VIRGINIA
EMPLOYMENT LAW LETTER
Part of your Virginia Employment Law Service

April 2017

How to protect against and respond to cyberattacks, part 2

by Milton Whitfield and Jayna Genti
DimuroGinsberg PC

Last month, we reported on the costs of data breaches and steps you can take to help prevent what has become a very common occurrence at businesses and organizations across the country. If a data breach occurs at your organization, you need to be aware of Virginia laws that require you to undertake a number of steps to mitigate the potential harm to any individuals who may be affected.

States act to protect individuals against identity theft

Virginia, along with 46 other states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, has enacted legislation requiring private-sector, governmental, and educational entities to notify individuals when there are data security breaches involving personally identifiable information. These security breach laws typically include provisions addressing:

- Who must comply with the law (e.g., businesses, data/information brokers, and governmental entities);
- What is considered "personal information" (e.g., a person's name combined with his Social Security number (SSN), driver's license, or state ID; financial account numbers);
- What constitutes a breach (e.g., unauthorized acquisition of data);
- What's required with regard to notice (e.g., who must be notified and the timing or method of notice); and
- What is exempt (e.g., encrypted information).

Virginia's security breach notification laws include Virginia Code § 18.2-186.6 (breach of personal information), § 32.1-127.1:05 (breach of medical information), and § 22.1-20.2 (student data security). Some of the key aspects of these Virginia laws that employers should understand are set out below.

Virginia's security breach notification laws

Who is subject to Virginia's laws? The data breach laws apply to any individual, legal, or commercial entity that owns or licenses computerized data that include personal information and any organization supported by public funds that owns or licenses computerized data that include medical information of a resident of the Commonwealth.

What constitutes "personal information"? Virginia's data breach laws protect the personal and medical information of Virginia residents. "Personal information" means the first name or first initial and last name in combination with and linked to one or more of the following types of information belonging to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:

- SSN;
- Driver's license number or state ID card number issued in lieu of a driver's license number; or
- Financial account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a person's financial accounts.

What is "medical information"? "Medical information" means the first name or first initial and last name in combination with and linked to one or more of the following types of information belonging to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:

- Any information about an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional; or
- An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals.

What is a "security breach"? A "breach of the security of the system" means the unauthorized access and acquisition of your unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained as part of your database of personal information and that causes, or you believe has caused or will cause, identity theft or other fraud affecting any resident of the Commonwealth.

Are there any exceptions? A breach of the security of your system doesn't include the good-faith acquisition of personal information by your employees or agents if the personal information isn't used for an unlawful purpose or subject to further unauthorized disclosure.

What is the "encryption safe harbor"? The unauthorized acquisition of your encrypted or redacted data, without access to the encryption key, doesn't trigger the notice requirement under the statutes. The safe harbor isn't available if personal information is encrypted but the encryption key is compromised.

What is "encryption"? "Encryption" means the transformation of data through the use of an algorithmic process into a form in which there's a low probability of assigning it meaning without using a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable.

When are your notification obligations triggered? If a security breach causes, or you reasonably believe it has caused or will cause, identity theft or other fraud affecting a Virginia resident, notification is required.

What are the notice procedures? You must provide written, telephonic, or electronic notice to victims of a security breach without unreasonable delay, unless the disclosure would impede a law enforcement investigation (in which case notification is delayed until it's authorized by the law enforcement agency). Notice to affected residents must contain specific information described in the statutes. You may provide substitute notice by means prescribed in the statute if your notification costs exceed $50,000, more than 100,000 people are affected, or you have insufficient contact information or do not have consent to provide notice by the primary means required by the statute.

What is "substitute notice"? Substitute notice includes all of the following:

- E-mail notice if you have e-mail addresses for the affected residents;
- Conspicuous posting of the notice on your website; and
- Notice to major statewide media.

When must you notify the AG and consumer reporting agencies? You also must provide notice to the Office of the Virginia Attorney General (AG) without unreasonable delay. If you are required to notify more than 1,000 persons of a security breach at one time, you are also required to notify consumer reporting agencies without unreasonable delay.

What are your third-party notice requirements? If you maintain computerized data that include personal information you don't own or license, you must notify the owner or licensee of any security breach without unreasonable delay following your discovery of the breach.

Are there other exemptions? You are considered to be in compliance with Virginia law if:

- You maintain and comply with your own notification procedures as part of an

information security policy and those procedures are consistent with the timing requirements of the Virginia data breach statutes;
- You comply with the notification requirements or procedures imposed by your primary or functional state or federal regulator; or
- You are subject to, and in compliance with, federal requirements under Title V of the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), or the Health Breach Notification Rule promulgated by the Federal Trade Commission (FTC).

How does Virginia enforce its notification laws? The AG may bring a lawsuit and impose a civil penalty not to exceed $150,000 for a security breach or a series of breaches of a similar nature that are discovered in a single investigation. Individuals may bring an action to recover direct economic damages resulting from a violation of the Virginia data breach statutes. Violations by state-chartered or licensed financial institutions are redressed by the primary state regulator. Violations by insurance companies are redressed by Virginia's State Corporation Commission.

Are private lawsuits permitted? Although security breaches are generally enforced by the AG, nothing in Virginia's data breach notification statute precludes an individual whose personal or medical information has been compromised from bringing a lawsuit and seeking recovery of economic damages.

Bottom line

The specific steps that you must follow when your security is breached can be quite complicated, as this article confirms. Accordingly, if you experience a data breach, it's always wise to consult with legal counsel experienced in data breach laws. An experienced attorney can ensure that you are complying with all of your legal requirements. That's significant because, as our article next month will explain, you may have obligations under federal law as well as Virginia law.

Milton Whitfield and Jayna Genti are attorneys with DiMuroGinsberg PC and contributors to Virginia Employment Law Letter. They may be reached at mwhitfield@dimuro.com or jgenti@dimuro.com.