



D&O/E&O INSURANCE COVERAGE FOR NETWORK SECURITY EVENTS

FREQUENTLY ASKED QUESTIONS

ICI Mutual has introduced a new “Network Security Event Endorsement” under its Directors and Officers/Errors and Omissions Liability Insurance Policy (“ICI Mutual Policy”). The new endorsement is designed to specify the scope of coverage available under the ICI Mutual Policy for losses that may be incurred by insureds in connection with network security incidents that result in disruption to, or interference with, the ability of insured entities to conduct advisory, shareholder servicing, or other day-to-day investment management operations. The new endorsement is designed to complement ICI Mutual’s existing “Shareholder Data Breach Event Endorsement.”

ICI Mutual’s new Network Security Event Endorsement will be provided to insureds at no additional premium. This guide is designed to respond to frequently asked questions regarding this new ICI Mutual endorsement.¹

1. Why is ICI Mutual introducing its new Network Security Event Endorsement?

A number of events—including a number of highly-publicized cyber incidents outside the fund industry—have fueled increased attention by regulators, fund boards and fund advisers to cyber risks within the fund industry, and to programs in place at fund groups to manage these risks. For the fund industry, two key cyber risks are the “shareholder data breach event” and the “network security event.” Not surprisingly, many fund groups (1) have been seeking guidance as to how their directors and officers/errors and omissions (D&O/E&O) liability insurance policies and other “traditional” business insurance policies may respond to these two cyber risks, and (2) have been evaluating whether to buttress their cyber risk management programs through the purchase of stand-alone “specialty” cyber insurance products.

ICI Mutual previously introduced an endorsement that is designed to specify the scope of coverage available under the ICI Mutual Policy for losses associated with the first of these cyber risks—i.e., the Shareholder Data Breach Event.² ICI Mutual is now introducing a new endorsement that is

¹ These Frequently Asked Questions (FAQs) provide an overview of the new endorsement and a general discussion of the coverage available thereunder. In any particular situation, the terms, conditions and limitations of the endorsement itself (as well as any other applicable terms, conditions and limitations of the ICI Mutual Policy) will govern any coverage questions that may arise. The capitalized terms used in these FAQs are defined either in the endorsement itself or in Section III of the ICI Mutual Policy.

² A Shareholder Data Breach Event can be broadly viewed as an incident in which the security or confidentiality of data is compromised, so as to result in the unauthorized acquisition or unauthorized dissemination of confidential information regarding fund shareholders (e.g., shareholder names, account numbers, social security or tax identification numbers). For more information on ICI Mutual’s “Shareholder Data Breach Event Endorsement,” please see “D&O/E&O Insurance Coverage for Shareholder Data Breach Events—Frequently Asked Questions,” at

designed to specify the scope of coverage available under the ICI Mutual Policy for losses associated with the second of these risks—i.e., the Network Security Event.

Broadly stated, a Network Security Event can be viewed as an incident that (1) affects the confidentiality, integrity, and/or availability of an insured entity’s internal computer systems (or of external computer systems operated by outside service providers to the insured entity), and (2) results in disruption to, or interference with, advisory, shareholder servicing, or other day-to-day investment management operations. Network Security Events may be associated with cyberattacks. But as the definition of “Network Security Event” in ICI Mutual’s new endorsement makes clear, such events may result from other causes as well (e.g., natural disasters).

As discussed in Question No. 2 below, the scope of coverage provided for losses associated with Network Security Events is not expressly addressed under the D&O/E&O policies now generally available to fund groups. ICI Mutual has developed its new endorsement to provide more certainty for its insured fund groups in this regard, and to reduce the potential for future misunderstandings or conflicting expectations as to the scope of coverage available under the ICI Mutual Policy for this type of cyber risk.

2. Are losses resulting from Network Security Events covered under current D&O/E&O policies?

The D&O/E&O policies now generally available to fund groups—whether issued by commercial insurers or by ICI Mutual—were originally developed prior to the emergence of cyber risk as a key area of concern for fund groups. At present, these D&O/E&O policies typically do *not* directly address the scope of insurance coverage available for financial exposures in claims arising from Network Security Events. Accordingly, there remains some uncertainty as to how D&O/E&O policies might respond to various of these financial exposures.³

ICI Mutual’s new endorsement is designed to address this uncertainty. By specifically describing the scope of coverage available on a prospective basis under the ICI Mutual Policy for Claims

<http://www.icimutual.com/sites/default/files/Shareholder%20Data%20Breach%20Event%20Endorsement%20FAQ%20June15.pdf>.

