PROGRAM MATERIALS
Program #3077
May 20, 2020

# The Shield Act: Are You Compliant?

Copyright ©2020 by Nick Akerman, Esq.- Dorsey & Whitney LLP. All Rights Reserved.
Licensed to Celesq®, Inc.

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

# THE NEW YORK SHIELD ACT

**Nick Akerman**

© 2020 Dorsey & Whitney LLP. All rights reserved.

# Stop Hacks and Improve Electronic Security Act

- **Effective March 20, 2020**
- **Relates to personal data as opposed to competitively sensitive data**
- **Reflects strong trend of mandating a proactive approach to cybersecurity**
- **Government regulation started out requiring businesses to react to a data breach**
- **Started in 2003 when California required notification to consumers if there was reason to believe there was a data breach of personal data**
- **Trend is requiring proactive protection of data to prevent a breach**

# What We Will Cover Today

- **Explain what the Shield Act requires of businesses maintaining personal data belonging to New York residents**
- **What you need to do if you have a data breach that includes data belonging to a New York resident**
- **What proactive measures are required to prevent a breach**
- **What penalties can be imposed for not complying with the law**
- **How you can respond to this law by instituting a data compliance program that can protect both personal data and the company's competitively sensitive data**

# New Requirements on Responding to Data Breaches

- **Expands the definition of personal data beyond the traditional information such as social security numbers and banking and credit card numbers in combination with the person's name**
- **Now includes biometric information including an individual's unique physical characteristics such as fingerprint, voice print or retina image**
- **A user name or email address in combination with a password or security question that would permit access to an on-line account**
- **Definition of a data breach is expanded to includes instances where the attacker merely views personal information as opposed to downloading or stealing the actual data**

# Requirement of a Data Compliance Program

- **Any business that has personal data belonging to a New York resident must “develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private” data**
- **There is no requirement that the business conduct business in NY**
- **The Statute sets out the benchmark requirements of a data security program**

# Must Meet Reasonable Administrative Safeguards

- **Designate at least one “employee to coordinate the security program”**
- **Identify “reasonably foreseeable internal and external risks”**
- **Assess “the sufficiency of safeguards in place to control the risks”**
- **Train and manage “employees in the security program practices and procedures”**
- **Select service providers capable of maintaining appropriate safeguards, and require those safeguards by contract**
- **Adjust “the security program in light of business changes or new circumstances”**


DORSEY™ always ahead

# Must Meet Reasonable Technical Safeguards


- **Assess “risks in network and software design”**
- **Assess “risks in information processing, transmission and storage”**
- **Detect, prevent and respond “to attacks or system failures; and”**
- **Regularly test and monitor “the effectiveness of key controls, systems and procedures”**

# Must Meet Reasonable Physical Safeguards

- **Assess “risks of information storage and disposal”**
- **Detect, prevent and respond “to intrusions”**
- **Protect “against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information”**
- **Dispose “of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed”**

DORSEY™
always ahead

# The Statute Accounts for Small Businesses


- **Small business is defined as having a) “fewer than fifty employees, b) “less than $3 million in gross annual revenue or less than $5 million in year-end total assets”**
- **Small businesses are deemed to have complied with the statute if its “security program contains reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of the small business’s activities, and the sensitivity of the personal information the small business collects from or about consumers.”**

# Enforcement and Penalties

- **Enforced by the New York Attorney General**
- **No private right of action**
- **The NY AG can bring an action against any person or business that fails to comply with the data security requirements to enjoin violations and obtain civil penalties, regardless of whether there is a breach**
- **Authorized courts to award actual damages to consumers**
- **Raises maximum penalty for failure to provide notice from $150,000 to $250,000**
- **A statutory penalty of the greater of $5,000 or $20 per instance of failure to notify**

# Data Compliance Program

- **Incorporate the protection of personal data and competitively sensitive data into an existing compliance program or create a data compliance program**

- **Seven steps to effective compliance**
  1. **Develop standards and procedures**
  2. **Assign a person with overall responsibility**
  3. **Take care not to assign someone who might pose a risk**
  4. **Communicate standards and procedures**
  5. **Regular Audits**
  6. **Consistently enforce the policies**
  7. **Mechanism in place to respond to violations**

# Cybersecurity Is Not Just IT Security

- **Multi-dimensional Problem**
- **Human Resources**
- **Legal**
- **Risk Management**
- **Compliance**
- **IT Security**
- **Corporate Security**

