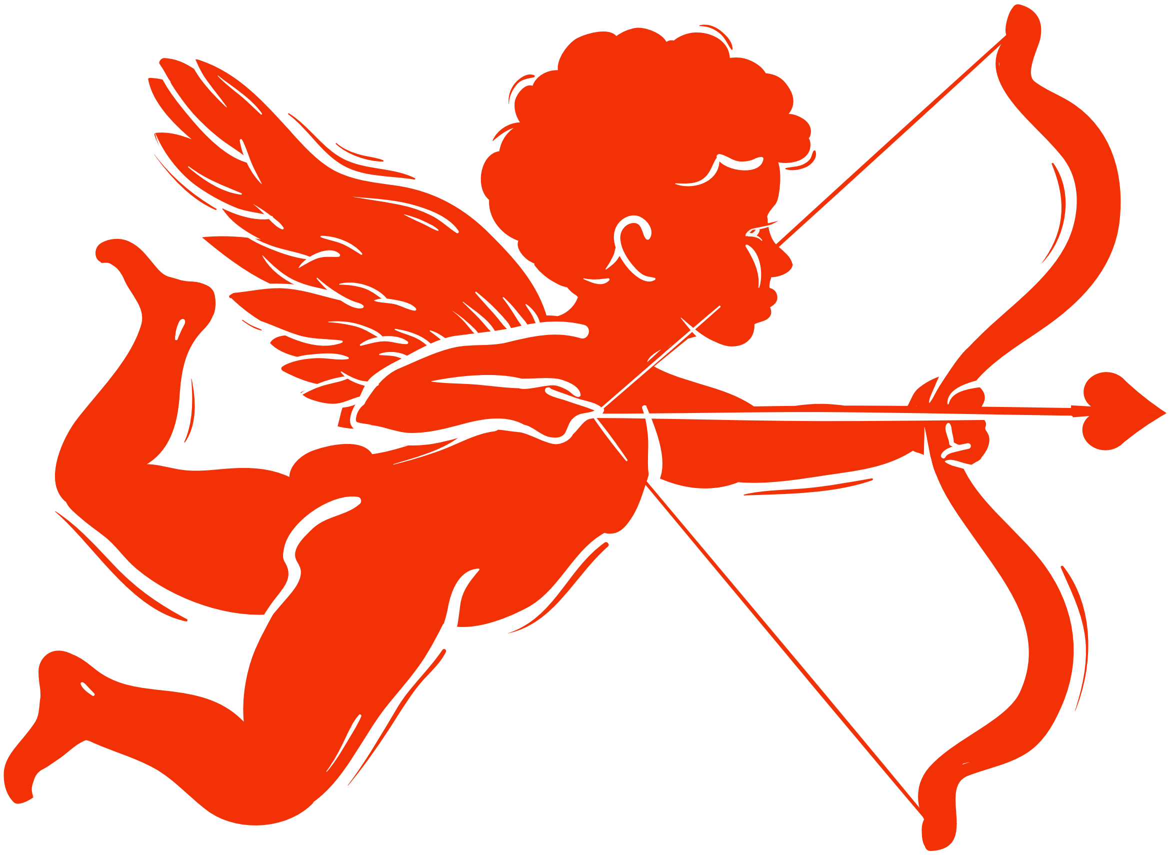

DON'T SHOOT THE MESSENGER: THINGS TO CONSIDER WHEN DECIDING WHETHER AND HOW TO "MESSAGE" AN INCIDENT

BY
SADIA MIRZA

&
KAMRAN SALOUR

Sadia Mirza and Kamran Salour are data privacy and cyber security attorneys at Troutman Pepper.

TechREG CHRONICLE
MARCH 2023

Visit www.competitionpolicyinternational.com for access to these articles and more!

DON'T SHOOT THE MESSENGER: THINGS TO CONSIDER WHEN DECIDING WHETHER AND HOW TO "MESSAGE" AN INCIDENT

By Sadia Mirza & Kamran Salour

When an organization experiences a data security incident, one of the first questions the organization asks is: Who do we have to notify? This question is often followed with two other ones: What do we have to say? And when do we have to say it? From a legal standpoint, applicable statutes, contracts, and regulations often dictate to the answers to these inquiries. But notification is not limited to a legal inquiry. Business considerations, such as maintaining customer relationships and goodwill, are important but often overlooked when organizations think about notification. This article explores non-legal notification of an incident, its benefits, its risks, and a framework of factors to consider whether to make a non-legal notification at all.

