VOL. 36, NO. 1 SPRING 2023

BENEFITS LAW JOURNAL

Protecting Plan Assets from Cybersecurity Risk – The Evolving Challenge

By Heidi J. Schmid

In this article, the author discusses the cybersecurity risk to retirement plans, examines the challenges participants face in recovering stolen funds, and explores the enhanced cybersecurity risk associated with plan investments in cryptocurrency and other crypto assets.

In 2011, the ERISA Advisory Council remarked:[1]

> When ERISA was enacted in 1974, state of the art technology was a fax machine, communications were mailed and distributions were made by writing a check. As technology has improved and expanded to include various forms of electronic communications, there are increasing concerns about privacy, security and fraud in the benefits area as many financial transactions are conducted

Heidi J. Schmid, counsel in White & Case's Employment, Compensation and Benefits practice, advises clients on compliance with ERISA fiduciary and plan asset requirements, including the structure and offering of complex securities and financial products, the formation and ongoing compliance of private equity and hedge funds, and compliance with ERISA's prohibited transaction rules and exemptions. Based in New York, she may be contacted at heidi.schmid@whitecase.com. Anthony Veveakis, an associate in the firm's office in New York, assisted with the research for this article.

> on-line and as plan participants are increasingly required to use technology to interface with their plans.

State of the art technology may be different today (the ERISA Advisory Council's 2011 report cited cases of data breaches on "electronic tapes" and compact disks), but the cybersecurity threats facing retirement plans are as relevant as they were twelve years ago. As Barry L. Salkin noted in a recent edition of the *Benefits Law Journal*, there has been an "increase in cybersecurity incidents directed towards tax-qualified plans."[2] Plan sponsors, IRA owners, plan administrators, and service providers are frequent targets for business email compromise[3] schemes and other attacks, resulting in data breaches, identity theft, and theft of plan assets.

Retirement plans represent particularly attractive targets of cybercrime due to the large pool of assets they represent – total U.S. retirement assets were $32.3 trillion as of September 2022.[4] In addition to a plan's funds, attacks are also aimed at gaining access to sensitive plan data, including participant names, Social Security numbers and account information.[5] Furthermore, plans are vulnerable targets due to the multiple points of entry that may be exploited by bad actors to gain access to plan assets and data, including the employees and systems of plan sponsors, service providers, counterparties, and administrators, as well as plan participants themselves.

Adding insult to injury, after their retirement savings disappear into a criminal's bank account, injured plan participants must go to court and battle plan fiduciaries and service providers to recover their stolen funds, since they are not protected by the plan's fidelity bond or fiduciary liability insurance policies, or by the cyber insurance policies held by plan sponsors and service providers, and federal law does not require that plans, plan sponsors, or service providers make participants whole or hold commercial crime coverage that will do so.[6] The shift over the last 50 years from employees being covered by defined benefit plans to being covered by defined contribution plans[7] has not only reallocated the burden of saving and investing for retirement to participants; participants have also been reallocated the risk of loss of plan assets due to theft and fraud.

The risk of cybertheft increases for plans offering cryptocurrency and other crypto assets,[8] which have been marketed as investment options to 401(k) plans and IRA owners. Crypto assets have been particularly vulnerable to theft due to hacks and other breaches,[9] highlighting the need to, in the words of the Department of Labor,[10] "exercise extreme care" when determining whether to invest plan assets in crypto assets (or offer access to crypto assets as an investment option) and evaluating which service providers and counterparties to engage with in the crypto market.

I. CYBERSECURITY RESPONSIBILITIES OF PLAN SPONSORS UNDER ERISA

Under ERISA, fiduciaries must act solely in the financial interests of plan participants and adhere to an exacting standard of professional care. Courts have commonly referred to these prudence and loyalty obligations as the "highest known to the law." Fiduciaries who breach those duties are personally liable for any losses to the plan resulting from that breach.[11]

In April 2021, ten years after the publication of the 2011 ERISA Advisory Council report, and five years after the ERISA Advisory Council's 2016 follow-on report[12] on cybersecurity considerations for pension and welfare benefit plans, the Department of Labor's Employee Benefits Security Administration (EBSA) issued its first formal cybersecurity best practices guidance[13] for plan sponsors, fiduciaries, recordkeepers, service providers, and participants and beneficiaries. This guidance was the first pronouncement from the Department that ERISA plan fiduciaries have an obligation to ensure that cybersecurity risk is properly mitigated. This guidance supplemented the Department's prior guidance[14] on prudently selecting and monitoring service providers.

Cybersecurity implicates multiple fiduciary duties under ERISA, including the duty of prudence, the duty of loyalty and the exclusive benefit rule. In the words of the Seventh Circuit, "The reasonableness of [a service provider's] cybersecurity services, and the extent of any breaches, is therefore relevant to determining whether ERISA has been violated - either by [the service provider] itself or by the employers that outsourced management of their ERISA plans to [the service provider].[15]

a. Duty of Prudence

An ERISA fiduciary must act with the same care, skill, prudence, and diligence under the circumstances that a prudent fiduciary acting in a similar capacity and familiar with these matters is likely to use in a similar plan with the same goals. Plans often engage third-party service providers to maintain plan records and keep participant data confidential and plan accounts secure. Plan fiduciaries have a duty under ERISA to prudently select and monitor service providers, and must include cybersecurity risk as a factor in their selection and monitoring criteria.

In engaging a service provider and monitoring a service provider's cybersecurity compliance, plan sponsors and fiduciaries should adopt policies and procedures which address the cybersecurity risk associated with the service provider relationship and the services being provided, which may include requiring that service provider agreements set forth the service provider's cybersecurity program compliance obligations,

such as cybersecurity program certifications, breach notification procedures, encryption requirements, and testing procedures. The EBSA cybersecurity guidance includes guidance for plan sponsors in selecting service providers with strong cybersecurity practices,[16] as well as "Cybersecurity Program Best Practices"[17] for recordkeepers and other service providers, and for plan fiduciaries selecting service providers.

b. Duty of Loyalty and the Exclusive Benefit Rule

An ERISA fiduciary must act solely in the interest of plan participants and beneficiaries with the exclusive purpose of providing benefits to them. Fiduciaries must use plan assets for the exclusive purpose of providing plan benefits and defraying reasonable expenses of plan administration (the exclusive benefit rule).

The duty of loyalty and the exclusive benefit rule require, among other things, that plan fiduciaries maintain plan records and procedures, avoid misleading statements and misrepresentations and make reasonable arrangements with service providers. Plan sponsors should adopt and follow cybersecurity policies and procedures that include best practices to protect plan participant and beneficiary data and that include a plan of action if a data breach occurs.[18]

The adoption of a robust cybersecurity risk management program should enable a fiduciary to demonstrate, in the event of a breach, that it has taken appropriate steps to secure plan assets and data. Since cybersecurity risks are constantly changing, these policies and procedures should be evaluated at least annually and updated as necessary to ensure that they address relevant cybersecurity risks.

