“[B]oards that choose to ignore, or minimize, the importance of cybersecurity responsibility do so at their own peril.”

SEC Commissioner Luis A. Aguilar, Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus, Speech at the New York Stock Exchange (June 10, 2014).

Data security and data privacy have been the hot topic in the business world for the last several years. With high profile data breaches impacting millions of customers across the globe, the business that hasn’t addressed the probability of not “if” but “when” the breach will occur has its head in the sand.

There are multiple issues this topic includes: the internet of things, storing data in the cloud, bring your own device (BYOD), privacy notices on websites and data tracking. Should a company counterattack a hacker? Will there be a federal law on data breach notification? All of those fascinating topics, and more, are beyond the scope of this paper. This paper will provide a primer on certain big picture issues for boards of directors.

Data security and data privacy issues are not the responsibility of only the information technology department. Various business functions, whether the business is large or small, need to be involved. These typically include IT, the board of directors, legal, human resources, public relations, the CFO and the Privacy Officer. In addition, outside resources should be utilized when a business is assessing its data security and data privacy needs. For example, a cyber-insurance carrier should be consulted to determine what type of coverage is appropriate and to ensure the coverage is sufficient. Outside legal counsel may be necessary if in-house legal is not well versed in data privacy matters. In addition, using outside counsel as soon as a breach occurs can assist in retaining the attorney-client privilege.

Prior to data breaches becoming a daily news event, some IT departments were having difficulty gaining buy-in from their board of directors regarding the importance of spending time and resources on data privacy and security. As the horror stories of the Target, Sony, Anthem, and Home Depot breaches, to name a few, became daily topics of conversation, management came to appreciate that it is no longer an anomaly to have a breach but something to anticipate and even expect.

If management needs additional encouragement to spend the time and resources on a good data privacy and security analysis, IBM and Ponemon Institute conduct an annual study on the cost of data breach incidents in the United States, which is always eye opening. According to the May 2014 study, the average cost of each lost or stolen record containing sensitive information was $201 per compromised record. The average total cost paid by organizations with a data breach
increased from $5.4 million to $5.9 million in 2014.\(^1\) Other interesting findings include the following:

- More customers terminated their relationship with a company that experienced a breach than in the prior year. Financial services industries are even more likely to have customers leave after a breach. “The average abnormal churn rate between 2013 and 2014 increased fifteen percent.”
- Malicious or criminal attacks rather than negligence or system glitches were the main causes of data breaches.
- The cost of lost business increased from $3.03 million to $3.2 million. Lost business costs include a higher than average loss of customers, increased customer acquisition activities, reputation losses and diminished goodwill.
- Malicious or criminal attacks cost more per record, at an average of $246 per record as opposed to an employee mistake, which costs an average of $161 per record.
- Business continuity management in remediation reduces the cost of a breach.
- Having a strong security posture or incident response plan in place prior to the incident reduces the cost of a breach by $17 to $21 per record.
- Some factors increase the cost of a data breach. For example, notifying customers too quickly before forensics are complete increased the cost by an average $15 per record.\(^2\)

One of the high profile breaches of the last few years was Target, which provides data privacy and security industry professionals with a number of valuable lessons. This paper will address a few of those lessons.

The Chief Executive Officer of Target resigned in May 2014.

During 2013 and 2014, Target spent a total of $252 million on the massive data breach it sustained in 2013. Even after receiving a total of $90 million in insurance proceeds, Target suffered a net total cost of approximately $162 million over those two years. Practice Point #1—buy adequate cyber insurance coverage relative to the size and scope of your business (as discussed more below).

On May 28, 2014, citing the data breach of November 2013, the proxy advisor Institutional Shareholder Services recommended Target replace seven of ten directors. ISS’s recommendation and (unsuccessful) efforts demonstrate that shareholders are paying ever closer attention to this area.