³ Thus, for example, and separate and apart from any specific exclusions that may be included in particular D&O/E&O policy forms, there may be issues—particularly with regard to E&O coverage—as to whether particular claims resulting from a particular Network Security Event fall within the overall grant of coverage afforded by the policy. See generally Latham & Watkins, *Cyber Insurance: A Last Line of Defense When Technology Fails* (April 15, 2014), <http://www.lw.com/thoughtLeadership/lw-cybersecurity-insurance-policy-coverage> (“E&O coverage for a cyber incident requires that the insured be able to show some sort of nexus between the cyber issue and the professional services in which the insured is engaged.”); cf., Michael Born, *The Law Firm Cyber Landscape—A Look at Emerging Exposures and Solutions* (May 2015) at p. 7, http://www.lockton.com/whitepapers/Born_Cyber_Exposures_for_Law_Firms_May15-lr.pdf (suggesting that network security liability claims are “unlikely to be covered” under lawyers professional liability insurance policies, “but claims by clients alleging breach of professional duty might trigger coverage”); Laura E. Bange & Amy Lock, *Insurability of HIPAA Claims Arising from Health Information Data Breaches Under Traditional E&O and D&O*, PLUS Journal (July 2014) (noting that “with respect to E&O policies insuring professionals, whether an alleged breach arises in the course of an insured’s performance of ‘professional services’ will be carefully examined”).

arising from Network Security Events, the new endorsement provides more certainty and guidance for fund groups. The new endorsement also thereby reduces the potential for misunderstandings or conflicting expectations between ICI Mutual and its insureds as to how the ICI Mutual Policy may respond to such Claims.

3. Is ICI Mutual’s new endorsement a substitute for specialty cyber insurance coverage?

Numerous “specialty” cyber insurance products are now available for purchase in the commercial insurance market. These specialty products—which are typically issued on a stand-alone basis—are often expressly designed to respond to an array of cyber-related exposures (including certain Network Security Event-related exposures) that are outside the traditional scope of D&O/E&O insurance. ICI Mutual’s new endorsement is neither designed nor priced to serve as a substitute for such specialty cyber insurance products. In particular, the new endorsement will not respond to certain Network Security Event-related exposures for which coverage may be afforded under specialty cyber insurance products (see Question Nos. 7 and 10 below).

In ICI Mutual’s view, deciding whether to purchase a specialty cyber insurance product involves a business judgment on which different fund groups may come to different determinations, depending upon their particular circumstances. This being said, ICI Mutual expects that many fund groups will choose to purchase specialty cyber insurance products, although some may not.

4. What is the basic design of ICI Mutual’s new endorsement?

The new endorsement is designed as an analogue to ICI Mutual’s existing Shareholder Data Breach Event Endorsement. The two endorsements are similarly structured, and share certain provisions in common.⁴ As in the Shareholder Data Breach Event Endorsement, the new Network Security Event Endorsement (1) divides into categories the types of Claims that might potentially be initiated in the aftermath of such an event, and (2) for each of these categories of Claims, sets forth the extent of coverage available for different subsets of Insureds.

The new endorsement divides the types of Claims that might potentially be initiated in the aftermath of a Network Security Event into two basic categories:

- (1) ***Traditional Claims (a/k/a “Securities Claims”)***: The first category comprises those types of Claims which have been relatively common in the fund industry over the years, and to which fund industry D&O/E&O insurance has traditionally been specifically designed and actuarially priced to respond (e.g., shareholder lawsuits alleging violations of federal or state

