What the FTX Scandal Reveals About Third Party Risk Evaluation

By Charles Cresson Wood

In light of the recent FTX scandal, this article takes a look at the third party risk evaluations that should take place going forward.

Abstract

The fact that a well-known cryptocurrency exchange (FTX) – not long ago valued at $32 billion – could go to a $0 valuation in several days should get our attention. Worse still, FTX was revealed to have no complete list of its bank accounts, no separation of customer funds and company funds, no complete list of its employees, and no Board of Directors. It also lacked adequate teams to handle cash management, accounting, auditing, risk management and information security. These and other deficiencies reportedly enabled frauds and thefts of customer funds to the tune of billions of dollars. At the same time, the firm was recommended by well-known newspapers, venture capital firms, investment firms, and high-visibility celebrities. If investors and third-party business partners relied upon these endorsements, in order to make decisions to trust FTX, they would now be suffering heavy losses. The fact that this sketchy FTX operation went on for years without receiving regulatory scrutiny, civil suits, and/or criminal prosecutions, indicates that private sector firms need to more aggressively do their own due diligence, and stop assuming that others have done, or will do, the work for them. This improved due diligence must be able to illuminate what's happening behind the scenes, for example in the domain of information security and privacy. What is now needed is an expedient, inexpensive, and more illuminating way to evaluate the state of corporate governance at other firms. What is also now needed is the increased use of third-party auditors who perform more significant due diligence testing, including the status of information security and privacy.

The FTX debacle demonstrates that private sector firms cannot realistically expect that regulations, the criminal or civil legal systems, or "the word" through the marketplace, is going to protect them. Private sector firms must now be considerably more proactive, and rather than waiting, as is too often the case, until things fall apart, and then reactively trying to put the broken pieces back together [1]. The tools now often used to measure third party risk, in the information security and privacy area, as well as in other areas, do not sufficiently and proactively evaluate the trustworthiness of third parties. They focus instead on external presentations of controls, which of course are important – but what is also needed is a look at the inside, specifically the state of corporate governance, and the attitude from the top ("tone from the top"). To fill this significant gap in third party risk evaluation, a new and much more revealing type of due diligence audit is required. This article discusses that type of more in-depth and more aggressive due diligence audit. With this new type of audit, private sector firms can protect themselves from the negligence and recklessness of other firms (like FTX), and from the fraudulent activity and theft of other firms as well (like FTX). This more aggressive risk evaluation approach is ready-to-go, is based on both existing professional standards and historically demonstrated independent auditing techniques and can also be practically deployed at firms in all industries.

Levels of Vetting and Trust

There are four significant general levels of vetting for third-party firms that need to be distinctly named, in order for a truly defensible, grounded, and reasonable decision, to trust and rely on another firm, to be achieved. This vetting is particularly important when negotiating outsourcing and hosting deals, security-as-a-service (SECaaS) deals, and managed security services (MSS) deals. The level of risk associated with establishing or renewing a relationship will determine how far along in this spectrum of four categories a firm evaluating a third party will want to go. The more potential risk involved, the farther along this spectrum the evaluating firm should go. These four categories are cumulative. For example, the first category can be performed alone. The second category is performed along with the first, the third category is performed along with both the first and the second, and the fourth is performed along with the first, second, and third. Since the FTX situation was so blatant and easily detectible, that will be the focus of the following discussion about these four levels. So as to focus

only on vetting, the following analysis deliberately omits many important parts of a vendor risk management program such as a risk rating system.

