FINNIUS

FACT SHEET | as of November 16, 2026

Cyber incident at your financial institution

Four practical tips from a financial regulatory view

Cyberattacks are a daily occurrence

Cyberattacks are one of the **most acute systemic risks** facing the financial sector. The AFM also states this in Trend Monitor 2027. They are constantly in the news: hacks on crypto platforms, DDoS attacks on payment service providers, and data breaches at partners of major banks. A hack or system failure can lead to **stolen customer data**, **financial losses**, **reputational damage,** and **critical questions from regulatory authorities**.

Finnius regularly assists financial institutions dealing with cyber incidents. We would like to share **four practical tips** for handling cyber incidents correctly and effectively to avoid regulatory consequences.

DORA: initial report within 4 hours

Under the Digital Operational Resilience Act (DORA), **IT incidents** must be **immediately documented and classified**. Serious IT incidents must be reported to the regulator as soon as possible and reported regularly:

4 hours	24 hours	72 hours	1 month
initial notification after classification	no later than 24 hours upon detection	Interim report	final report

Does a serious IT incident affect **customers' financial interests?** If so, you must inform the customers without undue delay.

Separate reporting requirement

A cyber incident may also be a reportable incident within the meaning of the Bpr/BGfo: conduct or an event that poses a serious threat to the integrity of the company's operations. An incident must be reported to the regulatory authority without undue delay. Failure to report an incident or reporting too late constitutes a violation in and of itself.

Does the substance of the reportable incident "fully overlap" with a major ICT-related incident under DORA? If yes, you only need to report it under DORA.

Does the overlap no longer apply? For example, because there is more at stake than just a cyberattack, or because compliance with regulatory requirements is at risk? In that case, reassess whether a separate Bpr/BGfo reporting requirement occurs.

Business Continuity

A cyberattack can cause significant **damage to your financial institution** - for example, due to investigation and recovery costs, customer attrition, or restrictions on daily operations, or even a temporary shutdown.

Therefore, **monitor** the **business continuity thresholds** and any additional thresholds relevant to the cyber incident, as set forth in your financial institution's business continuity policy.

Take appropriate measures when thresholds are at risk of being exceeded to ensure business continuity.

Customer complaints and claims

A data breach is often followed by **complaints or (claim) letters** from customers or their representatives.

Your initial response often determines the financial institution's position moving forward. Therefore, do not react hastily. Involve an advisor early on to assess liability risks and align communication with customers with the reports submitted to the AFM/DNB and, in the case of stolen personal data, the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*).

We're here to help. At Finnius, we advise financial institutions on cyber incidents and related reporting obligations, communication with the AFM and DNB, and how to respond to customer complaints and/or claims. Please feel free to contact Laurens Hillen, Rick Sanders, or Joris Viellevoije.



Laurens Hillen
laurens.hillen@finnius.com
M: +31 (0)6 216 637 76



Rick Sanders
rick.sanders@finnius.com
M: +31 (0)6 226 307 63



Joris Viellevoije
joris.viellevoije@finnius.com
M: +31 (0)6 151 160 35

This fact sheet contains general information and does not constitute legal advice. | © Finnius advocaten | finnius.com