

## **New Jersey Bill SB 3017, establishing a toll-free telephone number to report fraudulent account actions**

### **VETO REQUEST**

January 7, 2026

### **The Honorable Phil Murphy Governor of New Jersey**

On behalf of NetChoice, a trade association of leading internet businesses committed to promoting free enterprise and free expression online, I respectfully urge you to **veto** Senate Bill 3017.

While NetChoice shares the Legislature's concern about protecting consumers from account fraud, SB 3017's mandate that social media companies provide 24/7 live telephone support creates more problems than it solves. The bill introduces new security vulnerabilities, imposes state-specific operational requirements that fragment consumer protection nationally, and ultimately displaces more effective fraud-prevention tools already in use.

### **The Bill Creates New Privacy and Security Concerns**

Ironically, the bill's central requirement—live phone support for fraud reporting—creates new attack vectors for the very fraud it aims to prevent. Social engineering attacks targeting customer service representatives are among the most successful methods for unauthorized account access. Bad actors impersonate legitimate users and manipulate live representatives into granting access, resetting credentials, or bypassing security protocols. This is not hypothetical; SIM-swapping and impersonation schemes exploiting phone-based support are well-documented.<sup>1</sup>

---

<sup>1</sup> Federal Bureau of Investigation, Internet Crime Complaint Center, *2021 Internet Crime Report*; see also Norton, "What is SIM swapping? SIM swap fraud explained and how to help protect yourself" (June 14, 2023), <https://us.norton.com/blog/mobile/sim-swap-fraud>.

Digital verification systems—multi-factor authentication, security keys, automated identity verification—are specifically designed to resist these attacks. They remove the human vulnerability that phone support necessarily introduces.

The bill also requires platforms to collect additional personal information from users. Phone-based identity verification typically requires linking accounts to phone numbers and potentially collecting voice data or other PII from users who deliberately chose not to provide such information when creating their accounts. This expands the data footprint and increases exposure risk.

### **State-Specific Mandates Create Regulatory Fragmentation**

SB 3017 would make New Jersey one of potentially dozens of states mandating different customer service configurations. This patchwork approach undermines the goal of effective consumer protection.

When each state dictates specific operational requirements, platforms must build state-specific compliance infrastructure rather than investing in security improvements that benefit all users equally. A New Jersey user's account is not inherently more secure because they have access to a phone number unavailable to users in Pennsylvania or New York. Meanwhile, the compliance burden of maintaining fifty different customer service regimes diverts resources from developing better fraud detection, improved security tools, and more robust account recovery systems.

Effective online security requires consistent, scalable approaches—not a map of different state-mandated contact methods.

### **The Bill Displaces More Effective Existing Tools**

Platforms already provide multiple channels for reporting fraudulent activity: in-app reporting mechanisms, dedicated security and help centers, and support systems that create documented records for specialized security teams to investigate. These approaches enable immediate account lockdowns, systematic access log review, and pattern recognition across fraud attempts.

Digital-first fraud reporting is not a cost-cutting measure—it is a security measure. Written records provide documentation. Automated systems can instantly flag and freeze suspicious activity. Security teams can investigate patterns across multiple reports. A phone call provides none of these systematic

protections. The bill assumes that live human contact is inherently superior to digital systems for security purposes, when the opposite is often true.

**For these reasons, NetChoice urges you to veto SB 3017.** The bill's telephone mandate introduces security vulnerabilities, fragments consumer protection through state-specific requirements, and displaces more effective digital security tools. We welcome the opportunity to discuss approaches to account security that actually reduce fraud rather than creating new risks.

Sincerely,

Amy Bos  
Vice President of Government Affairs, NetChoice<sup>2</sup>

*NetChoice is a trade association that works to protect free expression and promote free enterprise online.*

---

<sup>2</sup> The views of NetChoice expressed here do not necessarily represent the views of all NetChoice members.