1. **Self-Advertised and Claimed Capabilities**: With this vetting approach, the third-party firm in question, in advertisements and in its own qualification materials, claims that it can perform certain tasks, take care of certain things, has certain internal operational systems, and/or has been diligent in the domain of information security and privacy. These claims may appear on websites or in questionnaires that the third-party firm in question returns to the evaluator firm. These claims may be made along with the provision of financial statements, information security policy statements, disaster recovery plans, periodic scans of configurations, or other so-called evidence indicating that the firm is truly diligent in information security and privacy (or any other area). These claims of diligence may also appear in certain government reports such as the public company revelations appearing in Forms 10-K and 10-Q. In all cases where any significant trust is being placed in a third-party firm in question, performance of this level of vetting will be insufficient to proceed with a decision to trust. But a poor showing at this level of vetting may be enough to disqualify the firm from further consideration about a relationship. For example, FTX clearly made false and misleading statements in its advertising. For example, it published statements like "no risk," "can't lose," and "guaranteed return." While these claims are worthy of a Federal Trade Commission false advertising investigation, they could also legitimately have been the end of a due diligence process for those seriously looking into whether FTX is a trustworthy entity. If the entity in question has already clearly been shown to be disrespecting common business laws and regulations, it's unlikely that it will be respecting the terms and conditions found in a contract with your firm.
2. **Apparently Unrelated Third-Party Recommendation**: With this vetting approach, a different third-party firm, which has no obvious and apparent connection to the third-party firm in question, endorses, recommends, or otherwise urges others to do business with the third-party firm in question. US federal law [2], as well as many state laws, require that paid endorsements for certain types of products be labeled as such. That labelling was not done with many FTX endorsers. An active lawsuit in Florida [3] alleges those paid endorsements were not so labeled, and that damages of $11 billion are owed. In those instances, apparently this vetting category effectively became the same as the Self-Advertised and Claimed Capabilities category. FTX was recommended and endorsed by celebrities and sports stars, well-known venture capital firms, giant software firms, investment management houses, and other high-visibility sources. The amount of money that a third-party firm in question spends on advertising and public relations should have nothing to do with the due diligence results. Although not expressly stated, in the minds of many people doing trust evaluations, the implication was that somebody somewhere in this long list of luminaries had already done the due diligence on FTX, so an investor or potential business partner didn't need to do that work (a dangerous assumption). Just as these recommendations in the case of FTX were effectively advertising, any unvouched information found on the Internet should fall into this same vetting category. Similarly, recommendations provided by the firm being evaluated, that cannot independently be verified as truly independent, should be taken with a huge "grain of salt" because the parties making those recommendations may just be shills. Recommendations that really aren't relevant, because they don't cover the scope of the matter of interest, should also be seriously discounted. For example, while FTX did have a "clean" financial audit, this audit work did not involve an evaluation of internal controls, something which is required for larger companies. Therefore, the final result of the accounting process (the financial statements) looked good to the auditors, but they had no basis on which to trust the underlying systems that generated those final results. A similar issue can happen with some information security and privacy due diligence tests, in that the final results can be falsified, because the underlying internal control systems were not examined (for example, a privacy policy can be posted on a web site, but not be implemented). Likewise, some sort of fashionable or trendy support for the firm in question, some evidence that other firms were deciding to trust because they are "caught up in the dream," or that other firms were deciding to trust because they felt like they "had to have a piece of the action" – all of which were true for FTX – should be considered red flags. In most cases, the recommendations and endorsements in this category, would be insufficient to proceed with a decision to trust the firm in question, if there is a significant degree of reliance to be placed on the third-party in question. More persuasive evidence should be still needed. For a relatively unimportant matter, this level of vetting may be sufficient.
3. **Independent Third-Party Audit**: In this category of vetting, an independent third party, such as an independent auditor performing a SOC2 audit [4], reviews the activities of the third-party firm in question, and then expresses a professional opinion about the propriety and rightness of the claims made by the third-party firm in question. A single professional opinion may be used by many parties seeking to know more about the trustworthiness of the third-party firm in question [5]. This type of vetting is sufficient in many cases where there is a low-level but significant dependency or reliance to be placed in the third-party firm in question. But this same third-party auditor must be shown to be demonstrably independent, and also must be at significant risk of losing its license, if it were to misrepresent the circumstances at the third-party firm in question (discussed further below). While reports like a SOC2 report, a PCI-DSS report [6], a HITRUST CSF certification [7], or an ISO 27001 certification [8], would fall into this category of vetting, and while these approaches are highly recommended, they all suffer from a significant problem. That is that they all look only at control manifestations – they do not look at corporate culture, the tone-at-the-top, and whether the Directors & Officers are actually

