Sharing of Passwords Under Certain Circumstances Unlawful

Prepared by:
Jeffrey M. Schlossberg
Jackson Lewis P.C.

LORMAN EDUCATION SERVICES
January 2017

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 700 available
- ☑ **Slide Decks -** More than 1700 available
- ☑ **White Papers**
- ☑ **Reports**
- ☑ **Articles**
- ☑ **... and much more!**

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: **www.lorman.com/pass/?s=special20**

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

Sharing of Passwords
Under Certain Circumstances Unlawful

Many companies have experienced the departure of an employee and the elimination of that former employees access to the company's computers and networks. In the recent case of *USA v. Nosal, D.C. No. 3:08-cr-00237-EMC-1 (July 5, 2016)*, the Ninth Circuit Court of Appeals was presented with the following facts: Nosal, a former employee of Korn/Ferry departed and launched a competitive entity. When Nosal left the company, the company revoked his computer access credentials. After his departure, Nosal was nevertheless able to continue accessing the company's confidential and proprietary information when his former secretary provided Nosal with her database access credentials. In *Nosal*, the question for the court was whether the jury properly convicted David Nosal of the crime of conspiracy under the Computer Fraud and Abuse Act ("CFAA") for accessing and downloading information from the company's database "without authorization." The Court in a 2-1 decision held that indeed Nosal violated the criminal provisions of CFAA even though he did not himself access and download the information.

The CFAA prohibits access to a computer or computer system by ones who are either exceeding authorized use or are not authorized users. 18 U.S.C. § 1030. The applicable section of the CFAA addressed in the *Nosal* case provides that:

> **Whoever . . . knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct further the**

> **intended fraud and obtains anything of value. . .shall be punished. . . . .**

The prosecution successfully argued that after Nosal left the company, he lacked any rights to use the company's network. Because he lacked rights to access the network, the use of the secretary's login credentials violated the CFAA's ban on access "without authorization." The court found that Nosal violated the CFAA because he "knowingly and with intent to defraud blatantly circumvented the affirmative revocation of his computer access. This access falls squarely within the CFAA's prohibition on access 'without authorization' and thus we affirm Nosal's conviction for violations of . . . the CFAA."

But, what about the fact that a person who did have authorization – Nosal's secretary – granted Nosal permission to access the database? On this point, the court stated that access:

> **'without authorization' is an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission. This definition has a simple corollary: once authorization to access a computer has been affirmatively revoked, the user cannot sidestep the statute by going through the back door and accessing the computer through a third party. Unequivocal revocation of computer access closes both the front door and the back door.**

The court further stated that an "employee could willy nilly give out passwords to anyone outside the company – former employees whose access had been revoked, competitors, industrious hackers, or bank robbers who find it less risky and more convenient to access accounts via the Internet rather than through armed robbery."

As a result of this decision, some privacy groups have expressed concern that the court's ruling could make it easier to prosecute people for ordinary password sharing, such as when a husband logs into his wife's Facebook account with her credentials and permission, or to print a boarding pass.

However, the majority addressed this concern square on stating that "hypotheticals about the dire consequences of criminalizing password sharing. . . miss the mark in this case. This case is not about password sharing" and noted that the case "bears little resemblance to asking a spouse to log in to an email account to print a boarding pass."

While this decision involved a criminal prosecution, with which most companies would not be involved, it is still worthy of consideration for employers. Many employers have some form of agreement in place that would make accessing the company's database after termination a violation. In light of *Nosal* it would be prudent for a company to also include in its policies and agreements what is seemingly obvious – prohibit current employees from providing their passwords to former employees. At least with this statement in writing, the company will have (1) a basis upon which to take appropriate disciplinary action – including termination – against the current employee who provided their password to a former employee, and (2) the ability to commence a civil legal action against the former employee under the CFAA.