⁴ Thus, for example, as in the Shareholder Data Breach Event Endorsement, the new Network Security Event Endorsement includes provisions that specify that a Claim to which coverage is extended under the endorsement will be deemed *not* to arise out of or involve actual or alleged “invasion of privacy,” “emotional distress,” “mental anguish,” or “loss or damage to any tangible property” for purposes of the application of certain exclusions in the ICI Mutual Policy. ICI Mutual recognizes that these particular exclusions may be of lesser relevance in the context of Claims arising out of Network Security Events than in the context of Claims arising out of Shareholder Data Breach Events. Nevertheless, given the limited claims experience to date with Claims arising from Network Security Events (either inside or outside the fund industry), ICI Mutual has determined it appropriate to “mirror” certain provisions in both endorsements, if only to reduce the potential for misunderstandings or conflicting expectations in the future.

securities laws, shareholder derivative lawsuits alleging breaches of fiduciary duty, investigations or regulatory actions by the U.S. Securities and Exchange Commission).

- (2) ***Non-Traditional Claims:*** The second category comprises those types of Claims which are not traditional, but which might, at least in theory, be brought in the aftermath of certain types of Network Security Events (e.g., lawsuits by outside service providers or business partners of a fund group charging that the providers or business partners sustained harm as a result of a cyberattack affecting the fund group’s computer systems).⁵ Fund industry D&O/E&O insurance has traditionally been neither specifically designed nor actuarially priced to respond to such Non-Traditional Claims.

For each of these two categories of Claims, the new endorsement sets forth the extent of coverage available under the ICI Mutual Policy (a) for *fund independent directors*, (b) for *insured funds themselves* (and their “inside” directors and officers), and (c) for *insured advisers and other insured service providers* (and their directors and officers). More detailed information as to the nature and extent of coverage available under the endorsement for each category of insured for each category is provided at Question Nos. 5 through 8 below. In summary form, however, the coverage afforded under the standard version of the endorsement can be diagrammed as follows:

⁵ At least in theory, outside service providers or business partners who allege that they have been damaged by a fund group’s inadequate or negligent cybersecurity measures (e.g., by a fund group’s inadvertent transmission of malicious code) might seek to pursue recovery through litigation under one or more legal theories. While certain commentators have explored the potential for liability in this area, there appears, as yet, to be little actual claims experience, either inside or outside the fund industry, from which to assess how viable such theories (particularly tort-based theories) might prove to be. *See generally* Paul Rosenzweig, “When Companies Are Hacked, Customers Bear the Brunt,” *New Republic* (Oct. 15, 2013) (“Legal developments in this area [i.e., a common law doctrine of tort liability for consequential damages caused by inadequate or negligent cybersecurity measures] are hesitant and incomplete”); *Critical Information Infrastructure Protection and the Law: An Overview of Key Issues* (The National Academies Press) (2003), at Chapter 3 (“Liability for Unsecured Systems and Networks”) (“Although tort-based liability with regard to CIP [critical infrastructure protection] is not well developed at present, many experts believe that a few CIP-related liability suits could change the cost-benefit analysis of securing critical infrastructures”); Eardley P. Grant, “System Security Liability,” *SANS Institute* (2004), at p. 4 (noting that “the applicability of downstream liability has not yet as yet been reviewed in the courts in any meaningful way.”)

Given the dearth of actual claims experience, there also remains uncertainty as to how, if at all, D&O/E&O insurance might respond to this type of “non-traditional” litigation. Absent clear precedents to the contrary, D&O/E&O insurers might be expected to take the position that coverage for such lawsuits should generally be precluded, whether by reason of (1) “breach of contract” exclusions or similar provisions in existing D&O/E&O policies (see Question No. 10), (2) a lack of a sufficient nexus between such lawsuits and an insured’s “professional services” (see note 3 above), and/or (3) other exclusions or provisions.

**Network Security Event Claims
Availability of Coverage under New ICI Mutual Endorsement (1)**

	Coverage For Traditional (a/k/a “Securities”) Claims (Defense Costs, Settlements, Judgments)	Coverage for Non-Traditional Claims (Defense Costs, Settlements, Judgments)
Fund Independent Directors	Yes	Yes
Insured Funds (And Their “Inside” Directors and Officers)	Yes	Yes (Subject to Sublimit on Settlements) (2)
Insured Advisers/Insured Service Providers (And Their Directors and Officers)	Yes	No (3)

- (1) This diagram is provided for general guidance only. The terms, conditions and limitations of the endorsement itself (as well as any other applicable terms, conditions and limitations of the ICI Mutual Policy) will govern any coverage questions that may arise in any particular situation.
- (2) Under the endorsement, coverage for Funds is subject to a per-Policy sublimit (typically, \$2 million) for payments made in settlements of otherwise covered Non-Traditional Claims. (Note that this sublimit does *not* apply to defense costs or judgments paid by Funds in otherwise covered Non-Traditional Claims.)
- (3) Under the endorsement, no coverage is potentially available for defense costs, settlements or judgments incurred by insured advisers or other insured service providers (and/or their directors and officers) in Non-Traditional Claims. See Question No. 7.