incentivized to support controls and also whether they are attending to their fiduciary duties to third parties such as shareholders [9]. In other words, the trappings of good security and privacy can be found, and the firm in question can pass this type of audit, but without there being a way to measure of corporate culture, the tone-at-the-top, and a leadership commitment to having good information security and privacy, the sustainability over time of the current desirable status is highly questionable. Thus, it is far better to have both control-related audits combined with an audit of corporate governance, the tone-at-the-top, and the commitment of Directors & Officers to information security and privacy. In general, since information security and privacy are both so complex, it is advisable to simultaneously obtain a variety of different types of Independent Third-Party Audit reports, and in some cases that multiple report approach may be an adequate alternative to moving-up to the next vetting level. Beyond an audit of the financials (looking only at the results presented, not the internal controls used to generate those statements), this author could find no evidence that such an Independent Third-Party Audit was performed for FTX by a demonstrably independent party. If a corporate-governance-related audit had been performed, along the lines of that just mentioned, the firm receiving the results would no doubt have decided not to trust FTX. This is because such an audit would have revealed a panorama of failed corporate governance mechanisms, such as extensive self-dealing, large personal loans to insiders, use of a group email account to share "private keys," and no centralized cash management system.

4. **Sponsored Independent Third-Party Audit**: For those situations in which using an Independent Third-Party Audit of the third-party firm in question is not sufficient (very high risk and very high dependency situations), the next level of vetting sophistication involves directly paying for an independent third-party audit so as to make sure there are no hidden conflicts of interest. In those cases where hundreds of millions of dollars are at risk, or where a significant number of human lives are at stake, or perhaps where there exists a grave potential danger to the environment, this level of vetting is absolutely the way to go. Where the firm choosing whether to trust has considerable leverage over the relationship – such as (a) a venture capital firm about to invest in a start-up, (b) a bank about to make a large loan, (c) a firm about to disclose an important trade secret, or (d) an insurance company contemplating whether to issue Directors' & Officers' liability insurance – it is in cases like these that this vetting approach is very illuminating. This type of vetting has the benefit that the financial sponsor (here the firm making a decision to trust) gets to choose the third-party auditor, and also gets to review the propriety of the auditor independence screening process. This type of vetting is somewhat akin to what is done in England, for publicly held companies, where the shareholders (not senior management and not the Audit Committee) select the independent financial auditor. This latter English approach is markedly better than the American approach, because the auditor, with the English approach, is not financially beholden to the same firm that he/she is auditing. With this fourth type of vetting, the auditor is thus not incentivized to paint a rosy picture because he/she wants to get the next year's audit engagement. Another example of the vetting falling into this category is where firms making a decision to trust send their own staff auditors out to do site visits, and then count inventory, inspect claimed equipment, assess environmental risks to a data center, etc. This author could find no public mention of any such Sponsored Independent Third-Party Audit project having been performed for FTX. If such an auditor had actually visited the FTX facilities in the Bahamas and seen the way staff lived/worked/played together in a communal mansion, no doubt that situation would not appear like a serious center of operations for an international crypto exchange worth $32 billion. Once this fact was revealed by the audit, the firm doing the evaluation would probably decide not to trust FTX.

