PROGRAM MATERIALS
Program #3122
February 3, 2021

What is "Authorized Access" and How Do Employers Deal with Misuse of Access Credentials Post-VanBuren vs United States

Celesq® AttorneysEd Center
www.celesq.com

5255 North Federal Highway, Suite 310, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

What is "Authorized Access" and How Do Employers Deal with Misuse of Access Credentials Post - *VanBuren vs United States*

Michelle A. Schaap
Chiesa Shahinian & Giantomasi PC
February, 2021

LEGAL DISCLAIMER

This outline has been prepared for a presentation regarding "Authorized Access" and How Do Employers Deal with Misuse of Access Credentials Post-*VanBuren vs United States*. Ms. Schaap is admitted to practice law in the State of New Jersey. This outline is for informational purposes only and is not intended to constitute legal advice. Every matter has specific facts and special circumstances requiring its own analysis by legal counsel. References to websites, resources or publications in this outline are not intended, and should not be interpreted, as an endorsement by the authors of any product or opinion set forth therein. Website and resource addresses are provided for reference only and the author makes no guarantee as to their accuracy or reliability.

CONSIDER THE FOLLOWING FACT PATTERN

- Employee is in sales for a tech company serving the financial industry
- Employee has a signed non-disclosure agreement ("NDA")
- Employee leaves the company voluntarily to work for another company in the financial industry (not a competitor)
- Employee, prior to leaving, uses a USB drive to download the entire CRM (customer relationship management) database

CSG
Chiesa Shahinian & Giantomasi PC

THE EMPLOYEE'S NDA….

- Employee was "**contractually bound not to "…make use of, or disclose… to any third party, any Confidential Information … [and] not to "remove any Confidential Information…. or make copies of any Confidential Information…." without the employer's consent.**
- Further, upon termination of the employment for any reason, the employee was contractually required to deliver to the Company "**all…electronic files, computer programs… customer lists… and all other materials containing Confidential Information, and all copies thereof**…"

IN THE DEMAND LETTER…

In addition to citing to the NDA (and the resulting breach of contract by the employee's actions), we cited to the **Computer Fraud and Abuse Act.**

CONSIDER ANOTHER FACT PATTERN

- Employee is on disability leave
- Employee has a company laptop, and access to the company Drop-Box account
- Employee's "activities" while on disability make clear that employee is abusing disability
- One hour before employee's telephone termination call (in theory, employee did not know purpose of call), employee asks to push the call back by 1 hour
- Prior to, and throughout the termination call, the employee proceeds to download and delete 27,000 files from the company's Drop-Box account

CSG
Chiesa Shahinian & Giantomasi PC

No NDA….

But, with the help of Drop-Box and computer forensic experts we were able to document theft and deletion of company trade secrets, proposals, contracts, work product and other company confidential information.

- Theft began at 10:00am on the day of termination (while employee was still employed)
- Termination notice was given at 10:34am
- Theft continued through at least 11:00am

In demand letter, we asserted that the employee's "***unauthorized use***" of a Company issued computer to access, download and then delete Company trade secrets and other confidential and proprietary information gave rise to an action under the **Computer Fraud and Abuse Act,** as well as other State and Federal Laws.

SO, WHY IS THE COMPUTER FRAUD AND ABUSE ACT (18 U.S.C. 1030) SUCH A POWERFUL TOOL FOR EMPLOYERS (IF YOU ARE IN THE RIGHT CIRCUIT)?

(a) Whoever….

(2) intentionally accesses a computer ***without authorization or exceeds authorized access***, and thereby obtains—**….**

(C) information from any ***protected computer***; or

(5)

(B) ***intentionally*** accesses a protected computer ***without authorization***, and as a result of such conduct, causes damage and loss…

shall be punished as provided in subsection (c) of this Section.

SUBSECTION (C) PROVIDES….

.....A person who violates Section (a)(2) may be subject to a fine or imprisonment of not more than one year, or both… (Section (c)(2)(A))… however

- Under the following subclause, the prison term could be as long as five years if
- " **(i)**the offense was committed for purposes of commercial advantage or private financial gain;… or….
- **(iii)**the value of the information obtained exceeds $5,000…"

AS TO A VIOLATION OF SECTION (a)(5)(B)

A fine and imprisonment for not more than five years, or both if….

(I) loss to 1 or more persons during any 1-year period … aggregating at least $5,000 in value;….

(VI) damage affecting 10 or more protected computers during any 1-year period…

DEFINITION OF "EXCEEDS" AUTHORIZED ACCESS:

- **(6)**the term "***exceeds authorized access***" means 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 so to obtain or alter***;

AND FOR EMPLOYERS… THERE IS….

