The Texas Lawbook

Free Speech, Due Process and Trial by Jury

SEC Enforces Identity Theft Red Flags Rule for the First Time: What it Means for Texas Businesses

By Toby M. Galloway & Justin Freeman

The Securities and Exchange Commission recently settled with a dually registered broker-dealer and investment adviser for violating two separate cybersecurity provisions of the federal securities laws: the Safeguards Rule and the Identity Theft Red Flags Rule.

The SEC has on several occasions enforced the Safeguards Rule, which requires certain SEC-regulated entities to safeguard private customer information. But the recent action is the agency's first enforcement of the Identity Theft Red Flags Rule.

This rule requires certain SEC-regulated entities to adopt a written identity theft program that includes policies and procedures designed to identify relevant types of identity theft red flags, detect the occurrence of those red flags, respond appropriately to the detected red flags, and periodically update the identity theft program.

The recent landmark action has very clear application not only to the securities industry but for all businesses, even those not in the financial sector.

Background

Voya Financial Advisors recently settled charges with the SEC for failing to meet the Safeguards Rule and Identity Theft Red Flags Rule due to deficiencies in its cybersecurity governance and response programs. VFA's vulnerabilities were by no means unique to the financial sector, and this order contains valuable lessons for all.

VFA, a dually registered broker-dealer and investment adviser, maintained its customer information – including personally identifiable information of customers – in a centralized web portal accessed by VFA independent contractors, many of whom who could effect securities transactions on behalf of VFA. The contractors used their own systems to access the portal, and the portal was supported by staff from VFA's parent company Voya.
As will be seen, it is vitally important for businesses to have cybersecurity policies and procedures in place as to not only its employees, but also its contractors.

The breach – socially engineered

In April 2016, in a targeted social engineering attack – a common tactic employed when an adversary attempts to circumvent system security by tricking personnel into providing access – an adversary impersonating VFA contractors contacted the portal support staff multiple times to request password resets.

Armed with just a couple of identifying pieces of information about various VFA contractors, the adversary was able to convince support staff to hand over the keys: resetting passwords and providing accompanying usernames. Using this access, the adversary gained access to approximately 5,600 customer PII records and moved laterally to Voya.com, where the adversary setup new accounts which gave it access to even more sensitive data.

The outcome – $1 million fine and compliance

The settled enforcement action included a $1 million fine, enhanced reporting obligations and

a requirement that VFA retain and cooperate with an independent compliance consultant.

Breach breakdown: lessons to learn

Governance is the backbone: Policies and audits are a lifecycle and not a point in time

VFA's cybersecurity policies were last updated in 2009. Cyberthreats evolve daily – even though there are clear trends in attack tactics that can be tracked on an annual basis.

For example 2018's banner compromise tactic, the Business Email Compromise, is noteworthy. As many businesses have recently moved to cloud-based email platforms without implementing two-factor authentication or strong passwords, attackers have found a veritable treasure trove of data allowing them to compromise email accounts and intercept payroll and payment instructions and information. Anything less than an annual review of policies invites extreme scrutiny from plaintiffs and regulators.

VFA performed audits of its systems and those maintained by independent contractors, but failed to integrate its findings into a living governance program. When the audits were performed, not all identified deficiencies were resolved. 30 percent of the systems scanned exhibited critical failures in antivirus or encryption requirements, but according to the order there was no follow up on these deficiencies.

Combined, these findings emphasize that governance must be integrated into an ongoing lifecycle in order to be effective in mitigating cybersecurity risk.

- Tactics are not static. Cybercriminals are sophisticated and have vast financial incentives to find the most cost-effective means of gaining access to private data, and they are highly innovative.
- Businesses must review their security posture regularly to ensure that cybersecurity policies are not only written and adopted, but also operationally implemented. Written policies are effective only if these reviews are acted upon. It is not just a potential waste of limited security resources to fail to follow up – the VFA case demonstrates that it can give rise to more serious liability.

Response is the lynchpin of mitigation

VFA had an opportunity to respond to the April 2016 breach before it even happened. From January through March of 2016, an adversary used the same tactics to attempt to solicit usernames and passwords from support staff. These tactics included using the same phone number, an element that is trivial for an adversary to change. An effective response to those attacks could have mitigated the adversary's effectiveness in the April 2016 breach.

VFA's response appears to have suffered from a failure to "un-trust" and validate all existing network connections as well as tunnel vision.

- From the moment unauthorized access is identified, existing connections should be treated as untrusted until verified. The order finds that VFA failed to terminate existing sessions established with the web portal, and that while VFA surveyed users who recently reset their passwords, VFA did not follow up with users who could not be reached.
- Identifying the window of vulnerability is a critical but complicated requirement of any breach response. The period over which VFA reviewed potentially compromised accounts appeared to be too short, as the adversary continued to impersonate contractors and effectively solicit further password resets.

Risk surface includes all contractors, not just employees

Unique to VFA's position in the financial sector, the SEC's regulatory authority stemmed in part

from its treatment of the independent contractors as "controlled by" VFA and thus associated persons of VFA as a broker-dealer, since the independent contractors were not independently registered broker-dealers. But make no mistake, each and every user, organization and vendor who maintains or has access to a business's sensitive data is *part of its risk surface*.

VFA appears to have had differing control requirements and enforcement between its internal users and the independent contractors. If businesses do not hold all users and vendors to the same security standard, then the business has no security standard. Adversaries will find the weakest link and the easiest route to private data as sure as water flows down a hill.

Social engineering attacks are a priority threat: Use training and controls

Employees are a major element of a business's risk surface *because they already have access to systems*. Every business must understand the value –and limits – of training.

After identifying the risk associated with suspect password reset attempts, the order describes VFA's incident-response team issuing a directive not to reset passwords over the phone. In at least one instance, however, this directive went unheeded.

Training can be effective, but modifying procedures and existing practices in midstream often is not. Training must include policies, procedures and awareness sufficient to empower employees to identify threats and report proactively within their organization.

There is no one-stop solution to the diversity of cybersecurity risks. Controls that limit an employee's ability to perform activities that are outside of established procedures should be operationally imposed, not simply trained on.

Password reset controls are well established – so are the harms of deviating from them

Proper password reset controls might not have stopped the adversary that attacked VFA – an attacker could capitalize on a compromised contractor's email account with the social engineering onslaught, for example. However, the provision of usernames and passwords together created a single and direct vulnerability in VFA's cybersecurity defense posture. Critically, although VFA employed multifactor authentication to further secure user account access, this behavior undermined such additional authentication measures entirely.

Common vulnerabilities

Make no mistake, VFA was the victim of a cybercriminal attack, and no business operating any internet-connected infrastructure is immune to attack. It isn't enough to have a set of written policies and perform audits: They must be incorporated into a living commitment to compliance.

Training, while essential, is insufficient unless it is supplemented by effective operational restrictions. Governance and response must be viewed within the context of ongoing security operations – not isolated activities related to single events. Effective cybersecurity defense requires a cohesive, integrated and ongoing commitment to a unified security posture.

Toby M. Galloway *is co-chair of Winstead's securities litigation and enforcement practice. He is a former chief trial counsel for the SEC's Fort Worth Regional Office.*

Justin Freeman *is of counsel at Winstead. He focuses his practice on cybersecurity and technology transactions. Before entering private practice, he was as the legal director for Rackspace US, Inc.*