II. PARTICIPANTS FACE SIGNIFICANT HURDLES IN RECOVERING STOLEN FUNDS

Cybercrime is endemic across all industries, and retirement plans are no different. However, because ERISA has not kept up with advances in technology, plan participants and retirees are less protected from losses from fraud in their retirement accounts than they are in their personal bank accounts.[19]

a. Standard Fraud Protections Do Not Protect Participants

The typical protections that plans must have in place do not protect participants against the risk of loss from cyber crimes. Fidelity bonds

required under ERISA protect plan assets from thefts by internal, not external, actors, and therefore would not cover most cyber breaches. Fiduciary liability insurance protects plan sponsors, but does not cover crimes. Plan sponsors and service providers may have cyber insurance or criminal liability insurance to protect against their own losses; cyber insurance policies typically are intended to cover losses related to data and information, not amounts stolen from participant accounts.[20] In contrast, a commercial crime policy, which is not currently required by ERISA, is intended to protect against direct loss of money, securities, or tangible property (typically not data) caused by employees as well as outside third parties.

b. Participants Face Challenges to Recover Stolen Assets

Recent cases illustrate the challenges facing plan participants who are victims of cybercrime. In each case, the plan fiduciaries, service providers, and insurers refused to take responsibility for the breach and refused to make the participant whole. Unless victims take the costly and burdensome step of going to court to sue those they entrusted with their retirement funds, they must bear the entire cost of security breaches they had no role in causing.

Paula Disberry, a retired senior executive of Colgate-Palmolive, had her retirement account completely drained by an unknown thief, resulting in a loss of more than $750,000. Her case against the plan's third-party administrator, Alight, and the named fiduciary of the plan recently survived a motion to dismiss, with the court[21] concluding that Alight could have been acting as a fiduciary, and that both Alight and the named fiduciary of the plan could have breached their fiduciary duties by failing to prevent the unauthorized distribution. Similar cases against Abbott Laboratories and Alight in 2020[22] and Estee Lauder and Alight in 2019,[23] alleging that plan fiduciaries breached their duties under ERISA by allowing unauthorized distributions (of $245,000 and $99,000, respectively) from the plaintiffs' retirement accounts, were both settled.[24]

A recent case illustrates the limited protection provided by typical insurance policies. IRA owners filed a class action[25] against their IRA provider and against crypto trading firm Gemini following a dramatic cyberattack (discussed in more detail in Section III of this article) which resulted in the IRA owners' Gemini accounts being emptied of more than $36 million. The IRA provider sued Gemini, Gemini blamed the IRA provider, and the IRA provider's insurance company filed a declaratory action seeking court confirmation that the insurance policy's "Cyber Liability Exclusion Endorsement" precluded coverage of the IRA owners' claims.[26]

c. Outcome-Based Regulation Is Needed to Protect Retirement Savings

Even with the best procedures in place, security breaches will occur. Without a rule allocating the risk of loss away from plan participants, or requiring commercial cyber risk insurance, participants will continue to bear the primary risk of loss of their retirement savings due to cyber risks and fraud – which is particularly unfair to the majority of participants, who cannot afford to sue. Absent economic incentives to the contrary, third-party administrators and other plan service providers will be incentivized to cut corners on their employee training and cybersecurity infrastructure. Currently, the burden of providing those incentives is on the plan fiduciaries negotiating the arrangements with and monitoring these entities; however, once a breach occurs, participants have no rights to reimbursement of their losses.

While the cybersecurity recommendations provided by EBSA are well-intentioned, they fall short of protecting the security of participants' retirement funds. At best, they provide important assessment tools for fiduciaries and may reduce the risk of security breaches; at worst, they simply provide guidance to ensure that fiduciaries will not be found liable to participants for their losses. But why, under a regulatory regime intended to protect plan assets against the risk of loss, should innocent participants bear the risk of loss due to cybercrime?

ERISA practitioners[27] have observed that, in order to fulfill ERISA's promise of protecting employee retirement security, outcome-based regulation is necessary. By requiring that plans reimburse participants for fraudulent transactions, or requiring that plans hold commercial crime policies that cover participant losses resulting from cybercrime, Congress could amend ERISA to ensure that participant funds are protected. Following a breach, plan sponsors and service providers would then make insurance claims and claims for indemnification against one another based on their contractual arrangements – and participants could rest easy knowing that their retirement funds are secure.

III. PLAN INVESTMENTS IN CRYPTO ASSETS

a. Unique Cybersecurity Challenges of Crypto Asset Investments

Plan fiduciaries today are evaluating whether to invest in crypto assets, or to offer such investments as an investment option in a self-directed plan or via a brokerage window. Such a decision is subject to ERISA's fiduciary duties, and while much of the discussion has, reasonably, focused on the broader prudence and loyalty challenges posed

by plan investments in crypto assets, including volatility, vulnerability to manipulation, the speculative nature of crypto assets, the challenge for plan participants to make informed investment decisions, valuation concerns, and the evolving regulatory environment, plan fiduciaries should pay particular attention to the unique cybersecurity considerations crypto asset investments present.

Critically, crypto assets are rife with operational risks due to the features of the technology itself, such as open-source software and distributed ledgers. Because cryptocurrencies operate as software, they are susceptible to bugs and hacks. A number of crypto service providers, including exchanges and wallets, have also been hacked. Between January 2011 and July 10, 2022, approximately $14.58 billion in cryptocurrencies was stolen – and over $3 billion was stolen in 2022 alone.[28] According to crypto analytics firm Crystal Blockchain,[29] "given that the number of blockchains keeps growing and the methods and technologies used by illegal hackers continue to become more sophisticated and advanced, we can assume that the number of hack attacks will also continue to grow." As noted by the Treasury Department, "cybersecurity practices and protections will need to keep pace with the scale of adoption" of crypto assets.[30]

The Department of Labor and other regulators and experts have highlighted the novel cybersecurity risks posed to investors in crypto assets, which plan fiduciaries are required to take into account as part of a prudent decision making process, both in selecting and monitoring custodians, recordkeepers and other transaction parties, and in evaluating the prudence of crypto asset investments. In order to satisfy its duty of prudence when considering an investment or an investment course of action, a fiduciary must give appropriate consideration to the facts and circumstances that the fiduciary knows or should know are relevant to the particular investment or investment course of action involved, and must act accordingly.[31]

It is particularly relevant, in the context of the rapidly-evolving crypto asset market, that ERISA's prudent expert standard of care requires plan fiduciaries to consult with appropriate experts when making investment decisions if the fiduciary lacks the necessary expertise. In addition, plan fiduciaries have an ongoing duty of care which requires them to continuously monitor a plan's investments and remove imprudent investments.[32] An investment can be imprudent for a number of reasons, including undue risk. In its guidance related to 401(k) plan investment in crypto assets,[33] EBSA noted that it "has serious concerns about the prudence of a fiduciary's decision to expose a 401(k) plan's participants to direct investments in cryptocurrencies, or other products whose value is tied to cryptocurrencies. These investments present significant risks and challenges to participants' retirement accounts, including significant risks of fraud, theft, and loss."

In evaluating the cybersecurity risk profile of service providers and other crypto market participants, plan fiduciaries should not assume that the same market practice, regulatory framework, or terminology applies. Plan fiduciaries, who are familiar with transacting with regulated counterparties and engaging with regulated service providers in the traditional financial system, should be particularly cognizant that most crypto market participants are not subject to, and/or have not structured their business to comply with, the same rules as traditional plan counterparties and service providers. Making this evaluation even more difficult, crypto market participants may misrepresent how they are regulated, falsely stating or implying that a given crypto-asset product is regulated to the same extent as other financial products. For example, many nonbank firms in the crypto-asset market hold themselves out as being regulated, including falsely advertising that deposits are FDIC insured.[34] Firms often emphasize money services business regulation, although such regulation is limited, largely focused on anti-money laundering controls or consumer protection.[35]

Needless to say, in such an environment, plan fiduciaries should not assume that crypto market participants have any familiarity with ERISA's requirements regarding the custody, recordkeeping and valuation of plan assets, or that they have the technical competence, systems, and infrastructure that plan fiduciaries typically expect from the trust banks, recordkeepers, and mutual fund companies which they customarily transact with and entrust with prudently safeguarding and accounting for retirement assets.