Section (g)
Any person who suffers damage or loss by reason of a violation of this section *may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.* A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses [5] (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages.

While we wait for the Supreme Court to Render its Decision, let's look at the current Interpretation and Why this is even an issue.

- **A broad interpretation from**:

  The First Circuit:

  EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581 (1st Cir. 2001)

  The First Circuit held that the use of a scraper software program to systematically and rapidly glean prices from a company's website in order ***to allow systematic undercutting of those prices*** "exceeded authorized access" within the meaning of the CFAA.

  The Court, in finding for the former employer, pointed to an all-encompassing confidentiality agreement, signed by the former EF employee, which prohibited the defendant from disclosing information considered contrary to his former employer's interests. Id. at 582-84.

VAN BUREN – THE ELEVENTH CIRCUIT:

The Eleventh Circuit ruled that 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 accessor is not entitled [so] to obtain or alter***." 940 F.3d 1192, 1207 (11th Cir. 2019), cert. granted, 206 L. Ed. 2d 822 (Apr. 20, 2020).

"exceeded his authorized access and violated the [computer-fraud statute]" Van Buren was found to have "exceeded his authorized access" when he used the Police Department systems to obtain what he thought was an exotic dancer's personal information for a nonbusiness reason. Id.

In reaching its ruling, the eleventh Circuit rejected….

- The Court expressly rejected defendant's argument that he was innocent of computer fraud and did not exceed his authorized access **because he accessed only databases that he was authorized to use, even though he did so for reasons wholly outside the scope of his duties**. Id.

Narrow Readings and the Concern before the Supreme Court

- The Ninth Circuit:
- hiQ Labs, Inc. v. LinkedIn Corp. The Court, referring to the rule of lenity, imposted a narrow interpretation of "***without authorization***" in the CFAA. 938 F.3d 985, 1003 (9th Cir. 2019).
- The Court observed that the "CFAA's prohibition on accessing a computer 'without authorization' is violated when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer." Id.

AND IN 2012….

- United States v. Nosal (also Ninth Circuit): The Court limited the interpretation of "exceeds authorized access" to violations of ***restrictions on access to information, and not restrictions on the information's use – or misuse***. 676 F.3d 854, 863–64 (9th Cir. 2012).
- WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 205-06 (4th Cir. 2012): The Court ruled that a departing employee ***did not exceed authorized access*** by downloading confidential information to a personal computer in violation of company policy because ***the employee was authorized to review the material in question***.
  - Remember the fact pattern with which we started our discussion?
  - And query how our second fact pattern would be viewed….

SO, WITHOUT OUR CRYSTAL BALLS OUT… HOW DO WE COUNSEL OUR CLIENTS?

- Uniform Trade Secrets Act (USTA) (more than 47 States and the District of Columbia have adopted the USTA

  A trade secret is defined as "information, including a formula, pattern, compilation, program, device, method, technique, or process that:

  - Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and
  - Is the *subject of efforts that are reasonable under the circumstances to maintain its secrecy.*

Think Coca-Cola formula

Basis for a Trade Secret Claim:

- The information at issue is a “trade secret”
- The employer (or whomoever holds the trade secret) has taken “reasonable” precautions to prevent disclosure
- And, the employer must show that the trade secret was misappropriated or wrongfully taken

For California employers, this is a particularly important tool given that NDAs that include a non-compete are generally unenforceable.

CRIMINAL PROSECUTION

- Jean Patrice Delia and General Electric Company (2017)
- Tesla employee steals autopilot source code and took them to Chinese start up (2019)
- Oklahoma oil and gas company controller charged in 35-count indictment for trade secrets theft to competing company

CSG
Chiesa Shahinian & Giantomasi PC

NEW JERSEY TRADE SECRETS ACT

For the purposes of "**exceed authorized access**," the NJTSA expands on the UTSA's definition of "improper means" by adding that it is improper to obtain a trade secret by using: (1) unauthorized access; (2) access that exceeds the scope of authorization; and (3) other means violating a person's rights under New Jersey law. N.J.S.A. 56:15-2.

New Jersey Computer Related Offenses Act

Prohibits a person from purposefully or knowingly without authorization "altering, damaging, taking, or destroying any data, database, computer program, computer software, internal or external computer equipment, computer system, or computer network. N.J.S.A. 2A:38A-3.

So…. What "reasonable precautions" can and should employers take?

- "Least rights" access controls
  - Changes in roles
  - Should all employees have the same access?
- "Acceptable use" policies
- Proscribe
  - the exfiltration, duplication and/or removal of any confidential information with any removable media (such as a USB drive);
  - the transfer of any company information to a personal cloud account or personal hard drive.

