Data Breach Enforcement On Both Sides of the Atlantic: Revealing Mechanics of Fines and Civil Penalties and Reinforcing Importance of Training

March 3, 2021

Three data breach enforcement examples, two under the GDPR and one in the U.S., highlight differences across the Atlantic in the mechanics of fines and civil penalties, including how and when to seek reductions, and the importance of data privacy training as a mitigation measure. This article was written in partnership with **Dr. Carolin Raspé of Hengeler Mueller**.

In November 2019, Germany's Federal Commissioner for Data Protection and Freedom of Information (BfDI) imposed a fine of 9.6 million euros ($11.3 million) against a German telecommunication service provider for poor customer authentication; at the time the second-largest GDPR fine in Germany. The German service provider appealed the decision and on November 11, 2020 a **district court in Bonn** reduced the fine to 900,000 euros ($1 million). Both BfDI and service provider claim this decision to be a victory. On the one hand, BfDI pointed out that the decision affirmed "that privacy infringements have consequences […] No company can afford to neglect data protection any longer." The court confirmed BfDI's assessment that a call center's request for the name and date of birth of a customer to verify their identity, and to provide the customer with additional contract information, constituted a breach of Art. 32 GDPR. **The service provider**, on the other hand, highlighted that the court found its violation minor, non-intentional, and not deserving of a fine in the millions, especially because there was never a risk of a mass release of data. Both parties have accepted the decision, which has become final.

The next month, Ireland's Data Protection Commission (IDPC) **fined** Twitter International Company ("Twitter") 450,000 euros ($545,000) arising out of a software bug that exposed nearly 90,000 European users' private tweets. The IDPC found that Twitter failed to meet the 72 hour data breach notification requirement under Art. 33(1) owing to a thirteen-day delay between notice of a bug report by a Twitter contractor on December 26, 2018 and internal notice of the bug to Twitter's data protection officer on January 8, 2019. The IDPC found that Twitter's incident response process had failed to adequately escalate the issue to the DPO despite flagging the incident as a privacy issue during its triage of the incident, the IDPC found Twitter's claims that the incident did not reach the DPO because it had been deemed "low risk" unavailing. The IDPC also found that Twitter failed to document the breach adequately under Art. 33(5) which delayed the investigation. While the IDPC had initially proposed a fine one-third to one-half the size of the final amount, objections from eight other countries' data protection authorities led to a first-of-its-kind European Data Protection Board review and **decision under Art. 65** resulting in a nine-month extension to the investigation and an increase in the fine amount.

These decisions from Europe offer important lessons for incident management:

- Violations by employees at any level of the company can lead to fines. The court in Germany confirmed that – other than for criminal fines – the GDPR does not require the violation to be committed by a manager of a company to hold a company responsible; rather, the misdeeds of any ordinary employee can trigger significant fines. Similarly, the IDPC found that Twitter failed to properly manage its incident response from the initial intake and triage process, preventing senior employees from recognizing the significance of the issue within the data breach notification timing requirements.

- Companies should review and reinforce security training. The court in Germany and the IDPC in Twitter both pointed to failures in company practices that should have been addressed through better training, consistent with GDPR. As a result, companies should ensure that every employee is trained for data privacy awareness and companies should be aware that with every new decision on GDPR, arguments that a company was not aware that its practices violated the GDPR as a mitigating factor will become harder to make and less likely to prevail as precedent clarifies reasonable security measures.

- GDPR fines are not always final and there are several avenues for fine and penalty modification. Companies should carefully review findings to consider appeals to reduce fines as in the German case while also realizing that other data protection authorities may invoke EDPB review to increase fines issued by a company's principal European data protection regulator. In the German case, the court found that the violation was only minor in nature and therefore the fine was inadequate: It was a single incident and no mass data loss was to be expected, the employee acted unintentionally, one data subject was knowingly harmed, no sensitive data (*cf.* Art 9 GDPR) was released, and was the first data protection infringement of the German service provider which had fully cooperated with the investigation. By contrast, in Twitter, the EDPB found that the information was more sensitive than the IDPC had determined in its initial decision, resulting in an increase in the fine amount.

On this side of the Atlantic, this December, New York Attorney General Letitia James announced a $2 million settlement agreement with online retailer CafePress in connection with a 2019 data breach that compromised the personal information of approximately 22 million consumers. An immediate payment of $750,000 will be divided among the coalition of seven states who brought the investigation. It was nearly six months after the intrusion, and five months after learning of the vulnerability, before CafePress conducted a full investigation into the breach and finally notified customers. According to the Attorney General, the settlement reflects CafePress's failure to protect consumers as well as a failure to take immediate action upon learning of the privacy vulnerability.

In the press release, Attorney General James stated that her office will "use every available tool to hold companies accountable when they fail to safeguard personal information." In addition to the monetary settlement, CafePress will also be required to implement a series of improvements designed to protect consumer personal information from future cyberattacks. These improvements include not only required training for management-level employees who will be responsible for implementing a new information security program, but also plans to ensure that training measures are in place for other areas of the organization, like incident response and data breach notification.

This settlement is the latest among a series of recent multi-state cybersecurity investigations conducted by state attorneys general, which companies should take note of. Each settlement required not only a significant monetary payout, but also a series of security changes to protect consumers. This provides companies with an opportunity to consider reviewing their current programs against the security measures set forth in these settlements in order to buttress their own security protocols and mitigate the risks associated with the type of data breaches that launched these multi-state investigations.

Unlike the German case, in which the company retained an avenue to reduce their penalties, these multi-state investigations and consensual settlements are more common in the U.S. Therefore, companies will need to try to negotiate up front the appropriate fine amount as an appeal will likely be unavailable. But the need to negotiate settlements with multiple U.S. states presents complexities also seen in the EDPB's involvement in the Twitter decision—companies need to recognize that security incidents have no regard

for borders and every affected jurisdiction is likely to have an opinion on the appropriate remedy, which will need to be negotiated to reach a final resolution.

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your usual Davis Polk contact.

Frank J. Azzopardi	+1 212 450 6277	**frank.azzopardi@davispolk.com**
Robert A. Cohen	+1 202 962 7047	**robert.cohen@davispolk.com**
Pritesh P. Shah	+1 212 450 4147	**pritesh.shah@davispolk.com**
Matthew J. Bacal	+1 212 450 4790	**matthew.bacal@davispolk.com**
Daniel F. Forester	+1 212 450 3072	**daniel.forester@davispolk.com**
Matthew A. Kelly	+1 212 450 4903	**matthew.kelly@davispolk.com**
Will Schildknecht	+1 212 450 3557	**will.schildknecht@davispolk.com**
Jennifer Kim	+1 650 752 2027	**jennifer.kim@davispolk.com**