In addition, four derivative suits by shareholders have been filed, which assert that Target failed to take reasonable steps to maintain its customers’ personal and financial information in a secure manner. The cases have been consolidated and are pending in the United States District Court for the District of Minnesota. The consolidated complaint alleges claims for breach of fiduciary duties, waste of corporate assets, gross mismanagement, and abuse of control.\(^3\) Specifically, the

---


\(^2\) Ponemon Institute Report. Page 2

complaint alleges that the Target board of directors and other officers failed to implement any
internal controls designed to detect and prevent data breaches. In addition, the company
aggravated the damages not only by failing to timely provide notice to consumers but also by
making false statements that created a false sense of security for affected consumers. As a result,
the complaint asserts that the board of directors recklessly disregarded their duties to Target and
also breached their duties of loyalty and good faith.4 Practice Point #2—boards need to
demonstrate to their shareholders they are implementing adequate data protection procedures and
actively monitoring and updating those procedures if they want to avoid D&O suits and potential
liability.

As additional background, practitioners should be aware of the difference between information
security and information privacy. Information security is the protection of information in order
to prevent loss, unauthorized access or misuse. Information security also involves the process of
assessing threats and risks to information and procedures and controls to preserve confidentiality,
integrity and availability.5 Information privacy is concerned with establishing rules that
governing the collection and handling of personal information.6

FEDERAL AND STATE LAWS APPLY

A patchwork of both federal and state laws govern data privacy and security issues. If the
business is in a regulated industry, such as banking or health care, additional laws and regulators
will come into play. This myriad of laws, with different reporting requirements, may conflict at
times. As an example with respect to differences among the states, what actually constitutes a
“breach” varies greatly. If a business has a data breach involving customers in multiple states,
the laws of each of those states must be complied with regarding, for example, notifying the
customer of the breach.

The Federal Trade Commission (“FTC”) has authority to bring enforcement actions under
Section 5 of the Federal Trade Commission Act against “unfair and deceptive trade practices.”
The FTC exercises this authority broadly against a variety of commercial entities, with certain
exceptions for example, the financial services sector, to take a leading enforcement role in data
breach situations. Often a company will enter into a consent decree with the FTC rather than
proceed to trial. Normally, the consent decree includes a fine and specific actions the defendant
must take and refrain from taking in connection with a data security and privacy program.7

In 2012, FTC brought an enforcement action against Wyndham Worldwide Corporation after a
series of data breaches. The FTC alleged that Wyndham and three of its subsidiaries failed to
take adequate security measures to protect the personally identifiable information of over
600,000 customers in three breaches over two years. The FTC claimed authority under the

4 Id. at 4.
5 Foundations of Information Privacy and Data Protection, Peter P. Swire and Kenesa Ahmad p. 77-78
6 Foundations of Information Privacy and Data Protection, Peter P. Swire and Kenesa Ahmad p. 2
7 Patricia Bailin, Study: What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and
https://privacyassociation.org/news/a/study-what-ftc-enforcement-actions-teach-us-about-the-features-of-
reasonable-privacy-and-data-security-practices/. This report provides an interesting analysis of FTC consent
decrees.
“unfairness” prong of the FTC Act and utilized 15 U.S.C. § 45 to bring the enforcement action and seek remedies. The Wyndham case is interesting from several perspectives, namely that Wyndham is one of the first defendants to refuse to acquiesce to a consent decree and actually challenge the FTC’s authority to bring enforcement actions under Section 5 in the data privacy arena.

DUTIES OF THE BOARD OF DIRECTORS

Under Kentucky corporate law, the statutory duty of care imposes on directors and officers the obligation to manage an entity in good faith, on an informed basis, and in a manner that they honestly believe to be in the entity’s best interest.8

A director or officer will be deemed to have acted on an informed basis if he acts with the care that an ordinarily prudent person would exercise in a like position in making inquiries into the business and affairs of the entity or in regard to a particular action to be taken or decision to be made.9

The statute further provides that:

“(3) in discharging his duties a director shall be entitled to rely on information, opinions, reports, or statements, including financial statements and other financial data, if prepared or presented by:

(a) One (1) or more officers or employees of the corporation whom the director honestly believes to be reliable and competent in the matters presented;

(b) Legal counsel, public accountants, or other persons as to matters the director honestly believes are within the person’s professional or expert competence; or

(c) A committee of the board of directors of which he is not a member, if the director honestly believes the committee merits confidence.

