Instant Actions launches shareholder identity disclosure service

10 September 2020

London, United Kingdom — Instant Actions today announced that it has released a ready-to-implement solution to address the data risks created by the Shareholder Rights Directive II (SRD2).

A new authentication service has been launched to head off what it sees as a major threat to intermediaries and shareholders posed by the recently introduced Shareholder Rights Directive II (SRD2).

From 4th September 2020, under SRD2, firms providing share custody are obliged to disclose client identities and positions when requested to do so by issuers.

Explains James Zorab, CEO of Instant Actions: 'Intermediaries can now mitigate against potentially catastrophic reputational and financial risk. Who owns a company is valuable information. Plenty of stock traders watch the activity of company insiders and major institutional shareholders, while investment banks have thrived on intermediating information about shareholders. Securities borrowing desks depend on brokers knowing who owns what so they can source the stock. Which is why the well-informed pore over stock ownership disclosure forms, looking for information on which to trade.

‘It will therefore come as no surprise if unauthorized phishing becomes prevalent on the back of ostensibly legitimate requests for shareholder identity disclosure. We have found ways to protect intermediaries from that threat.’

The new service, created by Instant Actions which provides globally verifiable company announcement information to the markets, protects intermediaries and shareholders from the risk of unauthorized phishing of their data by authenticating both the validity and identity of the requestor. Once authenticated the intermediary places the requested shareholder data in a secure, GDPR compliant Data Safe Haven ready for the issuer to retrieve.

Adds Zorab: ‘While well-intentioned, the legislation does not sufficiently address the issues of confidentiality, secure communication or the control of this data and so could give rise to the possibility of phishing and fraud. At its worst, firms could be exposed to data breaches on an epic scale.

‘There is a very real risk of bad actors masquerading as issuers and obtaining highly sensitive shareholder data. The financial consequences of this could be very significant but the reputational impact could be crippling for businesses. We were shocked to learn that some intermediaries were planning on communicating this highly sensitive data un-encrypted and by email. Our solution provides a secure, auditable way of locking out those bad actors.’

SRD2 requires firms to respond with shareholder data within 24 hours, a very short time to allow them to check that the request has come from a legitimate source, particularly when the request may have been forwarded to them and has not therefore come direct from the original issuer.

As a result, the best a financial intermediary can do is to check with the firm above them in the chain of communication that they have carried out their own validation checks. Adds Zorab: ‘What happens if the data is inadvertently disclosed? Whose fault will it be? Who will be liable? And how will disputes be resolved?’

SRD2 refers to ‘appropriate’ security defences and insists that firms should check whether the request has originated from the issuer. But it does not explain how this should be done, nor does it recognize that such a seismic change in industry workflows might require secure counterparty communications that simply don’t exist today.

And as Zorab points out, GDPR complicates the risk: ‘How will firms simultaneously satisfy their obligations to disclose data under SRD2 and seek customer consent to keep data private under GDPR? If they get it wrong, they face fines of up to €5m for SRD2 and up to €400m or 4% of turnover for GDPR.’

Instant Actions can take in and authenticate identity disclosure requests in any form, including the new ISO standardized messages Seev 45-49 developed by SWIFT. SWIFT messages are perfectly secure for point to point communications and adequately prove the source of origin, but they do nothing to prove whether the reply address has been changed, as would be the case in a phishing attack, if these messages are forwarded on to the next intermediary in the chain. This obligation to forward requests onwards through the chain is a specific requirement set out clearly in the directive with which intermediaries are obliged to comply.

About Instant Actions Solution for SRD2
https://instant-actions.com/srd2

For information about Instant Actions please contact
enquiries@instant-actions.com

For further press information please contact Matthew Barnett on
matthew.barnett@instant-actions.com