Plan investors should also be aware that concepts that have one meaning in the qualified plan context (such as "custody") may have a different meaning, and carry different legal rights, in the crypto asset context. Crypto platforms have historically commingled the assets of depositors with the funds of the platform, rather than segregating customer assets, putting assets at risk of being treated as assets of an insolvent platform's bankruptcy estate.[36] This contrasts with the protections a plan investor would be entitled to in a liquidation of an SEC registered broker-dealer, which is overseen by the Securities Investor Protection Corporation under the Securities Investor Protection Act, and in which customer assets are segregated from the brokerage's assets and cannot be used to satisfy the brokerage's debts to other creditors. Highlighting the cybersecurity risk posed by the differences between traditional plan asset custody and the custody and recordkeeping procedures used in the crypto asset market, EBSA noted:[37]

> Cryptocurrencies are not held like traditional plan assets in trust or custodial accounts, readily valued and available to pay benefits and plan expenses. Instead, they generally exist as lines of

> computer code in a digital wallet. With some cryptocurrencies, simply losing or forgetting a password can result in the loss of the asset forever. Other methods of holding cryptocurrencies can be vulnerable to hackers and theft. These are just a few examples of the custodial and recordkeeping issues that may present additional difficulties for fiduciaries of retirement plans.

The U.S. federal prudential banking regulators recently issued[38] a "Joint Statement on Crypto-Asset Risks to Banking Organizations", which highlighted a number of key risks associated with crypto assets and crypto-asset sector participants which are relevant for plan fiduciaries to consider, including: the risk of fraud and scams among crypto-asset sector participants; legal uncertainties related to custody practices, redemptions, and ownership rights, some of which are currently the subject of legal processes and proceedings; inaccurate or misleading representations and disclosures by crypto-asset companies, including misrepresentations regarding federal deposit insurance and other practices that may be unfair, deceptive, or abusive, contributing to significant harm to retail and institutional investors, customers, and counterparties; risk management and governance practices in the crypto-asset sector exhibiting a lack of maturity and robustness; and heightened risks associated with open, public, and/or decentralized networks, or similar systems, including, but not limited to, the lack of governance mechanisms establishing oversight of the system, the absence of contracts or standards to clearly establish roles, responsibilities, and liabilities, and vulnerabilities related to cyberattacks, outages, lost or trapped assets, and illicit finance.

Each layer of a crypto asset transaction implicates its own separate cybersecurity risk analysis, and plan fiduciaries should fully understand the cybersecurity arrangements of each counterparty at each layer, as well as the cybersecurity measures protecting the transactions between those layers, as well as the on-ramps and off-ramps for U.S. dollars in and out of the investment.[39]

As an initial matter, the plan fiduciary should understand how the security of the "private key" which secures title to the crypto asset will be maintained.[40] It must determine whether the participant (if permitted)[41] or a custodian will hold the private key, and it must determine whether the methods used for maintaining the private key are sufficiently secure to satisfy its cybersecurity standards.

Understanding the security of the private key is only the first step; a fiduciary's cybersecurity analysis must expand beyond the security of the private key to encompass the security arrangements of each of the counterparties and the transactions between the participant, the custodian, any crypto asset trading platform on which the crypto assets are bought and sold, and any counterparties of the crypto asset

trading platform with which the participant may transact, such as a crypto lending platform.

A plan fiduciary should conduct appropriate due diligence to determine whether the trading platform on which a particular crypto asset resides provides reasonable safeguards against parties who might seek to subvert the platform (through cyber measures or otherwise) for the purpose of misappropriating assets that reside on the platform. In February 2020, the Board of the International Organization of Securities Commissions ("IOSCO") released a report entitled "Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms."[42] Section 2 of the report, addressing safeguarding participant assets and protection against loss, and Section 7 of the report, discussing cybersecurity and resilience, raise issues of particular concern to plan fiduciaries. IOSCO notes in Section 2 of the report that, where the trading platform offers custody (that is, holding, controlling and safekeeping participant assets), the risks that could arise include "operational failure – the system may be compromised such that participant assets are lost or inaccessible (e.g., due to a cyber-attack), and theft, loss or inaccessibility of private keys – private keys are compromised (e.g., due to a cyber-attack or breach, or by an action of a trading platform insider) or lost resulting in stolen or inaccessible assets." Section 7 of the report highlights that cybersecurity is "particularly important for [trading platforms] due to the use of novel technology and the fact that many [trading platforms] hold participant assets. Security breaches and the exploitation of system vulnerabilities of [trading platforms] and wallets have resulted in significant losses of investor assets. [. . .] In addition, where investors, including retail investors, are on-boarded and provide personal information, cyber [v]ulnerabilities may be exploited to access that individual information."

Furthermore, crypto trading platforms or other counterparties may offer customers the ability to transact with other counterparties. For example, crypto trading firms may offer their retail customers the opportunity to earn returns on their crypto assets by lending those assets to crypto lending firms (such arrangements are often called "Earn" programs). In considering whether to permit participation in an Earn program, or in another product offered by a crypto trading platform, a fiduciary should understand the security protocols applicable to transactions between the trading firm and the lending firm or other counterparty, as well as the protocols applicable at the lending firm or other counterparty itself. Crypto lending firms, which are a type of "decentralized finance" or "DeFi" firm, have been the recent subject of frequent hacks and exploits. Many of the largest crypto lending firms are now defunct,[43] and the SEC has stated[44] that "Earn" programs constitute offers of unregistered securities by both the crypto lending

platforms and the crypto trading platforms that offer their customers access to Earn programs.

b. IRA Financial v. Gemini Trust Company, LLC

The events described in the recent dispute involving self-directed IRA provider[45] IRA Financial Trust ("IRA Financial") and crypto asset trading platform Gemini Trust Company, LLC ("Gemini")[46] over a cyberattack that resulted in over $36 million worth of crypto assets being stolen from IRA owners' accounts are illustrative of the cybersecurity challenges facing plan fiduciaries in prudently selecting and monitoring service providers and counterparties offering crypto asset investments.

In February 2022, in an event that New York State Attorney General Letitia James has described[47] as illustrating that "cryptocurrencies are widely subject to hacking in ways largely unheard of in traditional financial instruments," hackers "swatted" IRA Financial by calling the police and falsely reporting a kidnapping at IRA Financial's headquarters. When employees returned to their desks, they immediately noticed suspicious transactions in a client's Gemini account. Because IRA Financial was not able to freeze accounts itself, and was not able to call Gemini directly to request that the accounts be frozen, in the two hours between discovering the breach and Gemini freezing the accounts, IRA Financial staff alternated between frantically emailing Gemini and looking on helplessly as the hackers stole over $36 million in client crypto assets held by Gemini on its platform, by transferring multiple IRA owners' assets to one IRA owner's Gemini account and then draining the assets of that account.

