Mitigating risk as you consider incorporating digital assets

Insights from Insurance Industry Professionals

Summary

Advisors are increasingly seeking to be responsive to clients requesting advice and services related to digital assets. Whether you choose to advise on, trade, or take custody of digital assets, this begs the question of whether additional insurance is necessary, and in what form, to help ensure you and your firm are protected in the event of potential accusations of negligence as it relates to advice or appropriateness of investments for clients. What's more, advisors taking custody of digital assets will also want to consider protection against the potential loss or theft of those assets when managing overall risk to their organization. As a reminder, Digital assets are not insured by the Federal Deposit Insurance Corporation and are not protected by the Securities Investor Protection Corporation ("SIPC").

In this brief, we share excerpts from conversations with three insurance industry partners from Fidelity's Alliance Program. These professionals share their insights on the options available for mitigating the risks of offering digital assets and what it takes to secure coverage for you and your firm.

The opinions expressed are those of the contributors and do not necessarily reflect those of Fidelity Investments.

Contributing Insurance Industry Professionals from Fidelity's Alliance Program

David Goldstein

Senior Vice President, Corporate Risk & Broking

Willis Towers Watson (WTW)

Chad Ramberg

President

Box Professional Insurance, LLC

Jessica Thayer

Senior Vice President, Financial Institutions Practice Leader

Starkweather & Shepley Insurance

Fidelity INVESTMENTS

Fidelity:

Could you describe the solution set for advisors to consider when seeking to offer digital asset services?

David Goldstein:

"Whether advisors are advising on, trading, or providing direct ownership of digital assets, they should consider a mix of three types of coverage: professional liability insurance, crime insurance, and cyber liability insurance.

Let's start with professional liability, commonly referred to as errors and omissions (E&O) insurance. As advisors likely know, this type of insurance is typically associated with coverage for claims which may be brought by advisory clients or governmental regulatory authorities. While the insurance market has a lengthy history of underwriting relative to traditional investments, such expertise is relatively new for digital asset investments. There's a robust history and claim data about losses associated with traditional investment advisory services, so underwriters have established rate plans that correlate to this well-understood risk profile.

However, this type of data doesn't exist for digital asset services. So, there are not a lot of carriers ready to offer professional liability coverage for digital assets. This makes the market relatively thinner and more expensive. Further, the deductibles, what we call retentions, are often higher for digital asset related claims than those arising out of traditional investments."

Insurance Considerations for Offering Digital Assets

Errors and Omissions: Typically associated with coverage for claims which may be brought by advisory clients or governmental regulatory authorities.

Cyber: Associated with compensating the advisor in the event its network is hacked or subject to malware or ransomware, and liability to third-parties arising out of such a breach.

Crime: Designed to protect against theft of money, securities or other tangible assets.

Fidelity:

Could you describe the solution set for advisors to consider when seeking to offer digital asset services? *(continued)*

Chad Ramberg:

"An advisor's need for crime insurance is in some ways intertwined with the need for cyber insurance. As most advisors know, cyber coverage is important to protect the advisor's operating environment in the event that the advisor's digital systems are hacked or if there's malware. Where it gets more complicated is when some form of crime is involved—whether it relates to traditional investments or digital assets. Carriers look at crime in one of two ways: theft or what we call social engineering.

Theft of monies or assets in a digital world is relatively easy to understand and trace. There are instances when an incident is considered both a cyber and a theft incident. For example: an advisor's system may have been hacked, and then monies were stolen. In this scenario, the cyber event triggered the theft. There can also be incidents where there is a question of which event happened first.

The act of social engineering can confuse things. The easiest way to understand social engineering is that an advisor's client may be hacked, then a fraudster may impersonate the client and use any number of social engineering means to get that client's money—some of which could be under advisement with the advisor. Often, the fraudsters use multiple angles to impersonate the client and get the advisor to send money to a fraudulent account.

Given the examples I just shared, it's important for advisors to have both crime and cyber insurance, especially if trading or direct ownership of digital assets are involved."