# Companies Can Mitigate "Risk" by Re-Evaluating 7 Areas of Their Business


- Hiring Practices
- Company Rules
- Employee training
- Appropriate Agreements
- Use of Technology
- Termination Practices
- Protocols for Response

# The Hiring Process

- **Honor Prior Employment Agreements**
- **Explain Company Obligations**
  - **Company Policy**
  - **Employment Agreements**
- **Civil and Criminal Exposure based on competitor's data**

# Company Rules

- **Code of Conduct**
- **Employee handbook**
- **Rules on computer screens**
- **Terms of Use on company website**
- **Rules in various documents must be consistent**

# Computer Fraud and Abuse Act

- **Title 18 U.S.C. § 1030 – Enacted in 1984**
- **Federal computer crime statute including data theft**
- **Civil remedy in 1994 amendment**
- **Computers used in interstate commerce**
- **Amended in 2001 and 2008**
- **Computers in foreign countries**
- **Provides for damages and injunction**

DORSEY™ always ahead

# Violations Based on Unauthorized Access

- **First Circuit: the CFAA "is primarily a statute imposing limits on access and enhancing control by information providers"**
- **Companies can set predicate for CFAA violation**
- **Rules on limiting authorized access**
- **Agreements can set limits**
- **Similar to criminal trespass**

# Supreme Court Granted Cert

- **The Court will resolve the division among the Circuit Courts as to whether the CFAA applies to employees**
- **CFAA requires the perpetrator to have accessed the computer "without authorization" or to have accessed the computer in a manner that "exceeds authorized access."**
- **First, Fifth, Seventh and Eleventh Circuits apply the CFAA to employees**
- **Second, Fourth and Ninth Circuits do not apply the CFAA to employees**
- **The case before the Court is *United States v. Van Buren,* 940 F.3d 1192 (11th Cir. 2019)**
- **Now is the time to review computer policies to take full advantage of a Supreme Court ruling affirming *Van Buren*.**

# Employee Training

- **Part of onboarding process**
- **Review of rules**
- **Periodic**
- **Update new risks**
- **Encourage reporting**

# Agreements

- Top to bottom
- Incorporate computer policies
- Agreement to search personal computers
- Permissions re scope of access
- Confidentiality/Non-Disclosure
- Post employment restrictive covenants
- Anti-Raiding Covenants

# Economic Espionage Act

- **Federal criminal statute outlawing the theft and use of trade secrets**
- **Civil provision signed into law in May 2016**
- **Permits civil action for misappropriation and use of trade secrets**
- **Traditionally state court action unless diversity jurisdiction**
- **Provides for Seizure Order and double damages**
- **Amend your employment agreement and/or policies to include whistleblower immunity**

# Protocols for Response:  The Investigation

- Certain states require for breach of personal information
- Need to know facts to properly respond
- Use of outside forensic experts
- Must be immediate
- Gather admissible evidence
- Legal guidance on investigative techniques
- Investigative and response team in place
- Workplace rules in place to facilitate investigation

# Use of Technology to Protect Data

- **Password protection is simplest**
- **Two step verification**
- **Encryption**
- **Intrusion software**
- **Establish authorized access**
- **Access based on need to know**
- **Risks re transportable media**

# The Termination Process

- **Employees must return all company property**
- **Standard Exit Interview Form**
- **Explain post employment obligations**
- **Retain evidence**

**Nick Akerman**
**Akerman.Nick@Dorsey.com**

**212-415-9217**

**Follow on Twitter: twitter.com/nickakerman**

**For On-going Updates Go to**
**http://computerfraud.us**

THE NATIONAL LAW JOURNAL
APRIL 18, 2016
An ALM Publication
THE PRACTICE | Commentary and advice on developments in the law

# Cybersecurity Compliance Just Got Tougher

Companies need specific, well-executed plans to meet growing demands of federal and state agencies.

BY NICK AKERMAN AND DAN GOLDBERGER

KIRILL_SAVENKO/ISTOCKPHOTO.COM

While cybersecurity risks have increased, government regulation has traditionally lagged behind. Recently, some government entities have tried to catch up by mandating that companies take a proactive approach toward protecting personal and competitively sensitive data. The move is a departure from the traditional reactive response of simply notifying consumers after their personal data is breached.

With this shift in emphasis, companies are asking the obvious questions: "What are we expected to do and what is a proactive cybersecurity compliance program?"