When an organization experiences a data security incident, the organization likely must make certain, time-sensitive decisions. One such decision is whether to "proactively message the incident" — the act of voluntarily informing internal and external stakeholders of the incident. Whether an organization should proactively message the incident depends on a bevy of factors, some of which will be unique to the specific incident. But there are several factors an organization should generally consider when deciding whether to proactively message the incident.

Before delving into these factors, it is prudent to distinguish proactive messaging from the other categories of messaging that typically arise when an organization experiences a data security incident. When an organization experiences a data security incident, there are four general categories of messaging that may arise. The first category is statutory consumer notification (e.g. think of a data breach notification letter sent to individuals). The second category is regulatory notifications (e.g. notifications to attorneys general or industry regulators, such as the Department of Health and Human Services or the FDIC). The third category consists of contractual notifications; a contractual agreement that requires an organization to notify its customers or vendors of an incident. The fourth category, proactive messaging, comprises the voluntary messages an organization makes about an incident that are intended to promote the organization's relationship with employees, vendors, and customers.

Messaging under the first three categories is usually mandatory. And although an organization experiencing a data security incident may have discretion under the first three categories whether to message, such discretion is bounded by the applicable statutes, regulations, or contractual provisions. Those statutes, regulations, and contractual provisions largely dictate the timing and content of any such notification. Proactive messaging, the fourth category, is largely permissive. Because there are no timing or content requirements of such messaging, organizations often must decide whether to message at all.

So how should an organization decide whether to proactively message an incident? There are five central factors to consider.

01

FACTOR ONE: IMPACT OF THE DATA SECURITY INCIDENT ON OPERATIONS

The first factor an organization should consider when deciding whether to proactively message an incident is the data security incident's impact on business operations. If the data security incident disrupts operations such that an organization cannot communicate with customers or vendors or facilitate business with them, even temporarily, then the organization will likely have to acknowledge that an incident occurred. In the past, an organization may have been able to claim that a "network disruption" caused a cessation in business operations. Today, however, customers and vendors, generally interpret "network disruption" to mean a data security incident.

If the incident has not impacted operations, an organization should then consider factor two: the incident type.

02

FACTOR TWO: TYPE OF INCIDENT AN ORGANIZATION EXPERIENCES

The type of incident an organization experiences is the second factor to consider. If the organization experiences a ransomware attack that does not impact operations, it is still possible that the organization's employees, customers, and vendors may nonetheless be aware of the incident. Perhaps an employee has seen a copy of ransom note. If an employee has seen a copy of a ransom note, then the organization should consider proactively messaging the incident, at least internally to its employees. Similarly, if during the data security incident, a threat actor sent phishing emails to the organization's vendors and customers, then proactive messaging to them is likely necessary.

Conversely, if the data security incident has a more discreet impact on the organization, for instance the organization detects logins from suspicious locations or a threat actor attempts to take over a single employee's account, then proactively messaging may not be worthwhile. The organization should then consider factor three.

03

FACTOR THREE: THE TYPE OF DATA POTENTIALLY AT ISSUE

The third factor to consider is the type of data potentially at issue. The organization should consider the type of information it collects, stores, and shares. The organization should also consider from whom it collects, stores, and shares such information. If the organization does not collect or store Social Security numbers, driver's license numbers, or debit/credit card numbers, then it may behoove the organization to proactively message the incident because the potentially impacted customers may not be overly concerned. Conversely, if the organization does collect or store such information or proprietary information belonging to customers, the organization may want to hold off on messaging until the organization has a better understanding on whether that information has been impacted. This leads to the fourth factor to consider.

