REQUEST FOR COMMENT RESPONSE

Required Rulemaking on Personal Financial Data Rights

Docket ID: CFPB-2023-0052 or RIN 3170-AA78

December 29, 2023

I. INTRODUCTION

In response to the Consumer Financial Protection Bureau's ("CFPB") request for comment ("RFC") on its Proposed Rule to implement personal financial data rights under the Consumer Financial Protection Act of 2010 ("CFPA"), CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

CrowdStrike appreciates the CFPB's efforts to issue a final rule that recognizes the importance of personal financial data rights and facilitates consumer access to personal financial data. We welcome the goal to foster a data access framework that is safe, secure, reliable and competitive.

As the RFC notes, third parties' handling of credentials in the financial system can raise significant security, privacy and accuracy risks to financial systems. A cyber incident within a financial system could potentially impact the economy and even national security. CrowdStrike's most recent report on the cyber threat landscape notes that interactive intrusion activity against the financial services industry increased by over

80% over the past year.[1] Furthermore, the report found a 147% increase in access broker advertisements on the dark web[2], a 95% rise in cloud attacks, and a sharp increase in credential theft – making steps to enhance the protection of financial data in the sector timely and appropriate.

While we do not have feedback on every issue that the CFPB seeks comment on, we do want to offer several points that may be of value as the CFPB works towards a final rule.

1. ***Security Program***

The Proposed Rule seeks comment on whether it should address the current arrangements between data providers and third parties regarding the use of data providers' developer interfaces. As a leading cybersecurity provider, it is our view that perhaps the most significant threat to data comes from bad actors operating unlawfully, leading to data breaches, cyberattacks, exploits, ransomware attacks and other exposure of consumer data. Bad actors do not play by the rules, so the CFPB's ruling should have a focus on stopping data exfiltration by such actors. Without the proper protections from bad actors, any new arrangement will be vulnerable to the same risks as the current one.

There are steps that can be taken within the current arrangement that would significantly increase the protections of consumer financial data. These steps are necessary in light of the increased focus of adversaries on the financial sector, coupled with the fact that third-parties house large quantities of sensitive consumer information. We recognize that the CFPB has preliminarily determined that the Gramm-Leach-Bliley Act (GLBA) Safeguards Framework (or the FTC's Safeguards Rule for those data providers that are not GLBA financial institutions) addresses data security risks. However, we suggest the CFPB add the following additional cybersecurity best practices for a more mature security program in light of the ever-evolving cyber threat landscape.

Organizations should leverage several key technologies to defend against bad actors:

[1] 2023 *Threat Hunting Report*, CrowdStrike, https://www.crowdstrike.com/resources/reports/threat-hunting-report/.
[2] "Access Brokers: Who Are the Targets, and What Are They Worth?" CrowdStrike, https://www.crowdstrike.com/blog/access-brokers-targets-and-worth/

- **Cloud Services**. Leveraging cloud systems provides a series of potential security enhancements. Retiring legacy applications and infrastructure reduces attack surface and points of failure. Cloud systems enable comprehensive visibility of workloads. For security technologies specifically, native cloud-based solutions provide robust and scalable protection of distributed environments.

- **Extended Detection & Response (XDR).** Cybersecurity threats are exceptionally broad, and for too long industry players have focused on narrow solutions. No single-purpose network appliance, software agent, or other security tool will address the full scope of the problem. Security teams demand contextual awareness and visibility from across their entire environments, including within cloud and ephemeral environments. The next evolution of the ***Endpoint Detection and Response* (EDR)** concept, XDR, seeks to leverage rich endpoint telemetry and other security-relevant data, wherever it exists within the enterprise. EDR is a natural baseline security capability, but XDR drives more comprehensive cybersecurity outcomes.

- **Machine Learning-Based Prevention**. The core of next-generation cybersecurity solutions is the ability to defeat novel threats based on behavior cues rather than known signatures. Machine learning and artificial intelligence are essential to this end. Leveraging these technologies is essential to meeting constantly-evolving threats from bad actors.

- **Identity Threat Protection**: As organizations embark on a digital transformation to work from anywhere models, Bring-Your-Own-Device policies become commonplace, cloud services multiply, and enterprise boundaries continue to erode. This trend increases the risk of relying upon traditional authentication methods and further weakens obsolescent legacy security technologies. Identity-centric approaches to security use a combination of real-time authentication traffic analysis and machine learning analytics to quickly identify and prevent identity-based attacks.