Following the theft, IRA Financial investigated the breach and discovered that, in addition to stealing their crypto assets, the hacker had gained access to sensitive information of certain clients, including their names, Social Security numbers, and financial account numbers. Reports indicate that client U.S. dollar deposits were also stolen.[48]

IRA Financial claims that this theft was able to take place because Gemini had issued it a Master Application Program Interface (API) key which enabled hackers to circumvent cybersecurity protocols such as multifactor authentication and transfer assets between accounts, and this Master API key was accessed and then exploited by hackers. Anyone with access to the Master API key could access all of the IRA Financial customer accounts and withdraw unlimited assets without multifactor authentication, and without triggering notifications.[49]

It appears that hackers may have been able to access IRA Financial's systems, and, as a result, the Master API key, after an IRA Financial employee clicked on an unknown malicious link (a type of security

breach known as a "phishing" attack); a memo distributed to customers a few hours before the breach warned customers to remain wary of phishers and warned, "We have reason to believe that there are some bad actors posing as IRA Financial employees looking for crypto account-related information."[50] The Master API key may have been easily found in the email accounts of IRA Financial staff; the complaint indicates that Gemini personnel exchanged unsecured, unencrypted emails with IRA Financial containing the Master API key.

IRA Financial claims that Gemini was negligent in failing to provide an API that was reasonably safe for IRA owners, who "required an extra layer of security."[51] However, it is unclear whether IRA Financial engaged in a sufficient diligence and monitoring process to understand the API and the cybersecurity risk applicable to the transactions that it and its clients would engage in with Gemini and to evaluate whether Gemini (and IRA Financial) had the requisite security infrastructure and processes in place to provide IRA Financial's clients with that extra layer of security. In the complaint, IRA Financial states that, in researching potential custodians, it focused on the security of the private keys, stating that it focused its diligence on "crypto exchanges' ability to secure the crypto assets, which are notoriously subject to theft and fraud attempts". It is not clear whether, and do what extent, IRA Financial engaged in an analysis of cybersecurity risk that extended beyond the security of the private keys or otherwise took into account the risks of interacting with crypto trading platforms that IOSCO has identified.

IRA Financial also claims that Gemini falsely represented that it kept most crypto assets in cold storage (a digital wallet that is not connected to the internet and thus is less susceptible to theft), that it maintained insurance coverage for crypto assets that it held in its online "hot wallets," and that all customer assets and security events on the Gemini platform were insured.

i. IRA Financial's Engagement of Gemini & Launch of the Crypto IRA Program

IRA Financial is a provider of self-directed individual retirement accounts which permits IRA owners to invest in crypto assets and other "alternative" assets; it claims to hold over $3.2 billion in alternative assets.[52] It became an institutional customer of crypto exchange Gemini in September 2019, an arrangement it describes in the complaint as partnering with a crypto exchange as a custodian to handle trading, custody, and security of its clients' crypto assets.

In the complaint, IRA Financial states that it selected Gemini to secure its clients' crypto assets largely because of its "detailed statements" about its industry-leading focus on security. The complaint, which does not

include any breach of contract claims, states that IRA Financial relied on statements made by Gemini on its website; it does not cite any contractual undertakings, with respect to cybersecurity or otherwise, that IRA Financial obtained from Gemini in retaining it as a "custodian" before it facilitated the transfer of tens of millions of dollars of clients retirement assets to Gemini. When IRA Financial became a customer of Gemini, Gemini refused to provide a phone number that IRA Financial could call in emergencies and IRA Financial did not insist on being provided with one as a condition of retaining Gemini as a custodian; as a result, IRA Financial could only email Gemini for assistance.

Both IRA Financial and Gemini marketed themselves to customers as safe, trustworthy and secure, respectively stating "Trust is our name" and "Trust is our product."[53] IRA Financial advertised that customers could "trust Gemini as the licensed and qualified custodian of their cryptocurrency private key" and stated that "It is our strong belief that the best and safest way to purchase bitcoin and other cryptocurrency with IRA funds is with our digital solution. IRA Financial clients can perform transactions any time and will gain complete control over their crypto."[54]

When IRA Financial initially offered its clients the option to invest with Gemini, account creation was a multi-step process. When a client expressed interest in holding crypto assets, IRA Financial would provide Gemini, via Gemini's web-based platform, with the client's contact information. Gemini then contacted and directly onboarded these clients who wished to transact in crypto assets, performing Know-Your-Customer checks and creating a client account on the Gemini platform. Once the client was onboarded, IRA Financial then sent the client's funds to a Gemini-owned bank account at Silvergate Bank which IRA Financial had access to; a personal subaccount was created for that client and the client's funds were then transferred to the client's personal subaccount. Clients could then transact in crypto assets on Gemini's web-based interface, which allowed the IRA owner to purchase, store, and trade crypto assets on the Gemini platform. Beginning in 2021, clients could participate in Gemini Earn, which offered up to 7.8% in returns on crypto loaned by clients to crypto lender Genesis.[55] Gemini held all the client's crypto assets and maintained custody over the private keys.

Soon after it launched its crypto asset IRA program, IRA Financial quickly experienced high demand for crypto accounts, but Gemini's systems could not handle onboarding customers at the speed with which they were signing up. The onboarding problems documented in the complaint may have indicated operational weaknesses for IRA Financial to have considered in its ongoing monitoring of whether to continue use Gemini as a custodian.

When the program first launched, Gemini set up a Gemini-owned Silvergate Bank account called "Primary 1" and gave IRA Financial access to that account. As each new client was onboarded, the client's funds were sent to Primary 1. A subaccount within Primary 1 was then created for the new client, and IRA Financial sent the client's funds from Primary 1 to that client's subaccount. The Primary 1 account quickly reached the maximum capacity of subaccounts it was permitted to have, and Gemini created a new Silvergate Bank account, "Primary 2," which also quickly reached capacity.

It is not clear from the complaint whether these account capacity limits were imposed by Silvergate Bank or by Gemini. It is not clear why the Silvergate account capacity issues were not anticipated by Gemini before the program launch; facilitating the onboarding of a large number of client accounts would appear to have been an essential element of the IRA Financial-Gemini business relationship.

ii. The Switch to the API; The Master Account-Subaccount Structure at Gemini

Switching to Gemini's API, a software interface, was proposed by Gemini as a solution because there was no limit to the number of accounts that could be opened on the API. According to IRA Financial, Gemini "strongly pressured" IRA Financial to switch from using Gemini's web-based platform to its API, in order to onboard customers more quickly. IRA Financial switched from the web-based platform to the API in September 2021.

It is not disclosed in the complaint how the client onboarding process described above changed with the switch to the API, or how client accounts were funded following the switch to the API. It is not clear from the complaint, but it appears that clients who had been onboarded via the web-based platform and had been trading via the web-based platform were also migrated to the API; the complaint states that IRA owners contacted IRA Financial and expressed "prescient" concerns about the risk of storing assets on a crypto exchange.

It is not clear what, if anything, IRA Financial was told or understood about the API and its function or structure, or the structure of the client accounts within the API.