In terms of an overview of these four levels of vetting, decisions to trust a firm in question, relationships involving any significant level of risk or dependency, should at least involve an Independent Third-Party Audit. In many cases, several different types of these same audits will be required. The types of Independent Third-Party Audits employed should not exclusively be assessing the controls in question, but also evaluating the corporate culture and top management commitment (the tone-at-the-top), so as to ensure that top management will follow through with the right actions until such time as the next audit takes place. The measurement of the tone-at-the-top is necessary because these audits are relatively expensive, and cannot generally be performed continuously, as some types of technical audits can be (such as automated network configuration checking). In between the times when these more expensive types of audits are performed, there must be credible governance and management mechanisms in place to assure that prudent decisions about information security and privacy will in fact continue to be made. But how exactly can that objective be practically achieved? The next section answers that question.

As an aside, it should be said that several well-known firms, each of which invested hundreds of millions of dollars in FTX, claimed that they did "extensive due diligence," that there was "nothing else [of a due diligence nature] could be done," and that there were no "red flags." This author highly doubts these unsupportable assertions and considers the statements to be intended to limit the future liability of those uttering them (good luck with that). A number of different types of audits, in the category three and four vetting processes mentioned above, would have rapidly revealed that FTX not only was a fraud and Ponzi scheme, but also that it had extremely weak, and effectively non-existent, corporate governance practices.

Sarbanes Oxley Shows Us the Way Forward

In the wake of scandals like Enron, Tyco, and WorldCom, the US Congress enacted the Sarbanes-Oxley Act of 2002. That highly influential law was a big step beyond what had existed before, because it pointed-out the fact that it was not enough to simply have an auditor review the results of the accounting process (the finished version of the financials). Indeed, in all of these named giant Dot-Com era scandals, the "books had been

cooked" through a variety of sophisticated accounting tricks, such as the use off-shore entities to hide loans obtained to cover-up losses. To help prevent these and other abuses, Sarbanes-Oxley now requires that both the CEO and CFO personally attest to their personal knowledge about the adequacy of internal controls related to the financial accounting system, and to put that attestation in writing. This exposes the CEO and the CFO to personal liability for any misrepresentations since the company in question is publicly listed [10]. For publicly held companies, making false or misleading statements, or concealing material information, is a very big deal, and there has been considerable litigation on this point [11].

The Sarbanes-Oxley Act was additionally important because it illuminated that, to have the financial statements be truly reliable and credible, issuing firms had to have an appropriate tone-at-the-top (attitude of the Directors & Officers) dictating a culture of integrity and compliance with the law. That same tone-at-the-top is something that urgently needs to be measured, and attested to, in the information security and privacy area [12]. There is a process to do that, a process to use an independent attorney to attest to the fact that the Directors & Officers are attending to the minimum legally-defined fiduciary duties, and that process falls into either the third or the fourth of the vetting categories mentioned above. For those situations where there is a lot of money at risk (such as a merger or acquisition), or something very important is at stake (a trade secret is being revealed to a third party), or where a badly damaged reputation needs to be restored (such as after a major publicized breach), such a level of auditing of the tone-at-the-top at a third-party firm in question is absolutely warranted. This type of audit, this evaluation of the tone-at-the-top, naturally complements a SOC2 audit, ISO 27001 certification, independent penetration test audits, and other Independent Third-Party Audit approaches. That is because this evaluation of the tone-at-the-top covers the legally defined corporate governance and management areas that are not covered by SOC2 audits, ISO 27001 certifications, or related audits that look at controls.

Alignment of Incentive Systems

Embedded within the auditing approaches mentioned above there are typically a variety of ways that engagements are structured so that the auditor is always going to produce a quality work product. While the details are outside the scope of this article, these include a scripted process that auditors must follow, a rigorous independence screening process, the ability to have the auditor himself/herself audited by another auditor, a professional disciplinary process, and the possibility that a lawsuit involving malpractice might be brought. These go a long way to assure that the independent auditor's opinion can confidently be relied upon, and that the situation described in the opinion is in fact true. However, what is not generally aligned at many firms are the actions of the Directors & Officers. Often short-term financial considerations win-out over controls. For example, at FTX, the management allegedly allowed staff to use customer funds, without any customer authorization, to purchase houses for themselves, and the legal title to those houses was then placed in the names of the staff. No loan documentation was reportedly generated. Of course, this type of an arrangement was in blatant violation of the duty of care that a fiduciary accepting funds belonging to another owes the other providing those funds. But in the absence of an independent auditor's report revealing such behaviors, these problems will lurk in the shadows, and come to light only when there's a problem, such a bankruptcy, a lawsuit, or a whistle-blower's report. As Warren Buffett has famously said, "When the tide goes out, you find out who is swimming naked."