04

FACTOR FOUR: HOW MUCH IS KNOWN ABOUT THE DATA SECURITY INCIDENT

The fourth factor for an organization to consider is how much information the organization knows about the data security incident. Suppose an organization collects personal information belonging to third-party customers. But the organization does not yet know which customer information, if any, is impacted. If the organization tells its customers of an incident but cannot also tell the same customers that their information has not been impacted, then proactively messaging the incident may cause more uncertainty.

The purpose of proactively messaging is to minimize the impact of the incident on the organization. When a third party learns of an incident, the third party will likely want to know whether their information is impacted. At the early stage of an incident, an organization may not know, especially if the incident occurs outside of the organization's environment. Sending a message without being able to answer follow-up questions could do more harm than good.

05

FACTOR FIVE: WHO IS THE AUDIENCE?

The fifth factor to consider is the messaging's audience. If the impacted organization seeks to message the incident internally, the organization must consider whether it can trust that its employees will not disseminate the information outside of the organization. If the impacted organization seeks to message the incident externally, will the organization's customers and vendors appreciate the information and, in turn, be empathetic, or will they respond negatively.

When determining whether to proactively message a data security incident, the impacted organization's decision should be guided by a single question: Will proactively messaging the incident likely reduce the incident's impact on the organization?

06

TIMING: WHEN SHOULD AN ORGANIZATION PROACTIVELY MESSAGE?

Once an organization decides to message, there are additional considerations. The first consideration is when. In deciding when to message, an organization must balance the benefit of providing its employees, customers, and vendors with certain information about the data security incident against the risk of being unable to provide them with all the information they likely seek.

Suppose an organization experiences a ransomware attack. That organization collects and stores HR-related information of its employees and collects and stores proprietary information belonging to its customers. It is not unusual for an organization not to know the full scope of data access or exfiltration (theft). Upon discovery of a ransomware attack, it is unlikely an organization knows the extent of data access or exfiltration.

The organization must therefore weigh the benefits of informing employees, customers, and vendors upon discovery of the incident even though the organization will unlikely be able to tell them that their data has not been impacted by the data security incident. Not being able to answer a critical question, such as whether any data was impacted, can cause frustration. The other concern is of course whether the organization's employees, customers, and vendors will be more frustrated to learn about an incident that occurred 60 days prior, but now know that their information has not been impacted. How will the organization's employees, customers, and vendors react if they learn for the first time 90 days after the incident occurred both that there was an incident and that their data has been impacted?

07

WHY PROACTIVELY MESSAGE?

Proactively messaging requires an organization to weigh several factors. Often proactively messaging comes with risk. The question then becomes why should an organization even consider such messaging? Messaging, however, can how powerful benefits.

Consider the following scenarios:

- **Scenario 1:** An organization detects a data security incident. It notifies its customers immediately. After the investigation concludes, the organization advises its customers that **no** customer information has been impacted.

- **Scenario 2:** An organization detects a data security incident. It notifies its customers immediately. After the investigation concludes, the organization advises that certain customer information has been impacted.

- **Scenario 3:** An organization detects a data security incident. It does not notify its customers and instead elects to wait until after the investigation ends. After the investigation concludes, the organization advises that **no** customer information has been impacted.

- **Scenario 4:** An organization detects a data security incident. It does not notify its customers and instead elects to wait until after the investigation ends. After the investigation concludes, the organization advises that certain customer information has been impacted.

A. Benefits of Messaging: Avoiding Surprises

One such benefit is to avoid surprises. Consider the third scenario above — in which an organization notifies its customers of a data security incident shortly after discovering it. Several weeks later, when the organization's investigation is complete, the organization informs its customers that no information has been impacted. The customers in this scenario are undoubtedly pleased to know that both an incident occurred and the outcome of the incident.

Consider the fourth scenario. In this scenario, the organization decides not to message its customers upon discovery of its incident. Several weeks later, when the organization's investigation finishes, the organization informs its customers that their information has been impacted. The customers in this scenario are likely to question why the organization did not advise them sooner.

B. Benefits of Messaging: Maintaining Trust

A second benefit is to maintain trust. In scenarios one and two, the organization has taken a potentially negative situation (experiencing a data security incident) and minimized its impact because it notified its customers immediately. Conversely, in the third scenario, even though no customer data has been impacted, the organization may have damaged its trust relationship with its customers by not advising them of the incident sooner.