Similar to the subaccount structure described above for the Silvergate Bank accounts, Gemini set up the accounts for IRA Financial clients on the Gemini trading platform using a master account-subaccount structure. In this structure, IRA Financial itself was set up as the "master" account. All of IRA Financial's customers on the Gemini platform were subaccounts under IRA Financial's "master" account. Gemini's API, which is public, describes this as follows: "Gemini supports subaccount functionality which allows users to create multiple Gemini

accounts off of their primary account."[56] According to clients who say they were affected by the hack, IRA Financial clients were allocated "Trader" roles within the API and were not permitted to withdraw funds; only IRA Financial was permitted to withdraw funds.[57] It is not clear whether this master account-subaccount structure, in place after the switch to the API, was also in place before the switch to the API. It is also not clear whether IRA Financial knew about and approved this structure, or whether it considered having standalone accounts for each client instead of this master account-subaccount structure, and it is not clear why IRA Financial needed to have its own account at Gemini and have the power to withdraw client funds. It is not clear whether IRA Financial analyzed whether this structure, which was managed under the API, was secure and adapted to its particular business plan or its clients' needs.

iii. The Master Key; How the Cyberattack Happened

The Gemini API provides that a "group that contains multiple accounts can provision a Master API key." As the master account holder, IRA Financial would have been able to create a Master API key. Without the master account-subaccount structure, Gemini's API would not permit a Master API key to be created. It is unclear what, if anything, IRA Financial understood about its role as a master account holder within the API, or what it understood about the Master API key and its functions within the API. It appears that IRA Financial may have had no understanding of the cybersecurity implications of the master-subaccount structure, the Master API key, or the API.

As the cyberattack was taking place, IRA Financial staff logged on to the Gemini system and were able to observe that crypto assets in one IRA Financial client's account were being transferred to the Gemini account of another IRA Financial client. According to the complaint, "This shocked IRA [Financial], which was not aware that crypto assets could be transferred between customer sub-accounts. Since these were individual retirement accounts, there was no reason for transfers between those accounts. In fact, such transfers may violate federal law."

It appears that the master account-subaccount structure created on the Gemini platform is the feature that enabled the rapid transfers between subaccounts on the Gemini platform. With respect to the "Internal Transfers" API, the Gemini API states, "This API allows you to execute an internal transfer between any two accounts within your Master Group." If the master account-subaccount structure had not been used, it appears that the account-to-account transfers would not have been possible.

If there had been no master account-subaccount structure, the unauthorized withdrawals also would not have been possible, because no Master

API key, which circumvented the security protocols, could have been created. Gemini's platform provided security protocols such as multifactor authentication for account access and withdrawals, email confirmation for withdrawals, blocks on withdrawals for a certain amount of time after changes are made to an account, "whitelisting" of wallet addresses that are permitted to be used for withdrawals, fraud detection algorithms to detect unusual transaction patterns, and multi-signature storage of crypto assets to eliminate a single point of failure. Sub-account holders would receive the email confirmations, provide wallet addresses for whitelisting, and provide contact information for multifactor authentication.

However, the Master API key could be used to bypass all of these security protocols. The Gemini API states, "Master API keys can be used for any account level endpoint as well if the proper roles are assigned to it. For example, if a Master API key has the Administrator and Fund Manager roles assigned, the key can be used to check balances, create new deposit addresses and withdraw" and "Master API keys offer the convenience of invoking any account API on behalf of an account within that group."

Once the hackers accessed IRA Financial's Master API key, they were able to bypass the security protocols, including multifactor authentication, transfer assets between sub-accounts, and withdraw unlimited funds, making thousands of transactions within a very short period of time and stealing crypto assets from the IRA owners' accounts. When an attacker has access to a trading platform's API key, it can use the API key to program bots to quickly withdraw funds from the account or to perform multiple fraudulent trades.[58]

IRA Financial states that Gemini never informed it that the Master API key could be used to bypass the security protocols, permit account-to-account transfers and permit withdrawals, and states that if IRA Financial had been so informed, IRA Financial would have insisted that the Master API key be eliminated, or else IRA Financial would not have agreed to use the API.

IRA Financial describes the Master API key as a "single point of failure" within Gemini's API. However, it appears that the creation of the master-subaccount structure, which permitted the creation of the Master API key, resulted in a situation where IRA Financial itself, without its knowledge, became the single point of failure.

IRA Financial, by its own admission, did not understand the power of the Master API key.[59] Because IRA Financial held the Master API key without understanding its power, particularly within the master-subaccount structure, it failed to treat it as the cybersecurity risk that it was. In the words of one alleged victim of the IRA Financial hack, "Gemini might have built a security fortress, but for institutional customers they provide admins a master key, turn off the alarm system, and power down the cameras."[60]

IV. CONCLUSION

Many ERISA practitioners still remember the transitions from word processors to computers, library research to online research, and memos to emails. A generation of technological advances, together with the shift from defined benefit plans to defined contribution plans, has increased participants' exposure to cybersecurity risk. While fiduciaries have a duty of care to understand and mitigate the cybersecurity risks facing their plans, participants should not be required to bear the risk of loss to their accounts, which they cannot avoid and cannot be completely mitigated even by the most prudent fiduciaries. ERISA should be updated to protect participants' retirement savings from theft and fraud, whether via phone, email, fax machine, Minitel, teletype or compact disk.

NOTES

1. ERISA Advisory Council, *Privacy and Security Issues Affecting Employee Benefit Plans* (2011), https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2011-privacy-and-security-issues-affecting-employee-benefit-plans.pdf.

2. Barry L. Salkin, *Superseding Cause Under ERISA*, Benefits Law Journal, Vol. 35, No. 4, at 6, 11 (2022).

3. Business email compromise (BEC) is a type of social engineering fraud where an employee is misled into transferring money or making a payment to a cybercriminal based on fraudulent information provided to, and relied upon by, that employee. *See* INTERPOL, *Social Engineering Scams*, https://www.interpol.int/en/Crimes/Financial-crime/Social-engineering-scams; Federal Bureau of Investigation, *Public Service Announcement, Business Email Compromise: the $43 Billion Scam* (May 4, 2022), https://www.ic3.gov/Media/Y2022/PSA220504. The FBI reported nearly $2.4 billion in victim loss to BEC scams in 2021, a full third of the total cost of cybercrime. FBI *Internet Crime Report 2021*, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

4. Investment Company Institute, *Quarterly Retirement Market Data* (December 15, 2022), https://www.ici.org/statistical-report/ret_22_q3.

5. "The massive databases of personal and financial data that have been created and maintained by companies have become the target of cyberx attacks by nation states, hackers, and criminal groups. Law enforcement has documented the heightened risks of cyber breaches throughout the crypto ecosystem. In the past few years, these breaches have occurred with alarming frequency. Millions of personal and financial records have been stolen and huge losses to the companies and their investors have resulted. If consumer data falls into the wrong hands, there is a vibrant black market for stolen personal data, often posted on the dark web, and the risk of identity theft and fraud has increased dramatically." Consumer Privacy Ombudsman First Report to the Court, In re Celsius Network LLC, No. 22-10964, at 10 (Bankr. S.D.N.Y. January 27, 2023), https://cases.stretto.com/public/x191/11749/

PLEADINGS/117490127238000000086.pdf. The 2022 ERISA Advisory Council examined cybersecurity issues affecting health benefit plans. Its report had not been issued as of January 2023, https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2022-cybersecurity-issues-affecting-health-benefit-plans.pdf.

6. Austin R. Ramsey, *After Cyber Crime, Workplace Savers Face Long Odds to Get Repaid*, Bloomberg Law, August 20, 2022, https://news.bloomberglaw.com/daily-labor-report/after-cyber-crime-workplace-savers-face-long-odds-to-get-repaid; José M. Jara and Kelly Geary, *Is It Time for ERISA to Be Amended to Cover Cyber Crimes?*, 50 Tax Mgmt. Comp. Plan. J. No. 10 (Oct. 7, 2022), https://essential.bloombergindustry.com/?url=https%3A%2F%2Fwsauth.bloombergindustry.com%2Fwsauth%2Fbltxauth%3Ftarget%3Dhttps%253A%252F%252Fwww.bloomberglaw.com%252Fproduct%252Ftax%252Fdocument%252FXEMMJFRG000000%253Fbc%253DW1siQ29tcGVuc2F0aW9uIFBsYW5uaW5nIEpvdXJuYWwiLCIvcHJvZHVjdC90YXgvbGF3X3JlcG9ydHMvQk5BQ1BKIl1d--97a3150c7ac68e76d9519889d44a53e9064f9b88%2526jcsearch%253Dbna%25252520A0R9G7C4F9#jcite.

