Tennessee Legislature imposes new data breach notification requirements on employers

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to

steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.

From: Tennessee Employment Law Letter | 08/01/2016
by Melody McAnally
by Melody McAnally

On July 1, 2016, important changes to Tennessee's data breach notification law went into effect. The changes concern all employers. The new law removes the encryption safe harbor, requires notice of employee data breaches, and changes when organizations must send notices to affected individuals. The law applies to all employers, regardless of size. Here's what you need to know.

What is a data breach?

A data breach is the unauthorized access of an individual's computerized "personal information." Personal information includes an individual's first name (or first initial) and last name plus one of the following: (1) full Social Security number (SSN), (2) driver's license number, or (3) financial account number or credit/debit card number with a security code, access code, or password. As of July 1, it no longer matters whether personal information is encrypted in a company's computer system, which is an important change. If encrypted personal information is accessed without authorization, you have a data breach under Tennessee law. Tennessee is the first state to require data breach notification regardless of whether personal information is encrypted.

Virtually every employer keeps at least employees' SSNs, and some employers keep driver's license numbers. How do you store personal information? If you store personal information on your computer system, you're at risk of a data breach. If you don't need to store your employees' full SSNs electronically, redact all but the last four digits. If you store credit card numbers, use software that automatically redacts the full numbers. Those are simple, inexpensive ways to protect your company from a data breach.

As of July 1, unauthorized access also includes an employee obtaining personal information and intentionally using it for an unlawful purpose. That means you must provide notification of a data breach that is the result of improper access by an employee if personal information is used for any reason outside the scope of his employment. Before the change, conventional wisdom stated that all employees were "authorized" to access personal information.

You can prevent employee data breaches by limiting which employees have computerized access to personal information. This is often called the "principle of least privilege." No employee should be given computerized access to personal information unless it is absolutely needed. Do employees outside your HR department need access to personal information? Probably not.

How does a data breach happen?

The most newsworthy way data breaches happen is when hackers secretly install malicious software (also known as malware) on a computer system, allowing them to access personal information. The bad guys want to steal your employees' personal information to create fraudulent credit card accounts or sell it on the "Dark Web" to other bad guys, who will in turn steal your employees' identity.

However, a data breach can also happen as a result of employee negligence (e.g., e-mailing personal information to the wrong e-mail address and faxing personal information to the wrong number) or the theft of

laptops or smartphones. Make sure you keep your inventory of laptops up to date.

What must you do if you have a data breach?

You must provide written notice of a data breach to Tennessee residents whose personal information was—or is reasonably believed to have been—acquired by an unauthorized person. The law requires you to provide notification of data breaches affecting Tennessee residents regardless of where your business is located. What matters is the state of residence of individuals whose personal information was breached.

If a data breach requires you to notify more than 500,000 individuals or providing notice will cost more than $250,000, you may give "substitute notice" by e-mail, a conspicuous posting on your website, and notification to major statewide media outlets. If a data breach requires you to notify more than 1,000 individuals at one time, you must notify the credit reporting agencies: Equifax, Experian, and Transunion. It's also best to report a data breach caused by theft to local law enforcement and a data breach caused by hackers to the U.S. Secret Service Electronic Crimes Task Force.

When is notice of a data breach required?

Another important change to Tennessee's data breach notification law is that written notice must be provided "immediately" but not later than 45 days after discovery of the breach. The only exception to the 45-day deadline is if a law enforcement agency asks you to wait for it to investigate the data breach. That almost never happens. If law enforcement does ask you to delay providing notice, get the request in writing.

The 45-day deadline means you must be ready now; don't wait until you discover a data breach to plan your response. Establish a data breach response team now. Evaluate which types of outside personnel you will need to help you respond to a data breach: outside counsel, IT and forensics professionals, and public relations professionals, to name a few. Make sure your IT team is involved in the employee termination procedure so computer access is taken away immediately before employees are fired.

A civil lawsuit may be filed if you fail to provide notification of a data breach within 45 days of discovering a breach. Any such lawsuit must be filed within two years. Tennessee's data breach notification law does not apply if you are subject to the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act.

Bottom line

It is important for employers to understand the laws governing data breach responses. Failing to comply with those laws can expose employers to significant damages. Not only should businesses invest in technology to prevent data breaches, but they should also respond swiftly and appropriately when a breach takes place. An ounce of prevention is worth a pound of cure.

Melody McAnally is an attorney in Butler Snow's Memphis office. She can be reached at melody.mcanally@butlersnow.com.