(4) A director shall not be considered to be acting in good faith if he has knowledge concerning the matter in question that makes reliance otherwise permitted by subsection (3) of this section unwarranted.”10

A director shall not be held liable for monetary damages or injunctive relief unless (a) the director has breached or failed to perform his or her duties in accordance with the standard of care set forth in the statute and (b) in the case of an action for monetary damages, the breach or failure to perform constitutes willful misconduct or wanton or reckless disregard for the best interests of the corporation and its shareholders.11

8 KRS § 271B.8-300(1).
9 KRS § 271B.8-300(2).
10 KRS § 271B.8-300(3) and (4).
11 KRS § 271B.8-300 (5).
In Kentucky, the standard is whether a director “honestly” believes he is acting in the best interest of the corporation, but the Delaware standard is whether the director “reasonably” believes he is acting in the best interests of the entity. The duty of care as developed under case law entails a duty to reasonably monitor the entity’s business.\textsuperscript{12} This duty imposes a continuing obligation to keep informed about activities of the entity, including data privacy and security protocols. This duty only includes an obligation to investigate when there are circumstances that would alert a reasonable manager to the need for inquiry. Once these circumstance arise, the manager must make a reasonable investigation and take reasonable curative steps if a problem is found.

**FIDUCIARY DUTY AND BUSINESS JUDGMENT RULE ANALYSIS IN DATA BREACH CASES**

The Wyndham breaches also led to a shareholder derivative suit being filed against the directors and officers in the US. District Court for the District of New Jersey. The opinion in that case sheds some light on how a court might interpret a board of directors and officers actions pre-breach in determining whether they have met their obligations under the business judgment rule. The complaint alleged that the board of directors and officers of Wyndham breached their fiduciary duties by failing to prevent and properly disclose data breaches in the company’s online networks to mitigate against hacking incidents. The complaint alleged breach of fiduciary duties, corporate waste and unjust enrichment against certain directors and officers for failing to implement adequate security policies or update the company’s security systems. The complaint also alleged that the named directors’ and officers’ failure to timely disclose the data breaches in the company’s SEC public filings aggravated the damage caused by the data breach.

The court, applying Delaware substantive law, dismissed the plaintiff’s allegations that the board acted in bad faith in not filing a shareholder derivative suit and found that the Board’s investigation of the breach was reasonable.\textsuperscript{13} The court ultimately granted the Defendant’s motion for dismissal holding that the Defendant’s decisions with respect to pre-breach data security protocols and subsequent post-breach investigation fell under the purview of the business judgment rule and that the Plaintiff’s failed to overcome the presumptions afforded by that rule.\textsuperscript{14}

The opinion noted that the Board had discussed the cyber-attacks, the security policies and proposed security enhancements at fourteen meetings between October 2008 and August 2012. In addition, the Audit Committee reviewed the same matters during at least sixteen meetings during the same time period. Wyndham hired technology firms to investigate each breach and to issue recommendations on enhancing security. Wyndham began implementing the recommendations following the second and third breaches. At every quarterly Board meeting, the General Counsel gave a presentation on the breaches or Wyndham’s data security generally.

\textsuperscript{12} *In re Caremark Int’l Inc. Derivative Litig.*, 698 A.2d 959, 967 (Del. Ch. 1996).
\textsuperscript{14} Id. at *2-*3.
Action Plan

With the frequency of data breaches increasingly annually, directors and officers cannot continue to claim ignorance with respect to the need for proactivity in preparing for these threats to their company. The following are the types of actions management can take:

- Hire a dedicated Privacy Officer and/or Security Officer whose full time job is to implement data security and data privacy policies and ensure data is being protected. Depending on the size of the company, it may be appropriate to have additional employees in a dedicated department.

- Appoint at least one board member well versed in data privacy and security matters so reports to the board may be independently assessed and verified.

- Report to the Board on a regular basis on cyber security issues and security policies.

- Form a Data Privacy and Security board committee, which should include the tech savvy board member and the Privacy Officer and Security Officer.

- Conduct mandatory employee training on data security and data privacy. Update the training on a regular basis.