The answer to the Director & Officer incentive alignment issue lies in the domain of corporate governance. This is why it is so very important to have these independent audits look at the actions of the Directors & Officers, not simply look at technical and operational controls that have manifested some intention to have adequate information security and privacy. Such a corporate governance audit can for example be performed by using a third-party attorney auditor to evaluate whether the Directors & Officers are currently in compliance with all their legal duties in the domain of information security and privacy. To have performed such an independent audit on FTX would have immediately revealed these misuse of customer funds and other serious problems.

When a third-party attorney auditor [13] generates a standardized opinion letter, it appears much like the standardized opinion letter generated by Certified Public Accountants when they audit the financials of publicly listed companies. It is important that these feedback mechanisms, such as an auditor's report, show the tone-at-the-top and the related attitude about the importance of internal controls, the importance of integrity, and the degree of legal compliance. Whatever that attitude happens to be, that tone-at-the-top will flow down to all employees, out to contractors, consultants, business partners, customers, and others. When Directors & Officers know that their actions are not only visible, but that they will be independently evaluated and reported, ideally on an annual basis, they will be considerably more motivated to do a good job in the area in question (in this case information security and privacy). The performance of such an independent audit, of the actions of the Directors & Officers, on an annual basis, thus counteracts, and rebalances, the very powerful influence of the financial incentive systems that have hampered and impeded information security and privacy efforts for decades [14]. The examination of the actions of the Directors & Officers also helps to ensure that good corporate governance systems will be maintained until the time of the next audit (thus overcoming the traditional problem with audits, which is not only that they look at the results only, but that they are in the form of a series of snapshots, and what happened between those snapshots is unknown).

Using Legal Contracts Rather than Courts

Research has revealed that a proactive approach is not only less costly, but provides better protection, than a reactive approach to information security and privacy [15]. Rather than trying to salvage the remnants of an investment in another firm after a debacle (such as at FTX), or perhaps attempting to restore a reputation after a breach was caused by an attacker gaining entry through a third-party business partner (such as at FTX), it is much better to proactively (in advance) determine whether the firm is trustworthy. Then, as is appropriate, the evaluating firm can avoid putting itself in a position where it is vulnerable [16]. The types of independent audits mentioned above can all be proactively incorporated into legal contracts with third parties. Not only can these types of audits be performed before a relationship is established (such as before a multi-mil-

lion-dollar outsourcing deal is inked), but these audits can be performed every year, to make sure that the third-party firm in question continues to have good corporate governance. Just when the civil justice system and the criminal justice system will get around to making things right, if they will get around to making things right, remains a big question. These days, private sector firms need to be a whole lot more proactive, and in many cases, they also need to renegotiate the existing relationships they have with third parties [17]. We cannot any longer go on assuming that all is good at the other firms with which we do business – the FTX, Enron, Madoff, and many other scandals, have all clearly shown that the blind trust approach is ill-advised.

Appropriate Next Steps

The legislative and regulatory process is not just unpredictable in its results, but it is exceedingly time consuming, as well as burdened by a host of gridlocked political issues that do not directly bear upon whether or not a particular third party is in fact trustworthy. Firms that urgently need to upgrade their third-party risk management vetting process should not wait for the government to get its act together. These firms which have a serious question, regarding whether or not they should be trusting a particular third party, should proactively use more sophisticated independent auditing and due diligence risk evaluation approaches to vet the involved third parties. These mores sophisticated approaches are available now, and can be immediately adopted by those organizations which clearly see the risks they face.