Both on the state level and through federal regulatory agencies, the government is beginning to dictate a comprehensive compliance approach to data protection. Late last year, the U.S. Securities and Exchange Commission's Cybersecurity Examination Initiative directed broker-dealers to "further assess cybersecurity preparedness in the securities industry." Thus, the SEC announced that it "will focus on key topics including governance and risk assessment, access rights and controls, data loss prevention, vendor management, training and incident response."

In January, the Financial Industry Regulator Authority announced that in reviewing a securities firm's approaches to cybersecurity risk management its examinations may include "governance, risk assessment, technical controls, incident response, vendor management, data loss prevention and staff training." On the state level, Massachusetts is the only state thus far to require all businesses that store personal data of its residents to secure that data through a compliance program modeled after the federal sentencing guidelines.

The framework under the federal sentencing guidelines is the gold standard for an effective compliance program. Having expanded well beyond its original goal of detecting and preventing criminal activities, it is fast becoming the corporate framework to protect data. These guidelines establish seven steps for companies to follow: first, promulgate standards and procedures; second, establish high-level corporate oversight including the board of directors that

must provide adequate funding of the program in proportion to the size of the company and the risk; third, place responsibility with individuals who do not pose a risk for unethical behavior; fourth, communicate the program to the entire workforce; fifth, conduct periodic audits of the effectiveness of the program; sixth consistently enforce the polices; seventh establish mechanisms for reporting violations.

## COLLABORATION IS CRITICAL

Because a compliance program must be tailored to an organization's culture, it is critical to its success that all data-protection stakeholders collaborate in its creation and daily operation. This means that data compliance is not just an issue for information-technology security. Other stakeholders include human resources and legal, which are responsible for company rules, employee agreements and training, and may assist in responding to company data breaches; risk management, which may determine, along with legal, the adequacy of the company's cyber insurance; and compliance, which is often the logical focus of the company's data protection efforts.

Stakeholders in turn should focus on six areas of risk when developing a company-specific compliance program to minimize the risks posed by each area.

First, hiring is the time to explain to new employees the rules in place to protect the company's data. Additionally, companies must approach hiring defensively, ensuring new employees do not bring into the workplace data that belongs to a competitor that can result in civil or criminal liability.

Second, company rules and policies should spell out what employees can and cannot do with the company network and form the foundation of top-to-bottom workforce training. At least one court has recognized that such "explicit policies are nothing but security measures employers may implement to prevent individuals from doing things in an improper manner on the employer's computer systems." (*American Furukawa v. Hossain*).

Third, agreements with employees and other third parties are a key component of data protection. Employee agreements are an opportunity to reinforce the lack of an expectation of privacy in using company computers and define the scope of authorized access. When company data is outsourced to a cloud provider, agreements formalize the responsibilities of that third party to protect the company's data.

Fourth, technology can be employed not only to secure data but to define who is authorized to access what portion of the network and provide admissible evidence of a breach. Information-technology security, working with legal, can prepare mechanisms to capture audit trails in the network that can be used to identify the source and scope of a breach.

Fifth, effective termination procedures are critical. This is when insiders are most likely to steal company data to use at their next job. This is also the last opportunity to remind departing employees of their postemployment obligations to maintain the secrecy of company data, to return all company data and for the company to inventory the data returned.

Finally, if a breach occurs, it is important to have protocols in place to quickly determine the scope of the breach and the appropriate response. Companies must therefore have in place an overarching plan to investigate suspected breaches and to mobilize internal and external resources.

For a data-compliance program to work consistently, it must be a collaborative effort among all stakeholders and comprehensively focus on mitigating the risks to the company's data from multiple and unexpected sources.


**NICK AKERMAN** *and* **DAN GOLDBERGER** *are partners in the New York office of Dorsey & Whitney. Akerman's practice focuses on the Computer Fraud and Abuse Act and the Racketeer Influenced and Corrupt Organizations Act. Goldberger's practice focuses on financial services, intellectual property, trade secrets and data protection.*

Reprinted with permission from the April 18, 2016 edition of THE NATIONAL LAW JOURNAL © 2016 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382, reprints@alm.com or visit www.almreprints.com. #005-04-16-11

DORSEY
DORSEY & WHITNEY LLP

PUBLICATIONS

# Time to Re-examine Corporate Computer Access Policies

April 27, 2020

Last week the U.S. Supreme Court agreed to hear an appeal from a defendant who had been convicted of a felony charge under the Computer Fraud and Abuse Act ("CFAA"), the federal computer crime statute. Title 18, U.S.C. § 1030. The Supreme Court will resolve the issue of whether the CFAA applies to employees who use their authorized access to employers' computer systems to misuse those systems, including to steal data. The courts of appeals have been divided on this question for the past 8 years. It is an issue of high significance to business because this statute allows individuals or companies victimized by violations of the CFAA to bring a civil action against perpetrators for damages and injunctive relief. Title 18, U.S.C. § 1030(g). This alert will explain the scope of the issue before the Supreme Court and what the ultimate Supreme Court decision may mean for protecting company data.