Fidelity:

What are the key differences in coverage between E&O, crime, and cyber policies?

> "E&O providers will seek to understand how much digital assets contribute to the **percentage** of the advisor's overall AUM **and** the **particular services** offered."
>
> — David Goldstein

David:

"Since E&O policies primarily seek to protect against claims brought by investor and regulatory authorities, any advisor seeking to offer any form of digital asset services should review their current E&O policy to ensure adequate coverage exists to protect against such claims.

Fidelity:

What are the key differences in coverage between E&O, crime, and cyber policies? *(continued)*

David: *(continued from previous page)*

Crime insurance protects against the theft of money, securities or other tangible assets. In this context, carriers will want to know whether an advisor provides custody services for digital assets. If so, crime coverage protecting against the theft of those assets will be difficult to obtain. E&O insurance for services in connection with advising on digital assets is significantly more available than crime coverage for the theft of digital assets. The specie market, which offers coverage for things like fine art and jewelry may also be available, though it is expensive and can require significant and detailed underwriting."

Jessica Thayer:

"What we're currently observing is that if digital assets contribute to only 10–15% of total AUM, a larger part of the overall E&O marketplace is likely more willing to underwrite the policy.

For those advising on a higher level of AUM, e.g., 15–20%, premiums for E&O insurance can increase drastically along with a commensurate increase in the deductible, or retention level. This, in part, is because the pool of insurers willing to take on such risk shrinks.

I've observed E&O premiums that could be anywhere from $35,000 to $50,000 and upwards per $1 million of coverage, with deductibles starting at $150,000 and going up from there. If advisors offer trading and the direct ownership of digital assets, fewer insurers will want to write the E&O policy, and premiums can escalate even further.

What drives those premiums up could be a function of the insurer's underwriting analysis, or it could be their reinsurance requirements. A lot of the insurers in the marketplace actually reinsure out their risk, and they have certain requirements. Some reinsurers don't allow exposure to digital assets over a certain percentage, or maybe just in general, so that plays into premiums.

> "When advisors start getting into trading or direct ownership, insurers are going to look closely at third-party risk. Specifically, they're going to look at what **trading platform** the firm is using, and the **track record** and the **expertise** of the trading platform."
>
> — Jessica Thayer

Fidelity:

What are the key differences in coverage between E&O, crime, and cyber policies? *(continued)*

Jessica Thayer: *(continued from previous page)*

I want to point out that when advisors start getting into trading or direct ownership, insurers are going to look closely at third-party risk. Specifically, they're going to look at what trading platform the firm is using, and the track record and the expertise of the trading platform when direct ownership is involved. They are going to look at how that direct ownership is being held—whether it's cold storage or not. That's going to play into the overall risk exposure.

We've had deals where the E&O premium for direct ownership of digital assets, or maybe it's a fund that has more risky digital assets, can be quite high. It's not unusual to see $75,000 or $100,000 for $1 million of coverage. That's because there have been losses and claims in this area.

So, crime insurance is important to consider, especially if the advisor is doing any trading or direct ownership that is occurring outside of an exchange."

Fidelity:

What about cyber insurance?

Jessica:

"Cyber insurance provides protection against privacy-related liabilities and covers the advisory firm as the victim of a network instruction.

We've observed some stability in the market for cyber insurance. However, cyber-attacks are impossible to mitigate. As everyone knows, hackers are finding new ways into our systems.

Cyber extortion is one of the main sources of claims right now, where hackers shut down all systems, any access to any cloud—even if a firm is relying on a third-party provider. Ironically, these hackers demand some sort of digital asset like cryptocurrency or Bitcoin to get your systems back up and running."

Fidelity:

How do insurance carriers evaluate coverage eligibility for digital assets?

Chad:

"Having a written plan is critical to obtain any type of coverage for digital assets. It helps establish some credibility with the carrier and allows them to better evaluate risk, which ultimately impacts insurability and pricing.

