings of the statutes at play, individuals and corporations must take care to ensure that passwords are treated not as physical keys—interchangeable, replicable, and freely transferable—but as unique, non-transferable access credentials granted *solely* to their intended recipient.

* * *

If you have any questions regarding the issues discussed herein, please contact Gregory J. O'Connell (212-768-2686), Peter J. Sluka (212-768-1000), or the DOR attorney with whom you regularly work.

[23] 18 U.S.C. §§ 1028A, 1030.
[24] 18 U.S.C. § 1030(a)(4).
[25] *Id.*

Possible Outcomes for the Financial Sector in the Trump Era

By: Patty P. Tehrani, Esq.

The General Counsel calls you to prepare a summary of possible outcomes for the financial services industry following Donald Trump's unexpected victory. She has a meeting with your company's CEO to advise her on what to expect in the coming years. You don't have much to work with. The recent market surge would suggest that a Trump victory could be a huge win for the financial industry. On the other hand, the lack of specific proposals has resulted in more questions than answers.

The best you can do is outline what has been reported to help identify possible outcomes for the financial sector during a Trump presidency:

- **Weakening of Financial Regulations** – Trump made it clear during his campaign that he is not a fan of regulations and believes they hinder business. And with a Republican-controlled Congress, he'll have the support that he needs to weaken or eliminate financial regulations. No specifics have been provided about the extent to which he will do this but here are some possibilities:
    - **Weaken Dodd-Frank** – The Dodd–Frank Wall Street Reform and Consumer Protection Act (click here) or Dodd–Frank was enacted in response to the 2008 financial crisis. The Act issued various new rules designed to protect consumers and possibly prevent another financial crisis. Considering the billions spent to comply with Dodd-Frank repealing it is unlikely. However, it should not come as a surprise if Dodd-Frank is weakened. The Trump team has said as much on its "Financial Services" policy page:

        > *The Financial Services Policy Implementation team will be working to dismantle the Dodd-Frank Act and replace it with new policies to encourage economic growth and job creation*.

        - **The Volcker Rule** – Dodd-Frank's Volcker Rule is possibly the least favorite requirement of the Act. The rule was named after former Federal Reserve Chairman Paul Volcker and serves as a de facto ban on proprietary trading. The basis for this ban is to prevent banks from using their own funds to make these investments to increase their profits at the expense of their customers. Financial firms would love to see this rule eliminated with some even seeking a five year deferment (click here) on implementing it. Don't expect this rule to survive as is under Trump.

        - **Consumer Financial Protection Bureau** (CFPB) – The future of this watchdog agency created under Dodd-Frank is up in the air. A

continuation of its current powers is unlikely, and so we should expect efforts to weaken the agency as evidenced by the following:

- Passing of the September bill written by the chair of the House Financial Services Committee, Representative Jeb Hensarling (R-Texas) to:
  - rename the agency to the Consumer Financial Opportunity Commission (to make it sound more business friendly);
  - have it run by a five-member, bipartisan commission instead of one director;
  - water down its enforcement power; and
  - reduce its authority to ban bank services or products deemed "abusive."
- Changing leadership of the agency:
  - refer to the recent Court of Appeals for the D.C. Circuit ruling to bolster efforts to change how and whether a director is appointed; and
    - The court found (click here) that the CFPB's organizational structure is unconstitutional since a single director appointed by the president does not provide for sufficient checks and balances. The court seemed to favor agencies that were run by multiple-commissioners. CFPB is appealing the decision.
  - expect Trump to replace the current CFPB Director, Richard Cordray, whose term is up in 2018 with a much more business-friendly replacement.
- Changing the funding of the agency from the current structure funded through the Federal Reserve to Congress and most likely result in a reduction in its funding.

Notwithstanding efforts to weaken the agency, it will most likely be kept in place. The public likes this agency as evidenced by the one million plus complaints received by the agency thus far. Trump would most likely face staunch and possibly insurmountable resistance from Democrats and consumer advocate groups if he elects to undo the agency.

- **Whistleblower Rules** – The whistleblower rules under Dodd-Frank are another area for consternation among the business community. Dodd-Frank amended the Securities Exchange Act of 1934 (the "Exchange Act") with Section 21F to establish a Securities Whistleblower Incentives and Protection program. By August 2016, the program had rewarded more than $100 million (click here) to whistleblowers who came forward with tips of corporate

malfeasance. While the program is not expected to go away, parts of it could be changed:

- Section 21F provides that the whistleblower program is intended to complement and not replace existing corporate compliance programs. Whistleblowers are also encouraged to work within their company's own compliance structure, if appropriate. Despite this language, opponents take issue with the ability of whistleblowers to report to the government before making such reports to their companies. As such, one key change could be the requirement that whistleblowers report wrongdoing *internally first* to their companies before reporting to the government.

- **Re-birth of Glass-Steagall** –The original Glass-Steagall Act, which required separation between bank lending and securities underwriting, may be back. Trump has called for a "21st century" version of the former law but thus far offered no further details as to what and how. For now, we just know that:
  - Separation of commercial and investment banks could be reinstated.
  - Certain banks that converted to banking holding companies following the 2008 financial crisis could return to being investment banks to avoid:
    - increased regulation and examination by governmental agencies;
    - limited ability to take risks; and
    - having to hold more capital on reserve.

- **Power of the Financial Sector Regulators** –Trump will most likely appoint pro-business financial sector regulators with conservative views on everything from enforcement penalties to governance. And with the Senate under Republican control, Trump will most likely fill these positions quickly. Consider some of the current choices for key administration positions:
  - Trump's senior adviser /strategist, Steve Bannon (a former Goldman Sachs Vice President);
  - Treasury Secretary, Steven Mnuchin, a former Goldman Sachs vice president); and
  - Securities and Exchange Commissioner (SEC) Chair, former Republican SEC Commissioner Paul Atkins is a top contender to replace Chair Mary Jo White. Atkins is currently running the relevant transition team.

- **Volatile Markets** – Markets are expected to be volatile considering the many unknowns and how they will impact the relevant sectors and company stocks. Consider the following as examples:

- Repeal and replace the Affordable Care Act and how this will impact the healthcare industry and insurance company stocks.
- More stringent immigration policies and how these could adversely impact companies that rely heavily on immigrants, such as food producers, hotels, and restaurants.
- New and revised tax and trade policies.
- Changes to the minimum wage and whether they could conceivably hurt or help companies (help by putting more money in consumers' pockets or hurt with a more expensive labor force).

- **Financial Services Sector Jobs** – A key Trump campaign promise was to bring jobs back to America. It is unclear how this promise will extend to the financial services sector. A less-regulated financial sector may result in the following:
  - Weakening of regulations may cause financial institutions to re-consider hiring plans for legal and compliance professionals originally slated to help with implementation and maintenance of these rules; and
  - Hiring efforts may focus more on front-office personnel.

Conclusion

In conclusion, what we know right now:

- We don't have enough specifics about Trump's financial policies to determine next steps.
- The unknows and uncertainty will result in periods of market volatility.
- Financial regulation will change due to:
  - Changes expected to Dodd-Frank and its requirements;
  - Selection of financial regulators and heads and the authority they will – less or the same but certainly not more; and
  - Efforts towards less regulation and weakening of those in existence.

Patty P. Tehrani, Lawyer and Founder of Policy Patty Toolkit, a consulting business that helps organizations in their efforts to develop, assess, or enhance their governance, compliance and risk management programs, policies, controls and processes.