Using the Self-Advertised and Claimed Capabilities of third parties in question is these days absolutely not sufficient. In most cases, whenever there is a significant reliance or significant risk, the addition of one or more Apparently Unrelated Third-Party Recommendations will not be enough either. What is needed is a combination of several Independent Third-Party Audits, indicating for example that a SOC2 report was issued, and/or that the Directors & Officers have met all their legally dictated duties as currently defined by laws and regulations. For still more assurance and trustworthiness, investigating firms can move up to a Sponsored Independent Third-Party Audit, where they pay the bills, and where they supervise the selection of the independent auditor. The degree of the risk associated with the evaluating firm's relationship, with the third-party firm in question, will dictate which type of vetting is now required. Given the tens of billions of dollars lost in the FTX collapse, this latter type of due diligence would absolutely have been warranted for a significant number of firms [18]. And if the firm in question refuses to reveal the details of their internal operations [19], that is itself a red flag, because they may very well have something significant to hide.

About the Author

Charles Cresson Wood, Esq., JD, MBA, MSE, CISSP, CISM, CISA, CGEIT, CIPP/US, is a compliance-related attorney and management consultant specializing information security and privacy. He is best known for his book entitled "Information Security Policies Made Easy," which has been used by 70% of the Fortune 500 companies. His latest book is entitled "Corporate Directors' & Officers' Legal Duties for Information Security and Privacy: A Turn-Key Compliance Audit Process." He can be reached via his web site www.dutiesaudit.com.

References

1. One such unfortunate business partner of FTX is BlockFi, which has gone bankrupt due to its close dealings with FTX. BlockFi only learned about the dire situation at FTX via Twitter, much like the rest of the world. If close business partners are put in such awkward positions because they don't know about the state of corporate governance at associated firms, then major customers, insurance companies, and other connected entities cannot be much better informed. This article discusses how to spot these problems in advance, before bankruptcy, a major breach, or other highly damaging events take place. This article discusses how greater transparency about what is happening behind the scenes at other firms can be achieved.
2. See "Guides Concerning the Use of Endorsements and Testimonials in Advertising," Federal Trade Commission, 16 CFR Part 255 (2009).
3. See for example the $1.26 million settlement with the SEC involving Kim Kardashian, where she endorsed EMAX tokens, a crypto asset offered by EtherumMax. Kardashian failed to disclose to her social media followers the fact that she was paid for the endorsement. See "SEC Charges Kim Kardashian for Unlawfully Touting Crypto Security," SEC, October 3, 2022.
4. See "What are you doing to prevent cyberattacks? SOC2 and SOC for Cybersecurity: How they're different and how they can help," AICPA (2018).
5. It is critical that these third-party firm audits be verifiable, that is to say that they can be confirmed by parties independent of the firm in question. For example, the same result will be achieved when the work is replicated by another auditor.
6. See "Payment Card Industry – Data Security Standard," v.4.0, May 2022.
7. See "Health Information Trust Alliance (HITRUST) Common Security Framework," v.9.6.0 (2022).
8. See "ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems - requirements," ISO/IEC JTC 1/SC 27 (2022).
9. There are ways to achieve this measurement of the tone-at-the-top, and the corporate culture, that will help to assure that the current level of security and privacy is maintained. For example, see Charles Cresson Wood, Corporate Directors' & Officers' Legal Duties for Information Security and Privacy: A Turn-Key Compliance Audit Process, InfoSecurity Infrastructure, Inc. (2020).
10. See the anti-fraud provisions of the Exchange Act of 1933, which prohibit any person from making a false or misleading

statement, or from omitting a material fact in connection with the purchase, sale, or reports about a security.