The ICI Mutual Policy is a third-party liability insurance product. As such, the ICI Mutual Policy, like D&O/E&O policies generally, is neither designed nor priced to cover First Party Costs arising from a Network Security Event (e.g., forensic investigations, temporary relocation expenses, public relations initiatives, lost business or lost revenues). The new endorsement underscores that no coverage is available under the ICI Mutual Policy, directly or indirectly, for such First Party Costs, subject to certain limited exceptions.⁶

5. What coverage is available under the new endorsement for Fund Independent Directors?

Traditional (a/k/a “Securities”) Claims: Independent Directors may be at risk of being named as defendants or respondents in Traditional Claims arising from Network Security Events (e.g., derivative lawsuits alleging breach of fiduciary duty in oversight of cyber risk, regulatory investigations by the U.S. Securities and Exchange Commission). Coverage is available under the endorsement both for Costs of Defense and for other covered Loss that Independent Directors may incur in connection with such Traditional Claims.

Non-Traditional Claims: In contrast to Traditional Claims, Independent Directors are likely to be at lesser risk of being named as defendants or respondents in Non-Traditional Claims (e.g., lawsuits brought by outside service providers or business partners to a fund group whose network has been compromised).⁷ Even so, coverage is available under the endorsement both for Costs of Defense and for other covered Loss that Independent Directors may incur in connection with otherwise covered Non-Traditional Claims.

First Party Costs: As noted above, the ICI Mutual Policy, like D&O/E&O policies generally, is a third-party liability insurance product. As such, it is neither designed nor priced to provide coverage, directly or indirectly, for First Party Costs. Because First Party Costs are typically an exposure for entities rather than for individuals, it appears unlikely that Independent Directors could themselves be held responsible for them. Even so, the endorsement extends special

⁶ These limited exceptions are described in the endorsement and in Question Nos. 5 and 6 below.

⁷ There is little, if any, precedent inside or outside the fund industry to gauge the viability of Non-Traditional Claims that might be brought in the aftermath of a Network Security Event, or to gauge the likelihood that any such Non-Traditional Claims could target fund independent directors. By analogy, however, recent experience outside the fund industry in claims involving a different type of cyber risk—i.e., large-scale data breaches of customer personally identifiable information (i.e., the analogue to the fund industry’s Shareholder Data Breach Event)—suggests that in such instances, *traditional* claims (e.g., derivative lawsuits) have been directed at directors or officers, but that *non-traditional* claims have to date generally been directed only at the entities involved in the data breaches and *not* at the individual directors (or officers) of these entities. *See, e.g., Palkan v. Homes*, 14-cv-1234, 2014 WL 5341880 (D.N.J. Oct. 20, 2014) (shareholders derivative suit brought against board of directors of Wyndham hotel operating company following data breach at Wyndham); *In re Target Corp. Customer Data Sec. Breach Litig.*, 309 F.R.D. 482,484-85 & n.1 (D. Minn. 2015) (consolidated cases following data breach at Target Corp. naming Target board of directors as defendants in only shareholder derivative suits and not with respect to other causes of action); *In re Home Depot, Inc. Shareholder Derivative Litigation*, No. 1:15-cv-02999-TWT (N.D. Ga. Jan. 20, 2016) (shareholder derivative suit brought against directors and officers of Home Depot following data breach at Home Depot stores; individuals not named in suits brought by Home Depot customers).

protection to Independent Directors in this regard. It does so by making coverage available for Independent Directors in the event that lawsuits (or other Claims) are brought against them seeking recovery of First Party Costs.

