Data breaches in a whistleblower's world: What you should know, why you should know it

pwc

Two trends today are on a collision course that harbors hidden challenges for Corporate America and other organizations wishing to stay out of the courts and out of the headlines. On the one hand, a decade of scandals has raised the bar for compliance and integrity while significantly protecting and encouraging the role of the whistleblower. On the other hand, reliance on today's highly digitalized operations has rendered corporations and other entities more vulnerable than ever to data breaches and related fallout. Data today is like quicksilver — flowing freely and fiercely fast, through a vast ecosystem, often out of sight of business leaders, who tend to be intent on growth and often removed from the nitty-gritty details of the digitized microcosm of their own enterprise.

Meanwhile, those who would take an entity to task for wrong-doing, whether its genesis is intentional or even a mere misstep, have perhaps never before had more incentive to follow through on their instincts. The Dodd Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), the Sarbanes-Oxley Act of 2002 (SOX), and other state and federal laws and regulations have sought to encourage employees and other stakeholders to step forth with information about and allegations against corporate wrongdoing. Dodd-Frank, in particular, went a step further than other similar laws by offering generous bounties in the offing for those whose charges bear out as part of an effort to provide incentives for more whistleblowers to come forward.

Data breaches, whether triggered by deliberate cyber attacks or tripped by unintentional oversights, can expose an organization's proprietary information, unleashing for the world to see highly sensitive data about the entity, its employees, customers, and other stakeholders. When financial assets, intellectual property, and such personal and vulnerable information as Social Security numbers become potentially compromised, the stakes grow dear. The entity's reputation is on the line: how and how quickly the business responds will have a powerful impact on its risk of litigation and/or regulatory action, and on the confidence and trust of its employees, customers, third parties, and shareholders. These risks make it more than an IT issue; it’s a business issue that can affect future cash flows.

Taken together, the whistleblower impetus and digital data vulnerability point toward serious implications for companies that have data breaches and fail to notify those potentially affected by them. If not addressed proactively, underlying issues that may be raised by a potential whistleblower can bring with them the possibility of costly investigations, regulatory inquiries, ensuing penalties, and securities litigation at a time when the plaintiff's bar is vigorously zeroing in on new targets.

When breaches hit — and they all but inevitably will — business leaders should proceed with great urgency. Not only are we operating in a world in which cyber criminals are more sophisticated and aggressive than ever, but we're also only a handful of years removed from a scandal-rife decade that spurred a strong, global anti-corruption environment and a strong compliance climate in which such breaches won't be treated lightly. Law enforcement agencies, such as the Department of Justice, may begin to seek punishment with greater frequency against corporations that fail to disclose and respond to data breaches in a timely manner.[1]

[1] The Department of Justice is being encouraged to take a more active role in data breach investigations. For example, in an April 2011 letter to Attorney General Eric Holder, Senator Richard Blumenthal of Connecticut sought to have the Department of Justice investigate a large corporate data breach.

At the same time, cyber attacks — from hackers, nation states, competitors, criminals, third party vendors, and even employees — are on the rise, bringing with them data breach threats and financial implications, including the costs of replacing stolen assets and increasing internal controls. While breaches occur often in the information technology context, they can have serious ramifications for a business's sales, finance, operations, and security functions.

The confluence of data breach issues and the need to have robust compliance mechanisms that swiftly field and address whistleblower concerns should sit among those challenges that top the C-suite agenda. Corporations should remain aware of these trends and stand ready to mitigate the risks they pose. In particular, they should put in place internal controls against the risks associated with failing to correct, prevent, or act upon data breaches in a timely manner.

Your client's been hit by data breach. The investigation is underway. Now what? Act quickly on disclosure decisions.

1. **To investors:**

Although federal securities law doesn't have a disclosure requirement that explicitly refers to data breach incidents or risks, the SEC has said through a Disclosure Guidance[2] that standing requirements may already impose an obligation to disclose data breach information. The entity may have to disclose such risks consistent with its normal securities filings if the possibility of a data breach is among the most significant factors that make an investment in the company speculative or risky.

For example, Regulation S-K requires disclosure of various risks facing the enterprise. The SEC expects the disclosure to be determined based on prior data breaches, the frequency and severity of prior data breaches, the probability and potential magnitude of data breaches, and the adequacy of preventative measures.

A corporation that fails to disclose this information may also be at risk with respect to whistleblower provisions under the Sarbanes-Oxley Act,[3] the Dodd-Frank Act,[4] and other federal and state statutes. Note that numerous individuals can be eligible to receive a whistleblower bounty. Employees, former employees, vendors, agents, contractors, clients, customers, and competitors are all potential sources of tips and complaints that could justify a whistleblower reward.