Here's an example: An advisor client of mine in the Midwest who has about $500 million in AUM has decided to include digital assets as part of his firm's offering.

His approach to determining which clients and their risk tolerance begins with financial planning. The planning process allows him to evaluate the risk to the client in various scenarios and determine how much to allocate to digital assets in the client's high-risk portion of their portfolio.

Because he lays out his approach in a plan for the carrier to review, the carrier can see that he's considering offering digital assets from the ground up with each individual client. The carrier can also see how he is recommending it to the typical client, including their degree of exposure to that asset. If the underwriter at the insurance carrier understands that, they're going to rate his risk much lower than an advisory firm without such a plan.

In this situation, we were able to get $1 million, $25,000 deductible, for less than $15,000 a year. That covers a million in digital assets. Absolutely phenomenal terms. There was no restriction on if they were liquid, or if they were packaged within a publicly traded asset or not; he could do direct ownership or whatever he felt was appropriate. And the reason the underwriter was willing to do that was really because he was planning to keep a very small portion of each qualified client's assets in digital assets."

Elements of a written plan for offering digital assets

- The types of digital assets the firm is planning to offer (now and in the future)
- The types of clients they will cover
- The process for determining a client's risk tolerance
- Specifics of how the offering will be delivered
- The expertise of the advisor delivering the offering

Source: Chad Ramberg, Box Professional Insurance, LLC

Fidelity:

What happens if an advisor reaches out to get coverage for their digital assets offering, and doesn't have a concrete plan to share with you?

Chad:

Here's what typically happens, and it happens with increased frequency as digital assets becomes more prevalent in the marketplace, as well as in the media market.

A firm contacts me and says, "I want coverage for digital assets."

I say, "Great. Let's have a conversation. How are you planning to access those digital assets?"

Firm says, "I'm not sure yet. I do know I want to include digital assets as part of my investment offering."

I say, "Well, how are you going to recommend clients purchase the digital assets? Could you share your qualifications for doing so?"

Firm says, "I haven't figured out the process yet, though I do want to have a digital asset offering."

> "The number one thing a carrier pays attention to is how the advisor is going to access digital assets. Is it a **publicly traded asset** with a 40 Act Fund, **or** is the advisor looking for **direct ownership**?"
>
> — Chad Ramberg

When we get to the end of the conversation, **I say, "I don't know the exact price for E&O insurance, though I do know it will be $20,000 per year with a $150,000 deductible as a starting point, unless you can get more specific on what you want to do and how you're going to offer this."**

Advisors need to understand that when we go to the underwriters, our job is to add clarity that the advisor didn't know they needed. The number one thing a carrier pays attention to is how the advisor is going to access digital assets. Is it a publicly traded asset with a 40 Act Fund, or is the advisor looking for direct ownership?

There are several different tranches of risk regarding ownership that advisors need to consider. Some carriers will just say, "If it's not in a publicly traded asset class, we're going to exclude it." The way that I explained that to advisors is using a comparison to a traditional asset like gold. You can buy GLD which is an ETF that holds gold and get access that way, or you can buy a bar of gold and hide it under your mattress. Buying digital assets directly is like buying a bar of gold and sticking it under your mattress because whoever has that crypto key has access to the value.

What's more, if advisors don't approach offering digital assets with a plan, they're going to be dead in the water and the underwriter's never even going to offer terms. The insurer will view the advisor as just trying to gather assets with a digital offering because they think digital assets is the newest greatest conversation.

Fidelity:

What happens if an advisor reaches out to get coverage for their digital assets offering, and doesn't have a concrete plan to share with you?*(continued)*

Jessica:

"To opine on Chad's examples, expertise is critical. Insurers are looking at the advisor's overall experience. A younger advisor just coming out of college with no background in this area is obviously riskier than an advisor who previously worked for a regulator like the SEC. They're definitely going to underwrite to the expertise and background of the individuals within the firm who are deemed to be the digital asset experts."

Fidelity:

Let's get specific about crime insurance. How do carriers evaluate eligibility for crime coverage?