7. Congressional Research Service, *A Visual Depiction of the Shift from Defined Benefit (DB) to Defined Contribution (DC) Pension Plans in the Private Sector* (December 27, 2021), https://crsreports.congress.gov/product/pdf/IF/IF12007.

8. "Crypto assets" is used to refer to cryptocurrencies as well as assets marketed as "tokens", "coins", and other "digital assets."

9. "In the past, the use of cryptocurrency was regularly reported in other crime types seen at the IC3 [Internet Crime Complaint Center] (e.g., tech support, ransomware, employment), however, it was not identified in BEC-specific crimes until 2018. By 2019, reports had increased, culminating in the highest numbers to-date in 2021 with just over $40M in exposed losses. Based on the increasing data received, the IC3 expects this trend to continue growing in the coming years." FBI, *supra* note 3.

10. EBSA, 401(k) Plan Investments in "Cryptocurrencies," Compliance Assistance Release No. 2022-01 (March 10, 2022), https://www.dol.gov/agencies/ebsa/employers-and-advisers/plan-administration-and-compliance/compliance-assistance-releases/2022-01.

11. *See* Salkin, *supra* note 2, at 11, for a discussion of the challenges to establishing causation under ERISA section 409(a) in the cybersecurity context. As he notes, "[w]hile some causation issues under ERISA are frequently litigated [. . .], other issues, such as the type of causation required under ERISA Section 409, are infrequently discussed. However, with the increase in cybersecurity incidents directed towards tax-qualified plans, and likely to affect other types of benefits plans as well, it is likely that these issues will be increasingly litigated."

12. ERISA Advisory Council, *Cybersecurity Considerations for Benefit Plans* (2016), https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2016-cybersecurity-considerations-for-benefit-plans.pdf.

13. EBSA, Tips for Hiring a Service Provider with Strong Cybersecurity Practices (April 14, 2021), https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/tips-for-hiring-a-service-provider-with-strong-security-practices.pdf; EBSA, Online Security Tips (April 14, 2021), https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf; EBSA, Cybersecurity Program Best Practices (April 14, 2021) https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf.

14. EBSA, IL 12-01-1997, Information Letter to Theodore Konshak (December 1, 1997) https://www.dol.gov/agencies/ebsa/about-ebsa/our-activities/resource-center/

information-letters/12-01-1997; EBSA, Tips for Selecting and Monitoring Service Providers for Your Employee Benefit Plan (undated), https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/our-activities/resource-center/fact-sheets/tips-for-selecting-and-monitoring-service-providers.pdf.

15. Walsh v. Alight Sols., 44 F.4th 716, 723 (7th Cir. 2022).

16. EBSA, Tips for Hiring a Service Provider with Strong Cybersecurity Practices, *supra* note 13.

17. EBSA, Cybersecurity Program Best Practices, *supra* note 13.

18. For detailed discussions of cybersecurity fiduciary responsibilities and best practices for plan fiduciaries, *see* Michelle Capezza, *Practice Note: ERISA Fiduciary Responsibilities and Cybersecurity for Retirement Plans*, Practical Law, and Michelle Capezza, *Practice Note: Best Practices for ERISA Fiduciary Responsibilities and Cybersecurity for Retirement Plans*, Practical Law.

19. FDIC-regulated banking institutions are responsible for fraud losses to consumer bank accounts under Regulation E of the Electronic Funds Transfer Act, https://www.consumerfinance.gov/rules-policy/final-rules/electronic-fund-transfers-regulation-e/. As a result, banks typically have private insurance policies covering fraud losses. *See* Robert K. Knake, *No, the FDIC Doesn't Insure Your Bank Account Against Cybercrime (and Why That Is OK)*, Council on Foreign Relations Blog (December 2, 2015), https://www.cfr.org/blog/no-fdic-doesnt-insure-your-bank-account-against-cybercrime-and-why-ok.

20. In 2022, the ERISA Advisory Council engaged in an examination of cybersecurity insurance and the role that it plays in addressing cybersecurity risks for employee benefit plans, including the interplay between a plan's existing cybersecurity practices and the availability and cost of cybersecurity insurance coverage. Its report had not been issued as of January 2023, https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2022-cybersecurity-insurance-and-employee-benefit-plans.pdf. However, as noted above, cybersecurity insurance policies typically are intended to cover losses related to data and information, not amounts stolen from participant accounts. *See* Presentation by Matt Klein, Willis Towers Watson, to the ERISA Advisory Council (September 8, 2022), https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2022-cybersecurity-insurance-and-employee-benefit-plans-written-statement-klein-09-08.pdf

21. Decision And Order, Disberry v. Employee Relations Committee of the Colgate-Palmolive Company, No. 22 Civ. 5778, 2022 WL 17807188 (S.D.N.Y. Dec. 19, 2022), https://casetext.com/case/disberry-v-emp-relations-comm-of-the-colgate-palmolive-co.

22. Complaint, Bartnett v. Abbott Laboratories, No. 1:20-cv-02127 (N.D.Ill. October 30, 2020), https://si-interactive.s3.amazonaws.com/prod/planadviser-com/wp-content/uploads/2020/11/30113600/BartnettvAbbottAmendedComplaint.pdf.

23. Complaint, Berman v. Estee Lauder Inc., No. 3:19-cv-06489 (N.D.C.A. October 9, 2019), https://si-interactive.s3.amazonaws.com/prod/plansponsor-com/wp-content/uploads/2019/10/14132939/BermanvEsteeLauderComplaint.pdf.

24. EBSA has been investigating Alight since 2019 to determine whether any violations of Title I of ERISA have occurred. Order, Walsh v. Alight Sols., No. 1:20-cv-02138 (N.D.Ill. October 28, 2021), https://si-interactive.s3.amazonaws.com/prod/plansponsor-com/wp-content/uploads/2021/12/02120018/WalshvAlightOrder.pdf.

25. Complaint, Griffin v. Gemini Trust Co., LLC and IRA Financial Trust Co., No. 3:22-cv-01747 (N.D.C.A. March 18, 2022), https://www.scribd.com/document/577275663/

Gemini-and-IRA-Financial-Class-Action. Gemini successfully compelled arbitration; the case was dismissed against IRA Financial for improper venue.

26. Complaint, IRA Financial Trust v. Gemini Trust Company, LLC, No. 1:22-cv-04672 (S.D.N.Y. June 6, 2022), https://s3.documentcloud.org/documents/22054489/ira-v-gemini-complaint.pdf; Complaint, Wesco Insurance Co. v. IRA Financial Group LLC, No. 1:22-cv-23507 (S.D.Fla. October 27, 2022), https://assets.law360news.com/1544000/1544317/https-ecf-flsd-uscourts-gov-doc1-051125215645.pdf. Gemini successfully compelled arbitration in the IRA Financial v. Gemini case; the Wesco v. IRA Financial case is ongoing as of January 27, 2023. *See* Sarah Jarvis, *Insurer Says No Coverage For Claims Over $36M Crypto Theft*, Law360 (October 28, 2022), https://www.law360.com/articles/1544317.