The Dodd-Frank Act requires the SEC to award eligible whistleblowers a bounty of 10% to 30% of the monetary sanctions recovered in eligible SEC or related actions stemming from the whistleblower's information. The whistleblower must provide the SEC with "original information" about any violation of federal securities laws, and is rewarded for information that leads to a successful SEC enforcement action of $1 million or more.

2. **To affected individuals:**

At the state level, 46 states plus Washington, DC; Guam; Puerto Rico; and the Virgin Islands all have data breach notification laws. The European Union and a number of other countries have adopted similar laws. Within the United States, the laws typically require notification[5] to impacted individuals, the state's attorney general or another government entity, and credit reporting agencies. A lack of disclosure may result in fines.[6]

Most states require that a written notice be sent to the impacted individual. But email, conspicuous posting of a notice on a corporation's website, or a broadcast on major statewide media typically suffices if:

- The cost of providing the notice exceeds $250,000
- The number of affected people exceeds 500,000
- The corporation lacks sufficient contact information

---

[2] U.S. SECURITIES AND EXCHANGE COMMISSION, DIVISION OF CORPORATE FINANCE, DISCLOSURE GUIDANCE: TOPIC 2 (2011).
[3] Sarbanes-Oxley Act, 18 U.S.C. §73 (2012).
[4] Dodd-Frank Wall Street Reform and Consumer Protect Act, 15 U.S.C. §78a *et seq*. (2012).
[5] Such communication should be in the languages most likely to be understood by the recipients.
[6] Fines as much as $1.5 million, and potential criminal penalties, enforceable by state Attorneys General, are provided for under The Health Information Technology for Economic and Clinical Health Act (HITECH), which is part of the American Recovery and Reinvestment Act of 2009.

If a corporation fails to perform such notification, it may be at risk with regard to the whistleblower provisions under the applicable state and/or federal laws.

While just about anyone who is affected can report a data breach, employees play under special rules and protections. SOX, for example, allows employees of publicity-traded corporations to disclose data breaches or the entity's lack of disclosure and protects them from retaliation such as firing, demotion, or harassment. Similarly, SEC rules don't require employee-whistleblowers to report complaints internally, but SEC guidance does encourage the individual to begin with the employer by offering greater bounties by percentage to those that can demonstrate such an approach.

In almost one-third of the states or territories within the United States that require data breach notification, whistleblower statutes allow corporate employees to disclose information about the entity breaking federal or state law, under protection from corporate retaliation.

3. **To law enforcement:**

State and federal law enforcement officials appreciate cooperation. Factors such as an organization's internal controls and the incidence of corporate disclosure prior to a government investigation can affect whether the entity will face punishment, and if so, to what extent.

It's important for business leaders to demonstrate that they take breaches seriously and that they bring additional resources to the data breach investigation. Companies that fail to take sufficient steps may find that they are liable. For example, in states that have applicable data breach notification laws, failure to notify state authorities may well result in an investigation by the state's attorney general.

At the federal level, the Federal Trade Commission has played an increasingly active role in investigating and penalizing corporations for misrepresenting their privacy and information security practices with regard to personal information. Significantly, the recent advent of the Consumer Financial Protection Bureau provides another investigative agency to which whistleblowers can report a corporation's lack of disclosure of a data breach.

Meeting whistleblower challenges in the digital age

Data breaches are an ever-present reality in today's digital age. They can be among a corporation's steepest challenges, as the business's confidential and personal information explodes out of its systems and into the public domain. Affected employees and other stakeholders have perhaps never before had more incentive to raise a din about such slip-ups.

If a corporation fails to have a strong compliance culture and take action early and effectively when potential issues are raised by whistleblowers or other individuals, it's likely to be more vulnerable to significant ramifications, including costly litigation and law enforcement penalties. By proactively taking sufficient steps — notifying investors, impacted individuals, and law enforcement — clients can have a better chance of avoiding costly litigation, painful penalties, and a black-eyed brand.

For a deeper discussion, please contact:

Kristofer Swanson
Partner
PwC
(312) 298-6195
kris.swanson@us.pwc.com

We'd like to acknowledge the following co-contributors:

Thomas L. Kirsch II, Partner, Winston & Strawn and Ryan M. Dunigan, Associate, Winston & Strawn

The first publication of this article is attributed to the American Bar Association Criminal Justice Section Newsletter, Spring 2013 issue.