C. Benefits of Messaging: Building Empathy

A third benefit is generating empathy. If your organization experiences a data security incident, it is unlikely that none of its customers or vendors have not also experienced one. Those who have experienced a data security incident understand the stress and impact an incident may have on an organization and the time the incident response process takes away from the organization's day-to-day responsibilities and in general. A little understanding can go a long way.

08

RISKS OF PROACTIVE MESSAGING

Because of the main benefits of proactive messaging is to inform employees, customers, and vendors of an incident shortly after its discovery and often before all information about the incident is known, proactive messaging can present certain risks.

The main risk of proactive messaging is that an organization's employees, customers, and vendors learn of an incident. The more people that know of an incident, the more problems that can arise. For instance, now that the employee, customer, or vendor knows of an incident, they may have lost trust in the organization's security practices.

The loss of trust by itself can be costly to an organization. But it can also result in real, tangible cost increases during the incident response process. When an organization's customer learns of a data security incident, the customer may want to take a hands-on approach and have weekly update calls. This can slow down the response process of the organization and increase the organization's legal costs. This can also increase cyber-related costs as the organization may now be required to implement certain new safeguards to prevent the incident from happening again.

Messaging also brings with it a risk of litigation. Anything that is said in the messaging can be used against the organization during litigation. If the organization does not message, then the organization does not have any statements that can be used against it during litigation.

09
WAYS AN ORGANIZATION CAN PREPARE FOR THE PROACTIVE MESSAGING DECISION

It should be evident that whether to message is a complicated decision that depends on many factors. Some of those factors will not be known until the incident occurs. It is therefore prudent for the organization to take certain steps to prepare of messaging.

First, the organization should conduct "data mapping." Data mapping allows the organization to know what data it has and where that data is located. The data mapping should extend beyond the organization's data and include any third-party customer or company data. Why is data mapping important?

Consider the scenario where a company experiences a data security incident. The company knows that the data security incident impacted its cloud servers, but the company knows that it only stores third-party data on premises. In deciding whether to message, the company may determine that messaging the location of the incident, and the current belief that the third-party customer data is not impacted, to be a positive message. This also quells another inquiry that often follows with any incident messaging; how do you know my data is not impacted. Conversely, without knowing what data that the company has and where that data is located, the company cannot make such an assertion in messaging.

Second, knowing what type of data an organization collects and store is also important. If an organization only holds public information about a customer, then messaging that is likely to be received well. Conversely, if that organization holds Social Security cards or proprietary company information, messaging that may not be as well received.

Third, the organization should conduct a contractual analysis. If an organization's contracts require it to notify certain customers about an incident, that is important to know. Because of the contract states that an organization must notify its customer upon discovery of a suspected incident, then the organization should consider notifying all its customers. It is likely to assume that once one customer learns of an incident, then all other customers will. And the customers that hear it from another customer and not the impacted organization will not be happy.

Fourth, the organization should know its audience. Are the organization's customers and employees the type that will respond positively or negatively to messaging. In general, an older customer base may not fully appreciate the complexities of an incident response process, or the time that the process may take. A sophisticated audience may better understand that incidents are seemingly inevitable and therefore be more compassionate.

10
THE RULES OF MESSAGING

No matter the decision, there are certain rules to messaging. Perhaps, the most important rule is to not use the word "breach." The term "breach" is a legal term and can trigger certain legal obligations.

It is also prudent to avoid terms like "personal information," especially saying that no "personal information" is involved. Personal information is a defined term that may have a specific meaning in various contexts. It is preferable for an organization to specify the categories of information that are not impacted, for example, no Social Security numbers or governmental identifiers have been impacted.

Finally, it is important not to say anything that is untrue or that could be perceived as misleading.

There are a seemingly infinite number of items to consider when an organization decides whether to message an incident. Because every incident presents different considerations, there is not a one-size fits all response to that critical question. But the above sets forth important items to look at when making the decision. ■

> *It should be evident that whether to message is a complicated decision that depends on many factors*

CPI
SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY® INTERNATIONAL