- Maintain adequate security systems in light of complexity and size of the organization and the amount of personal and nonpublic data in its possession.

- Prepare and implement a written data security plan. Plans often include the following elements:  

  o A description of the physical, technical, and administrative safeguards to keep sensitive personal data secure;

  o A method to continually identify internal and external threats to the security of the sensitive personal data an organization maintains;

  o An assignment of ultimate responsibility to one employee, likely an officer, for maintaining and implementing the organization’s security policies for the sensitive personal data it maintains;

  o Maintain processes for data mapping. What information do you have, where is it and who has access? What is the company’s data retention program? Does the company have more information than it needs?

  o Implement criteria for the circumstances under which sensitive personal data may either leave the organization or move about inside the organization;

---

- Technical and end user requirements on protocols. Procedures such as:
  - user name and password, encryption, and destroying sensitive data.
- Prepare and implement a written data breach response plan for post-breach response and practice a breach response. The incident response team should be formed with members from various departments of the organization including the legal department, IT, human resources, and public relations. The cyber insurance carrier will be part of the team. Outside legal counsel will be part of the team. If the company does not have an internal public relations department, consider contacting a public relations firm ahead of time just to have a contact ready. Mitigating damage effectively often depends on the shortest possible response time following a breach.
- Maintain adequate insurance coverage for cybersecurity; See Cyber Liability Insurance below.
- Conduct due diligence on the company’s vendors. The Target breach started from a vendor.\(^{16}\)
- Be careful about statements made during the investigation of the breach and after the breach is made public. Various considerations come into play:
  - If law enforcement is involved, they may ask the company to not disclose that the breach occurred or certain information if the investigation is ongoing.
  - The attorney-client privilege should be considered and for example, counsel may want to retain the privilege in connection with some documents and should be careful about sharing documents or information from the documents with others.
  - Some commentators believe the next wave of shareholder suits on the horizon will involve 1934 Securities Exchange Act Rule 10b-5 suits alleging misrepresentations over cybersecurity risks.

Remember, any given company suffering from a data breach will be judged in hindsight. Will the company be viewed as having acted reasonably to protect the confidential information it held? What procedures and policies did it have in place and were they followed? What remediation plans did the company have to remedy problems once they were discovered? Were employees trained?

To further protect directors and officers, the board should consider directors’ and officers’ liability insurance. In addition, Kentucky law permits the articles of incorporation to provide for elimination of liabilities of a director to the corporation or its shareholders for monetary damages

---

\(^{16}\) Tanya Forsheit, *Vendor Contract Review and Cyber Risk Mitigation: How to Keep it Drama Free*, WWW.DATAPRIVACYMONITOR.COM (November 5, 2014), http://www.dataprivacymonitor.com/cybersecurity/vendor-contract-review-and-cyber-risk-mitigation-how-to-keep-it-drama-free/. This article provides an excellent overview of some practical “dos and don’ts” with respect to vendors and pre-breach data security procedures.
for breach of his duties as a director. Kentucky law does not, however, allow for the elimination or limitation of the liability of a director for any transaction in which the director’s personal financial interest is in conflict with the financial interests of the corporation or the shareholders, or for acts or omissions not in good faith or which involve intentional misconduct or are known to the director to be a violation of the law. Kentucky law also allows for indemnification of directors, officers, employees and agents under certain circumstances. Consider including an indemnification provision in the articles of incorporation as well as a provision for advancement of expenses.

CYBER LIABILITY INSURANCE

Along with having data privacy and data security plans in place a company will want to manage risk by reviewing its current insurance policies. Normally, a general liability policy will not provide coverage for a data breach. The costs of the forensic investigation as well as notification costs and damages can be extremely high. A cyber liability insurance policy is an increasingly popular way to manage the risk of loss posed by a cyber-attack. Cyber liability insurance protects the company, not the Board of Directors.

