4 Strategies For Drafting Effective Consumer Breach Notices

By **Kamran Salour, Ronald Raether and Sadia Mirza** (September 30, 2022)

Kamran Salour

Ronald Raether

Sadia Mirza

It is 2022, which means you've received your fair share of consumer breach notification letters.

At first glance, all the letters seem to look and say the same. Usually separated into five sections — we can thank California for that — the notices explain what happened, what personal information was involved, what the business is doing in response to the incident, what consumers can do to protect themselves and who the consumer can contact for additional information.

While there are formulaic requirements for consumer breach notifications, businesses responding to data security incidents should not treat their notification letters as a copy and paste exercise.

Businesses should instead approach these notices like every other step in the incident response process — as a tool intended to inform consumers while managing the business impact and legal risk.

Effective communication during the incident response process can have a lasting effect on the company, and often these communications start with the breach notice.

So what should businesses be considering when drafting these notices? Below are our top four strategies for effective consumer breach notification letters.

1. Know your audience and what is on their mind.

When drafting notices, it is important to know and understand your audience.

You should consider what questions the notification letter recipients will have when reading the notice in order to resolve those questions through the notice to minimize any follow-up or escalations. In the context of breach notifications, the audience is consumers and regulators.

Consumers are interested in learning how the incident relates to them personally, while regulators are interested in the business's response to the incident, including notification timing and information security improvements, and knowing whether the business is being transparent and direct about the incident while providing consumers with enough information and resources to protect themselves.

From a consumer perspective, questions that often arise include:

- Why do you have — or still have — my information?
- What specific information of mine was involved?
- Am I the victim of identity theft or other crime?
- What do I need to do?

- Can you delete my information?

From a regulator perspective, the focus is often on the following:

- Why did it take so long to provide notice?
- What security safeguards were in place before the incident?
- What changes has the business made to prevent the incident from recurring?

While the answers to some of the questions above are often included in breach notices at a high level, businesses should consider whether it is prudent to answer these questions more fulsomely, both in the breach notice and in prepared communication plans, e.g., FAQs.

For example, businesses should consider disclosing facts that would help consumers reach the conclusion that simply receiving a breach notification letter does not mean that the consumer is, or ever will be, the victim of identity theft.

For example, did the business conduct any dark web monitoring to confirm that exfiltrated data was not leaked? Did the business pay a ransom and receive assurance from the threat actor that data will not be further disclosed? Was there no evidence of data exfiltration?

Assuming these steps were taken, disclosing them in a breach notice may go a long way in addressing the questions on most consumers' minds. These statements, however, should not be drafted to steer the consumer away from taking certain precautionary steps, such as signing up for credit monitoring.

It is easy to make statements quelling consumers' concerns that at the same time may trigger regulatory scrutiny. It is, therefore, important to strike an appropriate balance.

Ultimately, consumers should always be encouraged to take steps to protect their personal information, and it should be up to consumers to decide whether there is no risk based on the facts.

Likewise, a few sentences explaining the timeline from the discovery of the incident to the date of notifications may alleviate regulators' timing concerns if this information is provided upfront.

For example, if data mining was a step taken as part of the response, explaining that a third-party vendor was hired to assist with determining the affected population may provide regulators with comfort as it is expected that this process will take time, and the business is taking the requisite steps to determine the nature and scope of the population requiring notification.

Businesses may also benefit from a statement indicating that at the time of discovery there was just not enough information to provide notifications. Time is needed to conduct the investigation, to determine whether notification is required, and, if so, to whom.

When appropriate, businesses may also want to consider the benefit of talking to regulators early and often, rather than waiting for the dreaded follow-up.

2. Consider the business, products and services at issue.

One question that consumers always ask is: "Why do you have — or still have — my information?"

This question highlights the need for businesses to begin breach notification letters with an explanation about the business and the products and services it provides.

For example, if you are a business that consumers are not likely to remember conducting any transactions with — e.g., a third-party service provider that has agreed to provide notice on behalf of another organization — explaining your relationship with the consumer, and why you have the consumer's information, is critical.

Having a good privacy policy businesses can point back to that explains what data is collected and for what purposes would help.

Even for businesses that have a direct relationship, consider the personal information involved in the incident and explain the context around why the personal information was properly collected. For example, if you're a retailer, why do you have a consumer's passport information? Perhaps it was collected in the context of a return and collected for identification purposes.

Explaining why the affected business has the information at issue reduces the number of individuals contacting the call center, and may provide a sense of relief and trust to the letter recipient.

This is also beneficial from a regulatory perspective and it likely will result in a reduced number of consumers contacting their attorney general's office to complain.

3. Exercise caution when making statements about the organization's information security posture.

The California Consumer Privacy Act, which soon will be significantly modified by the California Privacy Rights Act, allows consumers to bring an action for statutory damages in the event of a data breach due to a business's failure to implement reasonable security procedures.

However, before bringing an action, the consumer must provide the business with 30 days' written notice identifying the specific violation. If the business cures the noticed violation and provides the consumer a written statement indicating such, statutory damages are not available.

What qualifies as a cure remains unclear, but businesses should give careful thought to their breach notice as well as the written response.

On one hand, if a business believes that reasonable security procedures are intact, the business's breach notice, written response and actions should communicate this message consistently.

Statements concerning the health of the business's security environment in a breach notice — e.g., "we apologize that our security procedures did not meet your expectations" — or any changes to existing security procedures in the event of a breach will be a double-edged sword, so businesses should take caution.

On the other hand, if a business believes that heightened data security procedures are warranted, it would be wise to frame these steps — to the extent factually accurate — as steps the business is taking as part of its ongoing assessment of its information security program.

In other words, the changes should not be worded to suggest that certain safeguards or controls were previously lacking. Indeed, cybersecurity is a rapidly moving target, and thus consumers and regulators should expect to see such changes, especially after a data security incident.

4. Prioritize user-friendliness and tone.

If you have been tracking what's been happening in California concerning the CCPA and related enforcement efforts, you may know that there is increased attention on the manner in which information is conveyed to consumers.

The use of headers, bullets and bolded font especially with respect to the "what you can do" section, may help achieve this goal.

Businesses should also consider the demographics of their audience, including their ages and locale. For less technically savvy audiences, avoiding unnecessary legal or technical jargon is important to ensure the message does not get lost in translation,

Businesses should also involve the internal communications team in the drafting process to ensure that the tone of the notification matches the business's day-to-day messaging style. A breach notice that takes a sharp turn from standard messaging may trigger unnecessary fear or come off as disingenuous.

Public relations firms may be especially helpful in this context as they can provide honest feedback, from an outsider's perspective, how certain messaging may be received and what narratives may not work for the organization.

The consumer notification process should not be treated as a check-the-box exercise. Notification is a step in the incident response process businesses would be wise to use to minimize the incident's impact on the organization.

Kamran Salour is a partner at Troutman Pepper.

Ronald Raether is a partner and leads the privacy and cyber team at the firm.

Sadia Mirza is an associate at the firm.

Troutman Pepper partner Tambry Bradford contributed to this article.