David:

"In the traditional crime or specie insurance market, the main focus of the provider would be where those digital assets are stored. Either market is going to require additional supplemental applications, a call or potentially an onsite visit to inspect the actual storage system.

Insurance underwriters will also request a review of any segregation procedures in place between client access, client assets, and any sort of blockchain public addresses. The provider will also want to better understand whether those blockchain funds and all the RIA funds are commingled or held in separate addresses that are public to the blockchain, in which case the users would be able to verify that their funds are where they say they are.

There are a lot of underwriting questions that go into the private key generation if advisors are going to offer direct custody of digital assets. Underwriters will want to know the processes and the security procedures surrounding the generation of the private keys. And they also want to see details on the disposal of any sort of material information relating to the generation of private keys."

> "There are a lot of underwriting questions that go into the private key generation if advisors are going to offer direct custody of digital assets. Underwriters will want to know the **processes and the security procedures** surrounding the generation of the private keys."
>
> — David Goldstein

Fidelity:

Let's get specific about crime insurance. How do carriers evaluate eligibility for crime coverage? *(continued)*

David: *(continued from previous page)*

Lastly, they will seek a detailed report on the recovery or backup plan in the event that the servers storing the private keys go down, or any sort of natural disaster impacts storage of those keys.

One thing I'll add is that with digital assets, it's really a catastrophic loss or no loss. If someone has the ability to access funds in the wallet, the whole wallet will likely be drained. This means that losses in this space are typically large. This has implications for underwriting, as the carriers have to factor in any losses as a full limit loss. This is why they want to know all the details on the organizational structure within the actual wallets, and whether the advisor is planning to cap wallets at certain limits and start to reshuffle funds as those limits grow.

Fidelity:

Does it feel like the industry is in the early innings for providing crime insurance?

David:

It feels like it. There are not a whole lot of underwriters in the space with a high level of expertise when you start talking about the architecture of these wallets. Also, since the underwriters who do have knowledge and expertise in this area are often younger they usually have to seek authority to bind coverage from more experienced managers who may be less inclined to take on the risk.

I have had crime underwriters express concerns to me over events that were not possible from a technology standpoint. For example, they were concerned about overseas hackers getting into their network and withdrawing funds from their wallet. However, in reality, client multi-signature wallet architecture prevents this from happening: one individual hacking into their network does not give the hacker the ability to transfer funds from a wallet, which would require a physical device to be confirmed at time of transaction. There's still a long way to go in understanding everything.

Within the E&O industry, underwriters are better equipped to address advisory risk because as an investment, there is less need to understand the technical architecture of digital assets than within the crime insurance context. Here, underwriters have more information as to the nature of the investment risk and the volatility of cryptocurrency markets, which help inform their underwriting.

Fidelity:

What are providers focusing on today when evaluating coverage for cyber insurance?

Jessica:

Typically, providers look at revenues, and the types and number of personally identifiable information or records that you have. It's also based on the policies and procedures a firm has in place on the cyber front.

If you don't have multifactor authentication and end point detection, it's almost impossible to get cyber coverage. Historically, those areas were a "nice to have." Today, these are essential.

Fidelity:

What are the most common questions you receive from RIAs regarding insurance for advising on digital assets?

Jessica:

Advisors often ask about immediate things they should be doing as they explore offering digital assets or expanding any existing digital asset offering.

First, documentation and disclosures are going to be your two best friends. You cannot over-disclose. Make sure your policies and procedures clearly document how you're advising clients and the risks associated with doing so. This includes internal policies and procedures and the ADV. Addressing how you're offering digital services in your investment management agreement can be helpful as well, even if you are just advising and not necessarily trading or having direct ownership via a third-party custodian. Any kind of discussion with the client is considered advising.

Second: Expertise is crucial. If you're already in this area and looking to grow, seriously consider bringing in experts to help. It is a full-time job to keep up with what's going on in this market, and advisors need to be certain they're doing the right thing for their clients and advising them properly.