Additionally, there are multiple security program requirements that bolster organizations' security posture:

- **Speed**. When responding to a security incident or event, every second counts. The more defenders can do to detect adversaries at the outset of an attack, the better the chances of preventing them from achieving their objectives.

Adversaries work rapidly at the outset of breach to move laterally and escalate privileges, seeking to gain access to more systems and data and ensure persistence. This means that organizations should measure and reduce their response time.[3]

- **Threat Hunting**. Whether through supply chain attacks or otherwise, bad actors periodically breach even very-well defended enterprises. However, properly trained and resourced defenders can find them and thwart their goals. Proactive hunting is a leading indicator of the strength of an enterprise cybersecurity program. Central to hunting is properly instrumenting enterprises to support both automated and hypothesis-driven bad actor detection. The better-instrumented the environment, the more chances defenders give themselves to identify malicious activity as an attack progresses through phases. Multiple opportunities for detection increase defenders' chances of success and help avert "silent failures."

- **Zero Trust Architecture.** Due to fundamental problems with today's widely-used authentication architectures, organizations must incorporate new security protections focused on authentication. Zero Trust architecture concepts radically reduce or prevent lateral movement and privilege escalation during a compromise.

- **Logging Practices**. Organizations should collect and retain security-relevant log information to support proactive security measures, threat hunting, and investigative use-cases.

- **Managed Service Providers**. Some entities lack the cybersecurity maturity to run robust security programs internally, or seek to apply internal IT/security resources toward domain-specific challenges. Increasingly, such entities should rely upon managed security service providers to strengthen their security posture.

2. ***Data Protection and Cybersecurity***

[3] Elite organizations seek to identify a breach attempt within one minute, investigate within ten minutes, and isolate or remediate threats within sixty minutes.

To achieve true data protection, both personal and non-personal information are used to identify and stop security attacks[4]. Accordingly, it is important not only to draw this distinction but also to ensure that personal data can be processed for legitimate means. For example, cybersecurity best practices, such as identity protection, endpoint detection and response, log management, and threat hunting as listed above, are dependent upon unique identifiers, which may incidentally be categorized as personal information, to detect and mitigate security risks. This includes identifying which assets are being targeted by an adversary, whether or not a threat actor has moved laterally across a network, and mitigating the impact of breach attempts. In other words, a defender would not know which accounts had been targeted, when privileges were escalated or what data was exfiltrated if the processing of identifiable information were not permitted. We recommend the proposed rule continue to only apply to consumer financial information and follow the lead of other global data protection laws in permitting the processing of personal data for data protection and cybersecurity.

3. *Establishing Standards for Open Banking and Consumers' Data Rights*

The proposed rule discusses the challenges surrounding the industry's efforts to establish standards for open banking, the absence of clarity around the scope of consumers' data rights and the appropriate role of various parties. Generally speaking, Crowdstrike supports industry standards that are open, fair, inclusive, and risk-based.

Experience has shown that well-drafted, technology-neutral Standard Contractual Clauses (SCCs) can be a reliable, easy to use and manageable means to provide legal protections to consumers in today's global economy. Each of the parties in the SCCs – data aggregators, third-parties, and institutions that house financial data such as depository institutions – are contractually bound to those with whom there is privity of contract, and the resulting legal protections create a "Chain of Contractual Accountability."

Moreover, each party must abide by its own industry's legal requirements in a "Chain of Independent Obligations." In other words, consumers' rights remain protected by (i) enforceable contractual obligations between respective parties, and (ii) direct application of any federal laws that pertain to financial consumer data. Where both the Chain of Contractual Accountability and the Chain of Independent Obligations exist, the legal position of the consumer is adequately protected.

---

[4] *Data Protection Day: Harnessing the Power of Big Data Protection*
https://www.crowdstrike.com/blog/data-protection-day-cybersecurity-best-practices/

III. CONCLUSION

The CFPB's proposed rule provides a thoughtful analysis of a complex and constantly evolving policy area. As the proposed rule moves forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend that the strategy focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike®, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.

V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy

Robert Sheldon
Senior Director, Public Policy and Strategy

Email: policy@crowdstrike.com

***