CONSIDER PUTTING EMPLOYEES ON NOTICE WHEN THEY LOG IN:

"This computer system is operated by…… and may be accessed only by authorized users. Authorized users are granted specific, limited privileges in the use of the system. The data and programs in this system may not be accessed, copies, modified or disclosed without prior approval of….Access and use, or causing access and use, of this computer system by anyone other than as permitted by…. are strictly prohibited…."

From an exhibit presented in an unreported decision from the NJ Superior Court, Law Division in 2015. Courtesy of Kerry Brian Flowers, Esq., Flowers & O'Brien, LLC

CSG
Chiesa Shahinian & Giantomasi PC

CONSIDER REQUIRING ACCEPTANCE…

The files you are about to review contain confidential information regarding ……. clients….. Each time you log in, you agree: ·

- To keep all information you view strictly confidential ·
- Not to download these files to any other device or environment whatsoever ·
- Not to print these files ·
- Not to take picture of any images you view

- ***Please click here to confirm your agreement with the foregoing and to access the files.***

CSG
Chiesa Shahinian & Giantomasi PC

WHETHER A COMPANY OR PERSONAL DEVICE IS USED

- Consider mobile device management (MDM) technology
- Deploy technology and monitoring systems to detect large downloads of company data or other unusual online or system behavior
  - With a remote work force, what was “unusual” before may not be so now….

CSG
Chiesa Shahinian & Giantomasi PC

EMPLOYEES ON DISABILITY/PRIOR TO TERMINATION

- Suspend access
- Modify access
- Terminate access

Managing Disgruntled, Departing and Terminated employees

- Managing company issued devices
- Managing access credentials
- Managing social media accounts

An employee handbook is Not (necessarily) enough…. Breach of Contract Claims…

NDAs

- Definitions matter - Confidential information" should include an entity's systems and access credentials in addition to the other traditional information protected by such agreements (trade secrets, customer lists, etc.).
- Jurisdiction matters – especially if the NDA includes a non-compete
- Consider social media accounts
- Require return of confidential information
- Require delivery of all personal devices used to access any confidential information to ensure the permanent removal of that information from such devices.
  - BYOD vs company issued devices….

REMEMBER, NOT ALL THEFTS ARE FOR THE EMPLOYEES THEMSELVES

- Trade secret theft on behalf of …
  - foreign countries
  - competitors
- When considering contracts, restrict client's access credentials
  - "…Customer shall use all reasonable measures to protect the confidentiality of…… our proprietary database…. All uses of the portal to access the database through customer's account credentials to access the same shall be deemed as used by customer, for which customer shall be primarily responsible…."

ALSO REMEMBER THAT IT IS NOT JUST YOUR COMPANY DATA AT RISK….

- If compromised data includes:
  - PII: potentially reportable data breach
    - Consider what your CRM system contains
    - What do your project files contain?
  - PHI: depending on your business, a reporting obligation under HIPAA and a potential HIPAA violation
    - Are you a business associate of a healthcare provider?
  - Your clients':
    - Confidential information
    - Personnel's PII

"The risk of negligent employees and contractors causing a data breach or ransomware is getting worse. **Sixty percent** of respondents in companies that had a data breach say the **root cause of the data breach was a negligent employee or contractor,** …. **Sixty-one** percent of respondents say **negligent employees put their company at risk for a ransomware attack…**

https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf

The **2020 Insider Threat Report** [PDF] by Cybersecurity Insiders states that 68% of organizations feel moderately to extremely vulnerable to insider attacks.

Victims: Shopify (customer transactions and PII stolen)

Amazon (insider trading)
Twitter: user accounts compromised

And these are companies that invest significant resources into security measures….

WHAT IS YOUR RISK IF YOU DO NOT TAKE "REASONABLE" PRECAUTIONS AGAINST EMPLOYEE DATA THEFT?

- 50 different states have 50 different breach notification laws
- More than 25 states have some form of proactive legislation which requires businesses to take "reasonable measures" to secure data
  - NY SHIELD Act
  - CCPA
  - Reputation
- Sectoral mandates (HIPAA, GLBA)
- GDPR
- Common law duty to take reasonable measures to prevent a "foreseeable risk"

➢ ***All of these laws and regulations impose fines for failure to act "reasonably"***

AS OF THE DAY OF THIS PRESENTATION, WE STILL DO NOT KNOW THE FATE OF THE CFAA

- But we can still offer our clients guidance as to how to protect the crown jewels, and understand the risks if they do not!

Questions?

THANK YOU

Michelle A. Schaap

Member
Chiesa Shahinian & Giantomasi PC
973.530.2026
mschaap@csglaw.com