The appeal to the Supreme Court is from the 11th Circuit in the case of *United States v. Van Buren*, 940 F.3d 1192 (11th Cir. 2019). Nathan Van Buren, a sergeant with the Cumming, Georgia Police Department was charged with violating the CFAA for exceeding authorized access to a police database. Title 18, U.S.C., § 1030(c)(2). A government informant paid Van Buren to search a police database to determine if a "woman he [the informant] liked at a strip club" was an undercover cop. Van Buren later admitted to the FBI that "he knew" conducting the search "was 'wrong'" and that his "purpose" in searching the database was not a proper police function. The evidence at trial showed that "the database is supposed to be used for law enforcement purposes only and the officers are trained on the proper and improper uses of the system." The 11th Circuit affirmed the conviction on the basis that Van Buren had exceeded his authorized access to the police database.

The crux of what the Supreme Court will decide revolves around the CFAA's language that requires the perpetrator to have accessed the computer "without authorization" or in a manner that "exceeds authorized access." The phrase "without authorization" has been uniformly interpreted by the courts to mean "without permission." "Exceeds authorized access" is defined by the CFAA to mean "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." The conflict among the circuit courts centers on what it means for an employee or corporate insider to "exceed[] authorized access" to company computers. The 1st, 5th, 7th, and 11th Circuits take the view that using the computer for an improper purpose prohibited by the employer's policies exceeds authorized access and is a violation of the CFAA.

In *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001), the 1st Circuit concluded that a person "exceeds authorized access" when he uses information for purposes prohibited by a

confidentiality agreement. The defendant there had "authorization . . . to navigate around EF's public website," *id*. at 583, but in the First Circuit's view, he "exceeded that authorization" by his "wholesale use" of "proprietary information and know-how" to collect data from the website to aid a competitor's strategy. *Id*. at 582-83.

The 5th Circuit in *U.S. v. John*, 597 F.3d 263, 269, 272 (5th Cir. 2010), held that a Citigroup account manager, who accessed Citigroup's internal computer system to provide her brother with customer account information that he used to make fraudulent charges on those accounts, had exceeded authorized access based on "Citigroup's official policy, that . . . prohibited misuse of the company's internal computer systems and confidential customer information."

The 11th Circuit, which decided the *Van Buren* case now before the Supreme Court, also relied on internal organization rules in *U.S. v. Rodriguez*, 628 F.3d 1258, 1260, 1263-64 (11th Cir. 2010), to affirm the CFAA conviction of a Social Security Administration employee who accessed Social Security information for personal reasons in violation of the agency's policy against "obtaining information from its databases without a business reason."

The 7th Circuit's holding in *Int'l Airport Ctrs. LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006), is even broader and does not rely exclusively on an employer's policy to define unauthorized access. *Citrin* held that "when an employee accesses a computer or information on a computer to further interests that are adverse to his employer, he violates his duty of loyalty, thereby terminating his agency relationship and losing any authority he has to access the computer or any information on it."

In contrast, the 2nd, 4th, and 9th Circuit Courts of Appeals have each held that the CFAA's "exceeds authorized access" prong does not impose criminal liability on a person with permission to access information on a computer who accesses that information for an improper purpose. A person violates the CFAA in those

circuits only if he accesses data on a computer that he is prohibited from using at all, for any reason. *United States v. Nosal*, 676 F.3d 854, 862-63 (9th Cir. 2012) (*en banc*). *Nosal* reasoned that the text of Section 1030(a)(2) does not cover a person "who has unrestricted physical access to a computer but is limited in the use to which he can put the information." *Id*. at 857, 862-63. *Nosal* interpreted "exceeds authorization" to "refer to data or files on a computer that one is not authorized to access," *id*. at 857, as opposed to accessing data for an improper purpose prohibited by the employer. An example would be "an employee may be authorized to access customer lists in order to do his job but not to send them to a competitor." *Id*. Thus, as long as an employee is permitted blanket access to a company's computers, the CFAA does not prohibit an employee from accessing any data on that computer for any purpose, even if improper or contrary to the interests of his employer.