Places to consider documenting a digital asset offering and associated risks:

- Internal policies and procedures
- ADV
- Investment management agreement

Source: Jessica Thayer, Starkweather & Shepley Insurance

Fidelity:

What are the most common questions you receive from RIAs regarding insurance for advising on digital assets? *(continued)*

Chad:

One question I've repeatedly heard from advisors is "Do I really need insurance if I'm not truly interested in offering digital asset services?"

My feeling is that many advisors who may not intend to play in the digital space will be doing so. Taking a cue from Jessica's point that any discussion with the client is considered advising, advisors need to plan for every potential conversation they could have with clients and prepare for the unexpected.

It's not my intent to scare advisors, but to be realistic about what that planning means for those who don't believe they are playing in the digital space. For example, if you say, "I don't offer digital asset services," that's fine. However, if you introduce the client to somebody who does understand digital assets you defer some of that risk.

Carriers expect there are times when clients will be introduced to other professionals. Though it's very important to fully vet any referral partners as situations can arise where the individual accepting the referral did not meet the quality standards expected. When things go poorly enough, the advisor can get pulled into a claim. This is why high-quality coverage becomes very important to have.

Here's another example: What if a client expresses a desire to invest in digital assets during a conversation? My suggestion at that point is for the advisor to reply, "That's interesting. What's driving your interest in digital assets?"

If the answer is, "Well, because Uncle Joe told me the potential is there to easily make one million dollars off it," then a response to this type of exploratory interest drives one path of a conversation.

> "One question I've repeatedly heard from advisors is **'Do I really need insurance if I'm not truly interested** in offering digital asset services?'"
>
> — Chad Ramberg

However, if the answer is "Because I've actually been mining this particular digital asset and it has a lot of value and I'm trying to figure out how to diversify," that's a completely different conversation that immediately puts the advisor in the unintended position of advising.

While there are many more examples I could share, these two illustrate why it's critical that advisors prepare for the many client conversations that could occur and document a plan to handle them. I encourage advisors to take things one step further and share this plan with their insurance broker to determine whether their existing policies protect them in these various types of situations.

Fidelity:

What should advisors do to ensure their coverage is appropriate in light of a changing environment, where new regulations may be enacted, or market conditions offer surprises?

David:

When there's talk of any specific regulations, the first step advisors should take is to work closely with their broker to evaluate the impact on current coverage and how that coverage would respond to any type of digital asset exposure we've been discussing. I see more regulation coming into play in 2023.

Advisors should make a habit of reviewing their E&O coverage with their broker annually and start the renewal process early. This allows sufficient time to work together to address any issues or changes in the current policy.

There are a lot of insurers who realize this space is here to stay, and they are looking for ways to get in. I believe they are going to start slowly entering the market by offering modest coverage in niche areas.

Key takeaways from our experts

- A detailed written plan is essential for gaining coverage for a digital asset offering. Your plan should include, among other things, what the offer is, who it is for, and how you plan to deliver it.
- Ensure you have an experienced and knowledgeable team to deliver your offering.
- Maintain up-to-date documentation of your policies and procedures for offering digital assets and have the documentation ready to share with carriers.
- Amend your ADV and investment management agreements to reflect your offering.
- Plan for every potential conversation around digital assets, even if you do not intend on making it available for clients.
- Vet any third-party referral sources you may rely upon, or refer clients to.
- Stay current on regulatory changes.
- Review your coverage annually with your carrier. Start the process early to help address any unforeseen questions posed by carriers.
- Always keep your broker apprised of any changes in your business throughout the year.

Key Contacts

David Goldstein
Senior Vice President, Corporate Risk & Broking
Willis Towers Watson (WTW)
affinitytechnology.willistowerswatson.com/sales/Fidelity

Chad Ramberg
President
Box Professional Insurance, LLC
boxproinsurance.com

Jessica Thayer
Senior Vice President, Financial Institutions Practice Leader
Starkweather & Shepley Insurance
starshep.com/industry/financial-services

1095298..2.0