Cyber liability insurance policies, however, are far from standardized and can differ dramatically in terms of what the policy will cover and exclude, and the amount of retentions (or deductible). Policies often require that the insured notify the insurer following a breach or that the insured use certain post-breach data incident response professionals, such as certain investigators, credit monitoring services, mailing services, public relations firms, or outside counsel. What type, level, and terms of coverage are appropriate for a particular business often will depend on the size and the potential impact a data breach might have on the business. Policies should be reviewed annually in light of the rapidly evolving nature of data privacy and security law.

As with any policy, it should be reviewed periodically to determine what is covered and what is excluded and what the insured needs to do to retain coverage. Below are some common points to consider:

- What is covered? Is employee negligence covered? What if an employee allows a hacker into the system by clicking onto a tainted website or link? Will that be covered?
- Is the cost of retaining outside counsel to assist in post-breach investigation, organization, and damage mitigation covered. Is advising the company on its statutory obligations to notify consumers and taking other such appropriate actions to reduce the likelihood of consumer and shareholder lawsuits covered? Does the policy provide that

---

17 KRS § 271B.2-020 (2)(d)
18 KRS §§ 271B.8-500-271B.8-580
19 Although only 31% of companies have purchased insurance that covers part, or all, of the costs of a data security breach, other survey data indicates that the majority of companies that do not have cyber insurance are considering purchasing it within the next 24 months. Ponemon Institute, 2014 Cost of Data Breach Study: Global Analysis, at 22 (May 2014).
20 See Supra note 11.
21 See Supra note 11.
a certain law firm or lawyer be retained or may the insured choose from a panel of law firms or lawyers? Does the policy exclude certain services by the law firms, such as negotiating or participating in the post-breach investigation?

- Is the cost of any forensic investigation covered? If so, does it limit selection to a single investigator, or are there situations in which the policy would permit hiring multiple investigators if needed? Are there any sub-limits or sub-retentions?

- Is the cost of consumer notification covered? If so, are there any limitations? For example does the insurer or the company control how the notices are provided? If, for example, the insurance company requires the company to use substitute notice (notice by posting in newspapers or websites for example) when permitted under the law then the insurance company may not provide coverage if the company would prefer to provide notice by mail. Some companies prefer to provide notice by mail even though it may not be statutorily required in order to reduce reputational damage. Will the insurance cover such a notice? Is there a sub-limit or sub-retention on consumer notification?

- For consumers who may be impacted by a breach in a company’s data security, does the policy cover the cost of providing credit monitoring, identity restoration services, or identity-theft insurance? If so, does the policy provide that the insured choose from a panel of providers to provide for such services and are there any sub-limits or sub-retentions on these costs?

- Is the cost of any type of regulatory proceeding that may result from a breach covered by the policy. If so, does the coverage include any resulting legal fees for representation or fines or civil penalties related to such regulatory proceedings? Are investigations by certain regulatory agencies included and are there any sub-limits or sub-retentions?

- Is the costs of contractual liabilities arising from the data security breach covered by the policy? One common example is credit card payment processors, which are sometimes subject to Payment Card Industry (PCI) fines or assessments.

**KENTUCKY’S TWO NEW LAWS—Are You in Compliance?**

During the 2014 Kentucky general assembly, two data breach laws were enacted. One applies to Kentucky governmental agencies and non-affiliated third parties ("NTP"), KRS §§ 61.931-934 (the “Kentucky Agency Law”), and the other applies to Kentucky businesses, KRS § 365.732 (the “Kentucky Business Law”). The following is a brief overview of the two new laws.

**Kentucky Agencies and Non-Affiliated Third Parties (the “Kentucky Agency Law”)**

*Some Key Definitions*

In order to interpret KRS § 61.931-934 it is important to understand certain key definitions.

The definition of “agency” is very broad. The definition includes but is not limited to the executive branch of state government, every county, city, municipal corporation, urban county
government, or a department, ad hoc committee, public agency, special purpose governmental entity, instrumentality, of the executive branch or a county or city or municipal corporation or urban county government. The definition of agency also includes public school district, public institution of postsecondary education including every public university in the Commonwealth of Kentucky and KCTCS. Counsel should parse through the definition carefully to determine whether the definition of agency is met. For example, airport boards and water districts meet the definition.