27. *See* Carol Buckmann, *Another Cybertheft Lawsuit Spotlights 401(k) Recordkeeper Procedures* (July 17, 2022), https://cohenbuckmann.com/insights/2022/7/17/another-cybertheft-lawsuit-spotlights-401k-recordkeeper-procedures;. Jara and Geary, *supra* note 6.

28. *See* Crystal Blockchain, *Crypto & DeFi Hacks, Fraud & Scams Report*, at 7 (July 2022), https://crystalblockchain.com/security-breaches-and-fraud-involving-crypto/; Immunefi, Crypto Losses in 2022 Annual Report (2022), https://immunefi.com/reports/.; Consumer Financial Protection Bureau (CFPB) Complaint Bulletin: An analysis of consumer complaints related to crypto-assets (November 2022), https://files.consumerfinance.gov/f/documents/cfpb_complaint-bulletin_crypto-assets_2022-11.pdf.

29. *See* Crystal Blockchain, *supra* note 28, at 14. As a baseline, Crystal Blockchain notes that, while it is challenging to completely prevent breaches of security systems, particularly in relation to internet-connected hot wallets, it is possible for crypto exchanges to have mechanisms that will protect customers in the event of a breach, including blockchain analytics software, an in-house security team, proper insurance and backup reserves equivalent to the amount of crypto held in online storage.

30. U.S. Department of the Treasury, *Crypto-Assets: Implications for Consumers, Investors, and Businesses*, at 34 (September 2022), https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf.

31. Department of Labor Regulation §2550.404a-1(b). As noted in the preamble to the regulation, "plan fiduciaries may not add imprudent investment options just because participants request or would prefer them." Department of Labor, *Prudence and Loyalty in Selecting Plan Investments and Exercising Shareholder Rights* (December 1, 2022), 87 FR 73822, at 73842.

32. "[E]ven in a defined-contribution plan where participants choose their investments, plan fiduciaries are required to conduct their own independent evaluation to determine which investments may be prudently included in the plan's menu of options," Hughes v. Northwestern University, 142 S.Ct. 737, 742 (2022).

33. EBSA, 401(k) Plan Investments in "Cryptocurrencies," *supra* note 10.

34. Financial Stability Oversight Council, *Fact Sheet: The Financial Stability Oversight Council's Report on Digital Asset Financial Stability Risks and Regulation* (October 3, 2022), https://home.treasury.gov/system/files/261/Fact-Sheet-Report-on-Digital-Asset-Financial-Stability-Risks-and-Regulation.pdf; Financial Stability Oversight Council, *Report on Digital Asset Financial Stability Risks and Regulation* (October 3, 2022), https://home.treasury.gov/system/files/261/FSOC-Digital-Assets-Report-2022.pdf.

35. Complaint, SEC v. Genesis Global Capital, LLC and Gemini Trust Company, LLC, No. 1:23-cv-00287, at 15 (S.D.N.Y. January 12, 2023), https://www.sec.gov/litigation/complaints/2023/comp-pr2023-7.pdf.

36. *See* SEC Staff Accounting Bulletin, 17 CFR 211.121 (2022), https://www.sec.gov/oca/staff-accounting-bulletin-121; New York State Department of Financial Services Guidance on Custodial Structures for Consumer Protection in the Event of Bankruptcy (January 23, 2023), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20230123_guidance_custodial_structures. In the Celsius bankruptcy case, the bankruptcy court held that certain customer deposits held by the bankrupt cryptocurrency exchange are property of the bankruptcy estate and not customer property (Memorandum Opinion and Order Regarding Ownership of Earn Account Assets, In re Celsius Network LLC, No. 22-10964 (Bankr. S.D.N.Y. January 4, 2023), https://cases.stretto.com/public/x191/11749/PLEADINGS/1174901042380000000067.pdf. "Absent sufficient digital assets to cover all customer claims, customers may find themselves fighting to recover a pro rata portion of assets they may legally own. Furthermore, crypto bankruptcies involving fraud or Ponzi schemes may subject commingled customer assets to government forfeiture or restitution orders, further complicating customer recoveries." Jessica Liou and John Marinelli, *Crypto Bankruptcies Shed Light on Who Owns Assets for Recovery*, Bloomberg Law (January 27, 2023), https://www.bloomberglaw.com/login?target=https%3A%2F%2Fwww.bloomberglaw.com%2Fbloomberglawnews%2Fus-law-week%2FXD8GJFJ0000000%3Fbna_news_filter%3Dus-law-week#jcite.

37. EBSA, 401(k) Plan Investments in "Cryptocurrencies," *supra* note 10.

38. The Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC), *Joint Statement on Crypto-Asset Risks to Banking Organizations* (January 3, 2023), https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf.

39. Particular attention should be paid to how U.S. dollars will enter and leave the potential investment, and what banking partners and other entities are being relied on in the proposed arrangement, and the cybersecurity aspects of these transactions. The Federal Reserve has stated that a state member bank "must at all times conduct its business and exercise its powers with due regard to safety and soundness.[...] With respect to any novel and unprecedented activities, such as those associated with crypto-assets or use of distributed ledger technology, it is particularly important for a state member bank to have in place appropriate systems to monitor and control risks, including liquidity, credit, market, operational (including cybersecurity and use of third parties), and compliance risks (including compliance with Bank Secrecy Act and Office of Foreign Asset Control requirements to reduce the risk of illicit financial activity). Federal Reserve supervisors will expect state member banks to be able to explain and demonstrate an effective control environment related to such activities." Federal Reserve, *Policy Statement on Section 9(13) of the Federal Reserve Act*, 88 FR 7848 (February 7, 2023), https://www.federalregister.gov/documents/2023/02/07/2023-02192/policy-statement-on-section-913-of-the-federal-reserve-act.

40. Security of a private key (including any seed phrase used to authenticate a private key) is essential to maintaining security of crypto assets, whether the key is kept in cold (offline) or hot (online) storage. This was illustrated in 2020, when a thief used his brother's credentials to steal millions of dollars in digital assets from his brother's hardware wallet (a device that creates a secure public/private keypair that can interact with a wallet on a blockchain), which had been seized by federal agents. *See Explained, Why the Feds couldn't secure a crypto hardware wallet*, Protos (October 11, 2022), https://protos.com/explained-why-the-feds-couldnt-secure-a-crypto-hardware-wallet/; Department of Justice Press Release, *Ohio Man Pleads Guilty for Unlawfully Stealing Over 712 Seized Bitcoin Subject to Forfeiture in Brother's Pending Criminal Case* (January 6, 2023), https://www.justice.gov/usao-dc/pr/ohio-man-pleads-guilty-unlawfully-stealing-over-712-seized-bitcoin-subject-forfeiture. For a summary explanation of

crypto assets and private key custody, *see* Final Report of Shobha Pillay, Examiner, In re Celsius Network LLC, No. 22-10964, at 48 (Bankr. S.D.N.Y. January 31, 2023), https://cases.stretto.com/public/x191/11749/PLEADINGS/1174901312380000000039.pdf.

41. *See* Luke Bailey, *How Gold Coin Tax Ruling May Apply to IRA Crypto Holdings*, Law360 (February 18, 2022) https://www.law360.com/tax-authority/articles/1466286/how-gold-coin-tax-ruling-may-apply-to-ira-crypto-holdings.