6. What coverage is available under the new endorsement for Insured Funds?

Traditional (a/k/a “Securities”) Claims: Although Funds do not themselves generally operate computer networks, they may nevertheless be at risk of being named as defendants (or respondents) in Traditional Claims arising from Network Security Events (e.g., disclosure-based class action lawsuits alleging violations of federal securities laws). Coverage is available under the endorsement for Costs of Defense and for other covered Loss incurred by Insured Funds in such Traditional Claims. This same scope of coverage is likewise available for “inside” directors and officers of Insured Funds.

Non-Traditional Claims: There is little, if any, precedent inside or outside the fund industry to gauge what types (if any) of Non-Traditional Claims might be brought in the aftermath of a Network Security Event, to gauge the viability of any such Non-Traditional Claims, or to gauge whether any such Non-Traditional Claims could target Funds as entities. In a rational world, one would expect that any Non-Traditional Claims arising from a Network Security Event should be primarily directed at the service providers that generally operate the computer networks that are compromised, rather than at Funds themselves.

The endorsement nevertheless recognizes the possibility that Funds, as entities, might conceivably be included as defendants (or respondents) in Non-Traditional Claims. In this regard, coverage is available under the endorsement for Costs of Defense that Insured Funds may incur in the defense of otherwise covered Non-Traditional Claims, as well as for insurable judgments that might be entered against them in such cases. The endorsement also provides specified coverage for amounts that Insured Funds may contribute towards *settlements* of otherwise covered Non-Traditional Claims, subject to a per-Policy sublimit (typically, \$2 million) on such contributions.⁸

First Party Costs: As noted above, the ICI Mutual Policy—like D&O/E&O policies generally—is neither designed nor priced to provide coverage, directly or indirectly, for First Party Costs (e.g., forensic investigations, temporary relocation expenses, public relations initiatives, lost business or

⁸ The endorsement thus recognizes that there could conceivably be instances where (1) Insured Funds are named as defendants or respondents in Non-Traditional Claims seeking insurable damages, (2) the Non-Traditional Claims are not dismissed during the litigation process, and (3) the parties ultimately seek to pursue monetary settlements in lieu of litigating the Non-Traditional Claims to final judgment. In such instances, Funds might expect that the cost of the monetary settlements should be borne by the entities that actually operated the computer networks at issue, rather than by Funds themselves. Even so, the endorsement provides specified coverage for amounts that Insured Funds may contribute towards insurable settlements of otherwise covered Non-Traditional Claims, subject to an overall per-Policy sublimit on such contributions. This per-Policy sublimit is designed to strike a balance between two competing interests: (1) the interest of Insured Funds in having some amount of insurance coverage available for them, so as to facilitate their resolutions of otherwise covered Non-Traditional Claims in appropriate cases, and (2) the interest of Insured Funds (and of the fund industry more generally) in not having so much insurance coverage available as to incentivize the plaintiffs’ bar (and other potential claimants) to view Funds as attractive “deep pocket” defendants in Non-Traditional Claims.

lost revenues). Accordingly, coverage is generally *not* available for any First Party Costs that might be incurred or payable by Insured Funds.⁹

7. What coverage is available under the new endorsement for Insured Advisers and other Insured Service Providers?

Traditional (a/k/a “Securities”) Claims: Insured advisers or other insured service providers (and/or their directors and officers) may be at risk of being named as defendants (or respondents) in Traditional Claims arising from a Network Security Event. Coverage is generally available under the endorsement for Costs of Defense and for other covered Loss that insured advisers and other insured service providers (and/or their directors or officers) may incur in such Traditional Claims (e.g., disclosure-based class actions alleging violations of the federal securities laws, regulatory investigations by the U.S. Securities and Exchange Commission).

Non-Traditional Claims: Coverage is *not* available for Costs of Defense or for other Loss that insured advisers and other insured affiliated service providers (and/or their directors or officers) may incur in Non-Traditional Claims arising from a Network Security Event. There is little, if any, precedent inside or outside the fund industry from which to gauge the likelihood of any such Claims being brought against insured advisers or other insured service providers in the aftermath of a Network Security Event, or the viability of any such Non-Traditional Claims. Fund groups interested in securing coverage for Non-Traditional Claims for their affiliated service providers may wish to explore the purchase of “specialty” cyber insurance products.