“Non-affiliated third party” or “NTP” means an entity which has a contract with an agency and receives personal information pursuant to the contract. Notice the flow of personal information; it must flow from the agency to the NTP.

“Personal information” or “PI” means generally a person’s first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one or more of the following data elements:

- Account number, credit card number or debit card number that in combination with any required security code, access code or password would permit access to an account;
- Social security number;
- Taxpayer ID number that incorporates a social security number;
- Driver’s license number, state ID card number or other individual ID number issued by an agency;
- Passport number or other ID number issued by the United States government; or
- Individually identifiable health information, except for education records covered by FERPA.

“Security Breach” means either:

- unauthorized acquisition, distribution, disclosure, destruction, manipulation, release of unencrypted or unredacted records or data that compromises (or the agency or nonaffiliated third party reasonably believes may compromise) the security, confidentiality or integrity of personal information and result in the likelihood of harm to one or more individuals; or
- unauthorized acquisition, distribution, disclosure destruction, manipulation or release of encrypted records or data containing personal information along with confidential process or key to unencrypt the records or data and the agency or nonaffiliated third party reasonably believes may compromise the security, confidentiality or integrity of personal information and result in the likelihood of harm to one or more individuals.

So, if the personal information is encrypted and the key is not disclosed along with the information, then it is not considered a “security breach” under the statutory definition and is not reportable. Although the law does not mandate encryption, encryption when the data is stored and during transmission can save a lot of headaches.
Reasonable Security Procedures and Practices

A Kentucky governmental agency and a NTP must have “reasonable security procedures and practices” to protect and safeguard personal information against security breaches. In order to be in compliance, the “reasonable security procedures and practices” must be in writing and in accordance with the policies or regulations provided by the relevant state office.

The security procedures and practices under KRS § 931-934 must be reasonably designed to protect the personal information from unauthorized access, use, modification, disclosure, manipulation, or destruction.

Required Agreement

The Kentucky Agency law further requires that any new agreement between a NTP and a Kentucky governmental agency, or any amendment to an existing agreement, must:

1. Specify how the costs of any required notification and investigation are to be apportioned; and
2. Obligate the NTP to implement, maintain and update security and breach investigation procedures that are both appropriate to the nature of the information disclosed and at least as stringent as those required of the agency.

Data Breach Notification

The Kentucky Agency law implemented several new procedures to be followed in the event a security breach is determined or an agency receives notification of a breach from a NTP.

An agency must file Form FAC-001 with multiple state offices following a breach. The agency is responsible for making all appropriate filings, not any involved NTP. NTPs are required to assist agencies in making timely filings by notifying the agency with which it has a contract within 72 hours after the NTP determines a breach has occurred. The agency must file Form FAC-001 within 72 hours of determination or notification of a security breach unless certain conditions for a delay are met.

The filing of Form FAC-001 may be delayed if an agency or NTP is working with law enforcement, and law enforcement requests a delay in writing. Agencies and NTPs are advised to retain any documentation related to a delayed notification. If the agency has delayed notification, file form FAC-002. The forms can be found at [http://finance.ky.gov/SERVICES/FORMS/Pages/default.aspx](http://finance.ky.gov/SERVICES/FORMS/Pages/default.aspx).

No notification is required for disclosures of the PI in the following situations:

- PI has been redacted;
• PI has been disclosed to a federal, state or local governmental entity including law enforcement or court, to investigate or conduct criminal investigations and arrests or to perform any other statutory duties and responsibilities
• PI has been lawfully made available to the general public from government records or that an individual consented to have publicly disseminated
• Documents are recorded in records of county clerk, circuit clerk, or U.S. District Court.22

After the initial governmental notifications are filed, the agency must initiate a reasonable and prompt investigation in accordance with the security and breach investigation procedures to determine whether the security breach has resulted in or is likely to result in the misuse of personal information.