The 4th Circuit agreed with this reasoning in *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 202, 207 (4th Cir. 2012), and the 2nd Circuit followed suit in *United States v. Valle*, 807 F.3d 508 (2d Cir. 2015).

A major factor motivating these courts is a concern that reading the CFAA to cover "use restrictions" would reach activities "routinely prohibited by many computer-use policies" and would improperly turn "millions of ordinary citizens" into criminals, *Nosal*, 676 F.3d at 857-63, and that "such a rule would mean that any employee who checked the latest Facebook posting or sporting event scores in contravention of his employer's use policy" would be guilty of a crime. *WEC Carolina Energy Solutions, LLC*, 687 F.3d at 206.

Our best prognostication is that the Supreme Court will affirm the 11th Circuit and side with those circuits holding that "exceeds authorized access" applies to employees violating company rules and their duty of loyalty to their employers. The common sense

reading of the CFAA on its face seems unambiguous — "exceeds authorized access" means that even though an employee has access to a company's computers, the employee's access can be limited by company rules and the common law governing the loyalty that an employee owes to an employer, and that when the employee violates those rules, the employee "exceeds authorized access."

The argument that the CFAA can criminalize minor violations of an employer's use policies goes to prosecutorial discretion. This is precisely the same argument that has been leveled at the federal mail and wire fraud statutes because they could be used to prosecute individuals for stealing paltry sums of money through the wires or mails under circumstances that should not be prosecuted, yet the courts have consistently upheld both statutes.

The Supreme Court's interpretation of the mail and wire fraud statutes also argues in favor of the 7th Circuit's holding that an employee's authorization terminates when the employee commits a disloyal act like stealing data for a competitor, thereby terminating his agency relationship with the employer. *Carpenter v. U.S.*, 484 U.S. 19 (1987), relied on the same state law agency principles to uphold a "scheme to defraud," the key element of the mail and wire fraud statutes. *Carpenter* affirmed the conviction of a Wall Street Journal reporter who, prior to publication, had provided his upcoming financial columns to confederates, who bought or sold stock "based on the probable impact of the column on the market." *Id*. at 23. The Supreme Court held that "an employee has a fiduciary obligation to protect confidential information obtained during the course of his employment," and intentionally exploiting that information for his own personal benefit constituted a scheme to defraud his employer of confidential information. *Id*. at 29. The same employee duty should apply to the meaning of "authorized access" under the CFAA.

Given that the Supreme Court may affirm the 11th Circuit and give renewed national breadth to the CFAA, it is an opportune time for all businesses to re-examine their computer policies to determine whether they are in a position to take full advantage of the CFAA to retrieve stolen data from disloyal employees. As the 1st Circuit explained in *EF Cultural Travel*, 318 F.3d at 63, the CFAA "is primarily a statute imposing limits on access and enhancing control by information providers." Thus, a company "can easily spell out explicitly what is forbidden" through its policies and use those policies to take action against those employees who violate those policies by stealing and/or misusing company data. And, as the FBI reminded us in an April 23, 2019 notification to private industry, all companies face a regular threat to their data from insider employees. *See* https://bit.ly/3bGD1Ux.

## RELATED INDUSTRIES & PRACTICES

Cybersecurity, Privacy & Social Media

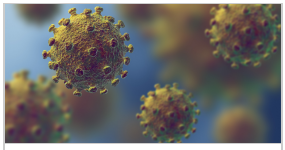
Government Enforcement & Corporate Investigations

Securities & Financial Services Litigation & Enforcement

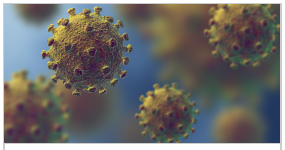
Nick Akerman
Partner

Joshua Colangelo-Bryan
Of Counsel

## featured resources



CLIENT



CLIENT

EVENTS

ALERTS/EUPDATES/ALERTS

## Global Pandemic Raises Importance of Privacy and Security Compliance as California Attorney General's Office Signals No Delay on CCPA Enforcement

April 10, 2020

ALERTS/EUPDATES/ALERTS

## FCC Narrows the TCPA's Emergency Purpose Exception Amid Pandemic While Greenlighting Certain Emergency Messages by Hospitals, Health Care Providers, and Government

March 23, 2020

*Western Alliance Bank and University of San Diego School of Law present CLASS ACTION LAW FORUM 2020*

March 4-5, 2020

Directions >