First Party Costs: As with Funds as entities (see Question No. 6 above), coverage is generally *not* available under the endorsement for any First Party Costs that insured advisers or other insured service providers (or their directors or officers) may incur, directly or indirectly.¹⁰

⁹ This being said, the ICI Mutual Policy does provide (through separate standard endorsements) a designated amount of insurance coverage for expenses incurred by Insured Funds in “Claim-Related Internal Corporate Investigations” and in “Shareholder Derivative Demand Investigations.” Under appropriate circumstances, these coverages could potentially be available to defray the costs of certain investigations that might be initiated by Insured Funds following a Network Security Event. For more information on these two ICI Mutual coverages, see:

- “D&O/E&O Insurance Coverage for Expenses of Claim-Related Internal Corporate Investigations – Frequently Asked Questions,” at <http://www.icimutual.com/sites/default/files/FAQ%20-%20Claims%20Related%20to%20Internal%20Corporate%20Investigations.pdf>, and
- “D&O/E&O Insurance Coverage for Shareholder Derivative Demand Investigations – Frequently Asked Questions,” at <http://www.icimutual.com/sites/default/files/SDDI%20FAQ.pdf>.

¹⁰ Thus, by way of examples, coverage is not available under the endorsement for any amounts that an insured adviser or other insured service provider might pay in settlement or judgment of a derivative lawsuit brought against the adviser/service provider on behalf of a Fund (and/or a direct lawsuit brought against the adviser/service provider by the Fund itself) alleging that the adviser/service provider breached its fiduciary and/or contractual duties in failing to adequately protect against a Network Security Event, thereby causing the Fund to sustain First Party Costs following such an event.

8. Is “costs of correction” coverage available under the new endorsement for Network Security Events?

As under mutual fund D&O/E&O policies generally, the “Costs of Correction” coverage provided under the Section II.B of the ICI Mutual Policy is purely an “E&O” coverage, and is therefore potentially available only to insured entities (and not to insured individuals).¹¹ Moreover, because operations-based losses in the fund industry (including operations-based losses that may involve cyber risks) can typically be expected to be traceable back to the acts or omissions of advisers or other service providers (rather than to the acts or omissions of Funds themselves), this coverage is generally regarded as an adviser/service provider coverage (rather than as a Fund coverage). ICI Mutual recognizes that an insured entity might decide, for one or more reasons, to make a “corrective” payment in the aftermath of a Network Security Event. Whether costs of correction coverage could be available under Section II.B of the ICI Mutual Policy for such a payment would necessarily depend on various factors, including the particular facts and circumstances involved.¹²

The adjustment of costs of correction insurance claims as between an insurer and an insured entity has the potential to be particularly challenging in the context of Network Security Events.¹³ Given the emerging nature of this risk and the dearth of established court decisions to serve as precedents,

¹¹ D&O/E&O policies are typically structured as “claims made” policies, meaning that coverage can be triggered only by the filing of a lawsuit or other third-party “claim” against the insured during the policy period. Costs of correction coverage—which has long been a standard feature of the ICI Mutual Policy but has not always been available in commercial insurance markets—is a departure from this basic insurance philosophy that D&O/E&O coverage can be triggered only by third-party claims. Broadly speaking, costs of correction coverage permits an insured service provider, even in the absence of an actual third-party claim, to seek recovery for payments it makes to “correct” designated types of operational losses, provided, among other things, that the insured service provider has *actual legal liability* for the loss. The requirement for *actual legal liability* is fundamental and critical—i.e., the coverage is *not* designed or intended to extend to payments that may be made by the insured service provider as a business accommodation, to avoid reputational damage, to reduce the risk that a third-party claim will be brought against the insured service provider, or for any other reason apart from the service provider’s own *actual legal liability*. See generally ICI MUTUAL, MUTUAL FUND D&O/E&O INSURANCE: A GUIDE FOR INSUREDS (2009), at pp. 35-36, and ICI MUTUAL, OUTSOURCING BY ADVISERS AND AFFILIATED SERVICE PROVIDERS: LIABILITY AND INSURANCE CONSIDERATIONS (2008), at pp. 2-3, both available at www.icimutual.com.