Once the agency has concluded the investigation and has determined both that a security breach has occurred and the misuse of personal information has occurred or is reasonably likely to occur, the agency shall:

• within 48 hours of completion of the investigation, notify the same governmental officials notified originally and the Commissioner of the Department for Libraries and Archives unless a law enforcement agency provides a written request to the agency to not send the notice.
• within 35 days of sending the notice above, notify the individuals impacted by the security breach, unless a law enforcement agency provides a written request to the agency to not send the notice or the agency has determined that measures necessary to restore the integrity of the data system cannot be implemented in that timeframe.
• at least 7 days prior to providing the notice to the individuals, notify certain governmental entities and consumer credit reporting agencies if more than 1,000 individuals are to be notified.

The statute sets forth the required notification procedures. If the agency determines the misuse of personal information has not occurred and is not likely to occur, the agency is not required to give notice but shall:

• maintain records that reflect the basis of the decision and,
• notify the agencies originally notified that a misuse of personal information has not occurred.

KRS 365.732 (8) provides that the requirements imposed on an NTP in KRS Chapter 61 shall not apply to “any person who is subject to” Gramm-Leach-Bliley Act or HIPAA. Pursuant to KRS § 61.932 (1) (c) (2) a NTP is required to provide the agency with which it has a contract a copy of any and all reports and investigations or notices relating to a security breach if it is required by federal law or regulation to conduct security breach investigations or to make

22 KRS 61.933 (5)
notifications and it is PI. Providing the agency with the report/investigation/notices constitutes compliance with KRS §§ 61.931-KRS 61.934.23

The Attorney General may bring an action for injunctive relief or, in the case of nonaffiliated third parties, other legal remedies, to enforce the statute.

**Kentucky Business Law**

KRS § 365.732 enacted general data breach notification requirements for any person or business that conducts business in Kentucky, called “information holders”, and is not limited to those who contract with governmental agencies. KRS § 365.732 does not apply to banks, health care providers or others who are subject to Gramm-Leach-Bliley or HIPAA. It also does not apply to any agency of Kentucky government, local government or subdivision. As opposed to the Kentucky Agency Law, which applies to a records of all types, the Kentucky Business Law only applies to computerized data.

The following are some highlights of KRS § 365.732:

- **Breach of Security of the System** means “unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality or integrity of personally identifiable information maintained by an information holder as part of a database regarding multiple individuals that actually causes or leads the information holder to reasonably believe has caused or will cause, identity theft or fraud against any resident of the Commonwealth of Kentucky.”24 There is an exception for good faith acquisitions of PII by an employee or agent of the information holder for the purpose of the information holder if there is not a further unauthorized disclosure. Notice there are several judgment calls to make in determining whether there has been a breach of the security of the system. Again, if the information is encrypted there will be no breach under the definition.

- **Personally identifiable information or (“PII”)** is defined an individual’s first name or first initial and last name in combination with one of the following:
  - Social Security number;
  - Driver’s license number; or
  - Account number, credit or debit card number in combination with any required security code, access code or password to permit access to an individual’s financial account.

An information holder is required to notify affected Kentucky residents if (i) the information holder suffers a data breach of electronically stored personally identifiable information; (ii) the information is not encrypted or redacted; and (iii) the information holder believes that the information has been or is likely to result in fraud or identity theft. An information holder which maintains computerized data that includes PII that the information holder does not own shall notify the owner or licensee of the information of any breach of the security of the data as soon

---

23 KRS 61.932 (1)(c) 2.
24 KRS 365.732 (1)(a).
as reasonably practicable following discovery, if the PII was or is reasonably believed to have been acquired by an unauthorized person.\textsuperscript{25}

Notice is required following discovery or notification of the breach in the security to any Kentucky resident whose unencrypted PII was or is reasonably believed to have been acquired by an unauthorized person. The disclosure is to be made in the most expedient time possible and without unreasonable delay, consistent with the needs of law enforcement.

Required notification methods are set forth in KRS § 365.732. In the alternative, if the information holder has notification procedures as part of an information security policy for the treatment of personally identifiable information that are otherwise consistent with the timing requirements of KRS § 365.732, the holder shall be deemed to be in compliance if notification is made in accordance with the holder’s own procedures.

If more than 1,000 persons must be notified at one time, then the person shall also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that maintain files on consumers on a national basis.

\textsuperscript{25} KRS 365.732 (3).