42. Board of the IOSCO, *Final Report, Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms* (February 2020), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf. IOSCO is an association of primary securities and futures regulators from over 130 jurisdictions, including the U.S. Securities and Exchange Commission and the Commodity Futures Trading Commission.

43. Crypto lenders Celsius, Voyager, BlockFi and Genesis have all filed for chapter 11 bankruptcy in the last six months. *See* Rahul Nambiampurath, *Crypto Lending Platforms Hit Hard as Contagion Spreads*, Investopedia (January 24, 2023), https://www.investopedia.com/crypto-lenders-crisis-7098041; Alexander Osipovich, *Genesis Demise Marks End of Era for Crypto's Pseudo-Banks*, The Wall Street Journal (January 22, 2023), https://www.wsj.com/articles/genesis-demise-marks-end-of-era-for-cryptos-pseudo-banks-11674342330; Genesis Global Holdco, LLC, et al., Case No. 23-10063 (Bankr. S.D.N.Y. January 19, 2023). For a summary of the rise and fall of the crypto asset markets to date, see Final Report of Shobha Pillay, Examiner, *supra* note 40, at 58.

44. SEC Press Release, *SEC Charges Genesis and Gemini for the Unregistered Offer and Sale of Crypto Asset Securities through the Gemini Earn Lending Program*, PR 2023-7 (January 12, 2023), https://www.sec.gov/news/press-release/2023-7; Complaint, SEC v. Genesis Global Capital, LLC and Gemini Trust Company, LLC, *supra* note 35.

45. *See SEC Investor Alert: Self-Directed IRAs and the Risk of Fraud* (February 7, 2023), https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/investor-14; Jesse Hamilton, *SEC Warns That Retirement Accounts' Crypto Stakes May Be Unregistered Securities*, Coindesk (February 7, 2023), https://www.coindesk.com/policy/2023/02/07/sec-warns-that-retirement-accounts-crypto-stakes-may-be-unregistered-securities/.

46. Complaint, IRA Financial Trust v. Gemini Trust Company, *supra* note 26, https://s3.documentcloud.org/documents/22054489/ira-v-gemini-complaint.pdf. *See also* Gina Kim, *IRA Biz Blames Winklevoss-Run Gemini in $36M Crypto Theft*, Law360 (June 6, 2022), https://www.law360.com/articles/1500106.

47. Letter from Letitia James, New York State Attorney General, to Senators Wyden and Crapo and Representatives Neal and Brady Re: Legislation to Protect Individual Retirement Accounts and Defined Contribution Plans from the Risks of Digital Assets (November 22, 2002), https://ag.ny.gov/sites/default/files/letter_to_congress_2022-11-22_1424.pdf.

48. Danny Nelson, *Drained Crypto Accounts at IRA Financial Leave Victims Searching for Answers*, Coindesk (February 15, 2022), https://www.coindesk.com/business/2022/02/14/drained-crypto-accounts-at-ira-financial-leave-victims-searching-for-answers/. *See also* William Turton, *IRA Financial Hacked, $36 Million in Cryptocurrency Stolen*, Bloomberg (February 14, 2022) (reporting that blockchain analysis firm Chainalysis Inc. said it was tracking the $36 million in cryptocurrency stolen from IRA customers, and said that it was being laundered through a "mixer" service known as Tornado, and quoting clients stating that their Gemini accounts only held cash, which was also stolen). According to blockchain security company Slowmist, the

movement of the proceeds of the IRA Financial hack follows the money laundering techniques used by the "Lazarus Group" North-Korea-sponsored hacking organization; however, no hacker has yet been identified by law enforcement, https://www.bloomberglaw.com/login?target=https%3A%2F%2Fwww.bloomberglaw.com%2Fproduct%2Fblaw%2Fdocument%2FR7B2OGT0AFB4%3Fcriteria_id%3Dbda183835688176c3b3e3c38bc2d90db%26searchGuid%3Dcfeee80a-9c5c-458c-b2b5-d641a2a8fdc1. Slowmist, *2022 Annual Blockchain Security and AML Analysis Report* (2022), https://www.slowmist.com/report/2022-Blockchain-Security-and-AML-Analysis-Annual-Report(EN).pdf.

49. The Gemini API describes "Master API Keys" as follows: "A group that contains multiple accounts can provision a Master API key. Master API keys offer the convenience of invoking any account API on behalf of an account within that group. To invoke an API on behalf of an account, add that account's nickname as an account parameter to your request payload. Master API keys are formatted with a prepending master-, while account level API keys are formatted with a prepending account-. The account parameter may be used on any API that performs an action for or against a single account." Gemini API, https://docs.gemini.com/rest-api/#private-api-invocation (last visited January 27, 2023).

50. Nelson, *supra* note 48.

51. Complaint, IRA Financial Trust v. Gemini Trust Company, *supra* note 26, at 28.

52. IRA Financial, https://www.irafinancialgroup.com/about-us/ (last visited January 27, 2023).

53. Complaint, Griffin v. Gemini Trust Co., LLC and IRA Financial Trust Co., *supra* note 25, at 7.

54. The Gemini website states, "Gemini is a fiduciary and qualified custodian under New York Banking Law and is licensed by the State of New York to custody digital assets." Gemini, https://www.gemini.com/custody (last visited January 27, 2023).

55. IRA Financial *Client Q&A: Crypto Loans, Reporting Solo 401(k) Distribution And More* (March 4, 2021), https://old-prod.irafinancialgroup.com/learn-more/podcast/episode-twenty-seven/. Genesis's (and as a result Gemini's) Earn program froze withdrawals in November 2022 and Gemini Earn participants have not been able to withdraw their crypto assets as of January 27, 2023. IRA provider Bitcoin IRA also permitted IRA owners to participate in an "IRA Earn" program through Genesis, which offered interest rates as high as 6% annually (at the time, the average national rate was 0.05%), but has stated that it ceased the IRA Earn program in mid-2022, before Genesis suspended withdrawals in November 2022. and filed for bankruptcy in January 2023. SEC Press Release, *SEC Charges Genesis and Gemini for the Unregistered Offer and Sale of Crypto Asset Securities through the Gemini Earn Lending Program, supra* note 44. Bitcoin IRA Press Release, *Bitcoin IRA™ Offers the first IRA Earn™ Program with up to 6% APY on Cash and Crypto Exclusively through Genesis* (February 4, 2021), https://www.prnewswire.com/news-releases/bitcoin-ira-offers-the-first-ira-earn-program-with-up-to-6-apy-on-cash-and-crypto-exclusively-through-genesis-301221926.html; Ben Strack, David Canellis and Jon Rice, *Circle Yield Reduced to Zero, Gemini Earn Paused as Genesis Contagion Spreads*, Blockworks (November 16, 2022), https://blockworks.co/news/gemini-circle-genesis-exposure.

56. Gemini API, *supra* note 49.

57. Comment by user "LucidBTC," *Ira Financial and Gemini,* Reddit R/Gemini (February 10, 2022), https://www.reddit.com/r/Gemini/comments/sp7raq/ira_financial_and_gemini.

58. *See* Consumer Privacy Ombudsman First Report to the Court, *supra* note 5, Appendix C.

59. Complaint, IRA Financial Trust v. Gemini Trust Company, LLC, *supra* note 26 at 22, 23.

60. Comment by user "LucidBTC," *Security and Liability Concerns for Gemini Institutional Customers*, Reddit r/Gemini (February 16, 2022), https://www.reddit.com/r/Gemini/comments/su8yys/security_and_liability_concerns_for_gemini/.