¹² Thus, for example, just as coverage is unavailable under the endorsement for any amounts payable by an insured adviser or other insured service provider in settlement or judgment of a Claim brought by or on behalf of a Fund seeking recovery for the Fund’s own First Party Costs (see note 10 above and accompanying text), coverage would likewise be unavailable for any amounts that an insured adviser or other insured service provider might seek to pay the Fund as “Costs of Correction” in such circumstances.

¹³ ICI Mutual’s decades of experience with costs of corrections claims evidences that this specialized coverage is best suited for the kinds of “ordinary” operations-based mishaps for which the coverage was originally designed—i.e., for situations where (1) an insured service provider affirmatively commits a commonplace operational error that affects a managed Fund or private advisory client (e.g., a “fat-fingered” trade, an inadvertent violation of private advisory guidelines); (2) the affiliated service provider’s legal liability for the error is clear-cut; (3) as a result of the error, the affected Fund (or advisory client) incurs a loss in an exact amount that can be readily (and fairly easily) ascertained; and (4) the amount of the dollar loss at issue is sufficiently modest to warrant avoiding the legal defense expenses that would be incurred by the service provider (and thus, indirectly, by the insurer) if the underlying claimant (i.e., the Fund or advisory client) were required to prove up its legal right to recover from the service provider in a more formal and impartial adjudicatory process (e.g., a court proceeding). In the context of a Network Security Breach Event, it seems unlikely that all of these criteria would be met.

it seems likely that reasonable minds could differ on coverage issues associated with a costs of correction insurance claim arising out of any given Network Security Event.¹⁴ The endorsement establishes a mediation process that is designed to facilitate the resolution of any disagreements over coverage that may arise as between insurer and insured in such cases.

9. Is coverage available under the new endorsement for Network Security Events that affect external networks?

Funds typically outsource their business operations to service providers, who may themselves be affiliated or unaffiliated with the Funds. These service providers may, in turn, sometimes subcontract specialized operational functions to third-party service providers of their own (“sub-service providers”). ICI Mutual recognizes that if a Network Security Event were to strike an “external” computer network (i.e., a computer network operated by a non-insured service provider or by a non-insured sub-service provider), there could be circumstances in which one or more insured entities (and/or their Officers or Directors) might be asserted to be legally responsible for all (or a portion) of resulting losses to Funds or Fund shareholders.

The fact that a Network Security Event strikes an external network would not, in and of itself, preclude coverage for associated Claims that might thereafter be made against insured entities (or their Directors or Officers), or for associated Unrealized Liabilities that might involve insured entities. This being said, it is important to recognize that the ICI Mutual Policy, like D&O/E&O policies generally, is neither designed nor intended to serve as a financial guarantee against any and all losses or exposures that Insureds may incur or face by reason of the acts, errors or omissions of non-insured service providers or non-insured sub-service providers.¹⁵ Whether coverage could actually be available under the ICI Mutual Policy in any given case would necessarily depend on various factors, including the particular facts and circumstances involved, and the impact of the terms, conditions and limitations of the endorsement and of the remainder of the ICI Mutual Policy.

¹⁴ Thus, for example, a service provider’s actual legal liability may be far from clear-cut in the case of a Network Security Event. *See generally* IM Guidance Update (April 2015), at <http://www.sec.gov/investment/im-guidance-2015-02.pdf> (SEC staff appears to acknowledge that the fact that a breach event has occurred does not itself necessarily prove that the victimized service provider has been negligent or has otherwise violated applicable law). Where there is room for disagreement over key underlying issues in a costs of correction insurance claim—e.g., Is there an actual legal liability? What is the correct measure of “damages”?—adjustment of a costs of correction insurance claim can be problematic, and it can be difficult for the claim to be resolved to the mutual satisfaction of the insurer and insured entity (especially since there will have been, by definition, no lawsuit or other formal and impartial adjudicatory process through which the underlying issues have been fully explored, contested and resolved as between the underlying claimant and the insured entity). The special processes and procedures set forth in the endorsement are designed to streamline and facilitate claims adjustment as between the insured entity and ICI Mutual in such cases.

