



Office of the Chair

UNITED STATES OF AMERICA  
Federal Trade Commission  
WASHINGTON, D.C. 20580

**Statement of Chair Lina M. Khan  
Regarding the Presentation on Data Security  
At the December 2022 Open Commission Meeting**

**December 14, 2022**

Thank you, Alex, for providing an update on how technologists here at the FTC have been contributing to our enforcement work. It's wonderful to get this perspective.

The Commission's consumer protection statutes were passed in 1938, over 80 years ago. But the digital revolution has caused our threat landscape to evolve constantly. A key challenge is making sure our consumer protection efforts keep up with the pace of technological change.

Our technologists are central to that effort. Their expertise helps us respond to emerging technologies and evolving business practices. I'm grateful that we've been able to increase the number and variety of technologists at the agency, including those with expertise across areas on topics like security and software engineering, data science, and artificial intelligence.

In many ways, the Commission's early work on digital privacy and security was forward-thinking. Under the leadership of Robert Pitofsky, the Commission adapted its old consumer protection statutes to address the new issue of consumer data, and under the leadership of Tim Muris, Commission staff began negotiating settlements that required companies to implement comprehensive security programs.

Over the last year, we have continued to press for improved orders. Three key principles ground these efforts: efficacy, accountability, and administrability.

Efficacy requires that orders address actual problems in a company's practices and calls on them to undertake best practices. Alex's overview of multi-factor authentication, phishing-resistant MFA, and the zero-trust architecture reflects the latest thinking on what truly secure systems should look like. When we require companies to incorporate these features, we also signal best practices to other companies that hold consumer data.

Our orders should not just be a cost of doing business, or a fee to be paid in exchange for harming consumers. That's where accountability comes in. Orders must deliver real accountability by changing business conduct. One way to do that is by holding accountable presiding individuals at companies who commit data security violations. We recently settled a case against the alcohol-delivery app Drizly and its CEO, James Cory Rellas, over the

company's alleged failure to protect consumer data from repeated breaches.<sup>1</sup> In doing so, the FTC reaffirmed that companies are obligated to protect consumer data and that data security must be a priority for any chief executive.

Finally, there is administrability. We've had significant success in enforcement in recent years, but we haven't always made orders easy to administer. To that end, we're thinking about how to craft orders that are easier to litigate if the company violates them. As Alex outlined, requiring companies to publish and abide by data retention schedules can help us know when exactly violations occur and gives us a clear roadmap when we are engaging in order compliance.

We'll continue to look closely at the conduct of companies under order. To do so, we will continue to rely on our talented team of technologists to ensure our remedies match the scope and scale of technological changes. Thank you again to our staff across the agency for their efforts to push this key work forward.

\*\*\*

---

<sup>1</sup> Press Release, Fed. Trade Comm'n, FTC Takes Action Against Drizly and its CEO James Cory Rellas for Security Failures that Exposed Data of 2.5 Million Consumers (Oct. 24, 2022), <https://www.ftc.gov/news-events/news/press-releases/2022/10/ftc-takes-action-against-drizly-its-ceo-james-cory-rellas-security-failures-exposed-data-25-million>.