11. See 18 U.S.C. § 1001, involving knowingly or willfully making false or misleading statements, or concealing information. Individuals convicted under this provision include Martha Steward, Bernard Madoff, and Jeffrey Skilling (Enron).
12. If this level of Independent Third-Party Audit is not added, then the prevailing incentive system emphasis on financial performance will overwhelm the existing decision-making systems, and information security and privacy will continue to be inadequately funded. For discussion of this point, see Charles Cresson Wood, "Solving the Information Security & Privacy Crisis by Expanding the Scope of Top Management Personal Liability," Journal of Legislation, vol. 43, issue 1 (December 2016).
13. I call this process a Duties Audit™, but it basically involves first identifying all the legal requirements to which the Directors & Officers at a particular firm are obliged to conform, then finding evidence to substantiate that they have in fact conformed to those duties. The opinion letter uses a standardized language, and indicates whether all material duties have been met, or whether they have not been met, or whether it was impossible to perform such an evaluation (for example because the auditee firm's management withheld essential information). The topics covered include matters like "disclosure controls," which determine which inside information is released to the public, and who must approve such a release. These are governance and management processes that are often left out of the technical and operational audits related to information security and privacy. The Duties Audit process is the same for all auditee firms, but the actual legal obligations to which the Directors & Officers must comply at a specific firm will vary from firm to firm. The baseline against which the audit is performed, the minimum required by law, is something that firms should be monitoring and adhering to anyway, so the performance of such an audit should not meet with serious objection in the course of negotiations with third parties. Such a Duties Audit can be performed annually as a condition of renewing a contract, not just at the initial time that a decision to proceed to establish a relationship is made.
14. An in-depth discussion of the conflicts between incentive systems is provided in "Solving the Information Security & Privacy Crisis by Expanding the Scope of Top Management Personal Liability," by Charles Cresson Wood, appearing in the Journal of Legislation, December 2016.
15. Juhee Kwon and M. Eric Johnson, "Proactive versus reactive security investments in the healthcare sector," MIS Quarterly, Vol. 38, Issue 2, June 2014, at 451–72. This same conclusion, that proactive efforts should dominate, rather than allowing reactive efforts to continue to dominate, was reached by the Air Force Research Laboratory, in Rome, New York. See their report, which reflects the results of a multi-industry analysis, entitled "Economic Analysis of Cyber Security," July 2006, AFRL-IF-RS-TR-2006-227, for further details.
16. The results of these independent audits can be kept confidential, perhaps used by a firm to improve its governance and management systems, until such a point in time when it can be demonstrably shown to be in full compliance in all material respects. These results can also be shared with selected business partners, such as insurance companies providing D&O liability insurance and cyber-risks insurance. Of course, the greatest value is created when they are made public, just as the opinion letter from a CPA regarding a public company's financials is made public. It is then that consumers and business partners can gain greater trust in the firm that has been audited. Trust is a very big and generally underappreciated issue these days. For example, according to the 2022 Consumer Intelligence Series Survey by PWC, 71% of consumers would be unlikely to buy from a particular business if it lost their trust.
17. The Payment Card Industry – Data Security Standard (PCI-DSS) follows this same approach, using contracts rather than the police, the regulators, and the courts. See www.pcisecuritystandards.org.
18. It is not just investors who have been licking their wounds from the FTX debacle. There are also business partners who have been severely damaged, some bankrupted, as a result of what has happened at FTX. These bankruptcy casualties include BlockFi and DeFi. Other firms that have been hit hard by the debacle include Genesis, Greyscale, Sequoia Capital and Paradigm. See "BlockFi Bankruptcy Is the Latest FTX Casualty," by Q.ai, Forbes Digital Assets, November 28, 2022.
19. When an independent auditor is involved, specific details about business plans, proprietary processes, the actual controls deployed, the ways these controls are implemented, etc., are all withheld from the firm making a decision to trust – only the one-page professional opinion is issued to the firm making a decision to trust. This fact should overcome many objections about disclosure of competitive information, assisting the hackers by revealing details about control implementations, etc.