GFELLER LAURIE LLP
ATTORNEYS AT LAW

The Insurability of Cyber and Privacy Fines

Vincent J. Vitkowsky

Connecticut New York New Jersey Massachusetts

The Insurability of Cyber and Privacy Fines

The question requiring a better answer. One of the most complex questions facing cyber insurers is whether fines and penalties for cyber and privacy-related violations are insurable. (For ease of reference, fines and penalties will be collectively referred to as "fines.") Almost every article and conference panel (remember those) addressing the insurability of fines in the U.S. concludes that "there is no clear answer." When the European Union's GDPR is involved, a frequent answer is that the question "must await court determination," presumably in whatever EU member state the relevant lead Supervisory Authority is based. But cyber underwriting and claims executives who are making real-time decisions need more guidance than that. They need a framework for analyzing and making informed decisions on the potential for coverage.

A multi-step process. To arrive at a decision requires a multi-step process, with the precise steps varying by context.

1. Review the policy language on point.
2. Identify the potentially-important factors.
3. Make the best possible assessment of what jurisdiction's law would apply to the issue if litigated.
4. Make the best possible assessment of the extent to which, if at all, that jurisdiction allows for insurability of fines.
5. Analyze the precise nature of the fine assessed and the specific violations that led to the fine.

Policy language. As always, the starting point is the policy language. After some early resistance in the market, many cyber policies will now attempt to provide a measure of coverage. Some common variations provide, in words or substance, as follows:

1. Fines are covered ***where insurable by law***;
2. fines are covered as long as the ***most favorable applicable law*** permits coverage; and
3. fines are covered except to the extent that the ***law of the jurisdiction imposing the fine*** forbids such coverage.

The third alternative allows you to skip a step, which is identifying the jurisdiction supplying controlling law. It is specified as the jurisdiction imposing the fine. But it does not answer the question of what the substantive law actually *is.* So it remains necessary conduct the analysis specified below in **Are Fines Insurable?**

If one of the other alternatives, or a similar alternative, is chosen, it becomes necessary to identify the following potentially-important factors.

Potentially-important factors.

- Which regulator imposed the fine?
- What nation or U.S. state would the reimbursement be paid into?
- What is the place of incorporation, domicile and principal place of business of the insured?
- What is the place of incorporation, regulatory domicile, and principal place of business of the insurer?
- Where is the place of contracting of the policy? Where was it brokered?
- What is the main situs (if any) of the underlying facts and circumstances?

A wild card. No authority that sheds light on how a clause calling for applying *the most favorable applicable law* may be applied. There is a split of thinking in the cyber insurance community. Some suggest that the insured may choose among any of the factors set forth above to identify the jurisdiction with the law most favorable to coverage. To this author, that is untenable. Instead, a court would apply the factors above in a choice-of law analysis. Thus, the parties should proceed to the next step, and identify what jurisdictions plausibly might apply.

What jurisdiction's law applies? Ultimately, the insurability of regulatory fines in the U.S. is a function of individual state law. This is so even if the fine arises from a federal agency such as the Federal Trade Commission or the Department of Health and Human Services, or the EU regulators. Many states also assess fines under their own statutes and regulations. The issue has come into particularly sharp focus with the EU's GDPR, and then acutely so with the recent enactments of rigorous requirements in New York's Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act") and the California Consumer Privacy Act.

If the cyber policy has a choice-of-law provision, it will almost always be enforced. If there is no choice-of-law provision, a court would use the choice-of-law test of the state in which it is located to identify the governing law. The tests include:

1. the most significant relationship test (applied in, among other states, Connecticut, Delaware, Illinois, Massachusetts, New Jersey, New York and Texas);
2. the place of contract test (applied in, among other states, Florida and Michigan);
3. the government interest test (California); and
4. several alternative tests, some of which are unique and others of which combine elements of the other tests.

If the analysis yields a clear answer, and it rarely does, it will identify the state's law which would be applied in a clause covering fines *where insurable by law*. But if more than one state's law might plausibly be applied, the parties should take that uncertainty into effect in evaluating whether the fine is *insurable by law*. Alternatively, if the policy calls for using the *most favorable applicable law*, the parties can make a selection from among the potentially larger pool of jurisdictions whose law might apply.

Are fines insurable? Once the choice-of-law analysis is concluded and the actual or potential governing jurisdictions are identified, the question of insurability can finally be addressed. Most of the uncertainty lies here. Many states might start by examining the insurability of punitive damages. There is a broad range of outcomes, mixing considerations of public policy and insurance policy language, into what is best described as an incoherent mix with at least four variations.