¹⁵ *See generally* ICI Mutual, OUTSOURCING BY ADVISERS AND AFFILIATED SERVICE PROVIDERS (2008) (discussing liability and D&O/E&O insurance concerns associated with outsourcing).

10. What kinds of Network Security Event Claim-related exposures are not covered under the new endorsement?

The following list provides examples of Claim-related exposures that might potentially arise in connection with Network Security Events for which coverage would generally not be available under the new endorsement. The list, which supplements and expands upon responses provided to previous questions, should be viewed as illustrative rather than exhaustive:

- ***Fines, Penalties and Matters Uninsurable under Applicable Law:*** As with D&O/E&O policies generally, the ICI Mutual Policy, as here relevant, defines Loss to exclude “fines or penalties imposed by law, or matters which may be deemed uninsurable under the law pursuant to which [the] policy may be construed” ICI Mutual recognizes that insureds and D&O/E&O insurers may sometimes differ over whether particular payments should be viewed as constituting covered “Loss” under a policy. In order to reduce the potential for misunderstandings or conflicting expectations in this regard, ICI Mutual’s new endorsement, like ICI Mutual’s previous Shareholder Data Event Endorsement, addresses the scope of coverage potentially available under that endorsement for certain payments (i.e., statutory damages, and educational fund payments and similar types of payments) that might conceivably come into play in Non-Traditional Claims.¹⁶
- ***Voluntary Financial Obligations:*** As with D&O/E&O policies generally, the ICI Mutual Policy generally does not afford coverage for financial obligations voluntarily undertaken by insureds. This principle is underscored by a specific provision—included in the ICI Mutual Policy and common in liability insurance policies—that excludes coverage for certain breach of contract claims and for claims arising out of provisions of agreements under which insured entities assume the liabilities of other parties.¹⁷

¹⁶ ICI Mutual recognizes that these two areas—i.e., coverage for statutory damages and coverage for educational fund payments and similar types of payments that may be made to state attorney generals—are likely to be of lesser relevance in the context of Non-Traditional Claims arising out of Network Security Events than in the context of Non-Traditional Claims arising out of Shareholder Data Breach Events. Nevertheless, given the limited claims experience to date with Non-Traditional Claims arising from Network Security Events (either inside or outside the fund industry), ICI Mutual has determined it appropriate to include these provisions in the new endorsement, if only to reduce the potential for misunderstandings or conflicting expectations should such claims arise in the future.

¹⁷ The ICI Mutual Policy’s exclusion (at Section V.M) is subject to certain specified exceptions (including exceptions for contracts between insured entities, and for investment advisory contracts between insured entities and their clients). See generally Kevin LaCroix, “D&O Insurance: The Contract Exclusion” (March 16, 2009), at <http://www.dandodiary.com/2009/03/articles/d-o-insurance/do-insurance-the-contract-exclusion/> (“Long standing case law establishes that liability insurance policies do not cover breach of contract claims, because a contractual duty is not a liability imposed by law but is rather a voluntarily undertaken obligation.”); 23 APPLEMAN ON INSURANCE 2D §146.6, at 120-21 (Eric Mills Holmes ed., 2003) (“Professional liability policies often contain an exclusion for ‘[a]ny ‘claim’ arising out of breach of contract, or out of liability assumed under any contract or agreement.’ Even in the absence of an express exclusion, courts have held that a claim alleging breach of contract is not covered under a professional liability policy because there is no ‘wrongful act’ and no ‘loss’ since the insured is simply being required to pay an amount it agreed to pay.”) (footnote omitted).

- ***Certain Exposures That May Be Insurable Under “Specialty” Cyber Insurance Policies:*** As discussed at Question No. 3 above, the “specialty” cyber insurance policies now available in the insurance marketplace are often expressly designed to respond to an array of cyber-related exposures, including certain network security event-related exposures, that are outside the traditional scope of D&O/E&O insurance. ICI Mutual’s new endorsement is neither designed nor priced to serve as a substitute for such specialty cyber insurance products. In this regard, it is important to underscore that the new endorsement, subject to very limited exceptions, does *not* afford coverage for various exposures that may be insurable under such specialty insurance products, including liability for “transmission of malicious code,” “multimedia liability,” and First Party Costs.