Similarly, several states have addressed whether regulatory fines are insurable. Some inquire whether the fines are "punitive" in nature. Some take broad, indiscriminate approaches. Some try to slice differences thinly. Any attempt to summarize them would be useless in the abstract. Careful research would reveal that even within a single state, case results can leave room for argument. It is thus necessary to examine the specific state and the specific violation.

What was the nature of the specific fine? What standards are identified in the relevant statute or regulations? What categories of monetary assessments can be made? What if anything is said about the nature of the fine in the order or ruling imposing the fine?

What was the violation? As a practical matter, the greater the degree of culpable conduct by the insured, the more likely the insurability of the fine would be improper. This is certainly true if the order or ruling imposing the fine contains language critical of the insured's conduct, though most do not. Even if the order or ruling does not, the apparent degree of culpability may affect the court's view of the nature of the violation.

The analysis should consider the broad range of conduct that might give rise to a fine. One end of the spectrum would include violations such as (1) a flagrant failure by a corporation's officers and directors to address cyber vulnerabilities in the face of specific warnings from the IT team, or (2) intentional business practices which violate data handling requirements for profit or otherwise. On the other end, some breaches arise from conduct that was merely negligent, or fairly considered, not negligent at all. An example would be a breach resulting from a nation-state attack utilizing a zero-day vulnerability.

Another wild card. As a final complication, it is possible that a court called upon to apply the law of another state might not apply the other state's law if the result would be inconsistent with the public policy of the court's own state. For example, it might not enforce provisions calling for application of the insurability of fines under the *most favorable applicable law.*

Deep diving required. There is absolutely no substitute for a deep dive. Following the process described above may not provide perfect clarity, but it will often provide enough guidance to allow the insurer to make an informed and reasonable decision.

A note on the position under the GDPR in the U.K. When the fine is imposed under the GDPR regime, the same considerations exist. The fact that the fine is imposed by an EU regulator does not necessarily determine whether a given insurer may reimburse a given insured, both of which are located in the U.S.

That is not to say that the EU member's law is irrelevant. It may be a factor in the analysis.

However, the position in the UK warrants discussion for several reasons. First, many U.S. insurers also have operations in the U.K., and could be subject to regulatory pressures there. Further, many leading companies from the U.S. and elsewhere have based their GDPR controller or processor in the U.K., thereby making their lead Supervisory Authority the U.K. Information Commissioner's Office ("ICO"). The ICO has declined to state a position on the insurability of fines, saying that a "focus on insurance rather misses the point," because the emphasis should be on compliance and security. This leaves companies to seek guidance from limited analogous case law, again in non-cyber contexts.

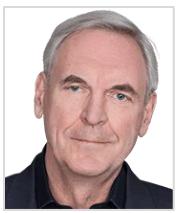
The basic position. Many of the leading English law firms have concluded, with variations in formulation, that there is a huge degree of uncertainty over insurability. Others flatly say that ICO fines for GDPR violations are probably uninsurable under English law. However, there may be a gray area.

The gray area. Some leading English law firms suggest that if the violation is totally innocent, there may be grounds to argue for insurability. This is because English cases recognize that some acts, although falling short of a crime, reflect an element of "moral turpitude" or "quasi-criminal" conduct which should be deterred or punished. Where that element is present, it weighs against insurability. Thus, if there is intentional bad conduct, the argument against insurability is stronger.

On the other hand, if the fine arose from conduct that was merely negligent or, fairly considered, not negligent at all, a substantial argument in favor of insurability could be made.

Impact of Brexit. A word should be said about whether Brexit has an effect on the analysis. The short answer is that it has no immediate effect. Under the terms of the Brexit arrangement as negotiated, the rest of 2020 is a transition period, in which EU rules will continue to apply in the U.K., and a new data protection arrangement will be negotiated later. With the onset of the COVID-19 pandemic, one would suspect the time period to be extended.

July 28, 2020



Vince Vitkowsky is a partner in Gfeller Laurie LLP, resident in New York. He focuses on cyber risks, liabilities, insurance, and litigation. Vince assists insurers and reinsurers in product development, and in all aspects of coverage evaluation and dispute resolution in many lines of business, including cyber, CGL, property, and professional liability. He also assists in complex claim evaluations, and if necessary, the defense of insureds in complex matters.
vvitkowsky@gllawgroup.com
www.gllawgroup.com