Browser Privacy Measures

Impact to Fraud Controls

Sam.Jackson@socure.com

An Explosion of Online Fraud

New account openings are exploding - with digital as the channel of choice.

We are seeing fraud at an unprecedented scale. For example, the Secret Service estimates that $100B of covid relief funds were stolen, with California’s unemployment fund seeing $10B of losses on their own. This digital-first fraud is impacting a huge range of institutions, from banking to healthcare to online merchants.

Successful identity verification is often the only thing standing between a fraudster and thousands of dollars of stolen funds. Device and IP signals are essential for establishing trust when assessing an identity.

Fraud detection does not end at verification. Digital risk signals are crucial to a range of other use cases, including:

- Funds transfers and Deposits
- P2P payments
- Account Take-Over
- eCommerce
- Password reset

Browser Signals and Identity Verification

Digital identity signals are of great importance for identity verification.

"Old fashioned" identity attributes like Name, SSN, and DoB - they are readily available on the dark web, can be easily compromised, or are being made irrelevant (e.g. physical address).

Digital identity provides a ground for the evaluation of identity attestations. They are also critical to strategies for risk based authentication.

We are gravely concerned that new browser privacy measures will inadvertently have a large impact on fraud controls, leading to widespread victimization of consumers and (even more) enormous financial losses.

Ambiguity Concerning Emerging Standards

On July 23rd, 2021, Google launched a website which includes timelines for privacy measures related to the deprecation of third party cookies.

It also mentions additional initiatives that lack a clear timeline. They are particularly problematic for fraud prevention. They include:

- Broad, internet-scale IP masking
- User-agent information reduction
- Efforts to defeat device fingerprinting

Key details are still being worked out. Given this uncertainty, we must assume that all of the proposals under discussion will be implemented in some fashion.

Impact to Existing Fraud Controls

We expect that existing fraud solutions will see substantial degradation in performance and precision due to the limited availability of digital signals. Expected impacts include-

- Limited ability to profile and stop fraud rings during organized attacks
- Inability to identify IP concealment schemes, such as TOR, proxy servers, or malicious VPN activity
- Limited ability to identify foreign actors or criminal networks
- Elimination of signals used to identify bots or traffic from hosting facilities
- Reduced capabilities around anomaly detection during verification and authentication
- Limited capabilities around re-identification of customer devices for risk based authentication
- Greatly reduced utility of IP geolocation as a signal in fraud models

Variable Coverage and Fraud Detection

Today’s best fraud controls leverage machine learning for identity verification.

Fraud is particularly challenging from a modeling perspective due to the high imbalance ratio between fraud and non-fraud.

Variables generally must be available in a large portion of the population to meaningfully contribute to a model.

By deprecating APIs, changing the format of key data points, and gating functionality with complicated user preferences, we dramatically reduce the level of intelligence that is serviceable for fraud modeling.

Privacy Budget as a Source of Volatility

Measures such as the Privacy Budget have the potential to introduce non-deterministic behavior concerning device observability. As a result, key variables may be too sparsely populated to be useful, or worse - a source of noise.

We expect that this would have a significant negative impact on model performance.

From the Privacy Budget FAQ:

“What happens if my site goes over budget? Will my API calls be blocked?

The enforcement mechanisms for the privacy budget aren't defined yet. Potential options are to block API calls, to noise or uniformize the output of APIs, or to use another enforcement mechanism.”

Browser Privacy Measures - Broader Context

Many of the proposed privacy measures stem from concerns about abusive or unwanted practices by marketing and advertising firms, as well as fears concerning surveillance.

Today’s fraud controls are a societal good and a necessary part of our global economy. Successful digital transactions are contingent on trusted identities. This is in stark contrast to practices that have been prevalent in the marketing and advertising space.

In some cases, digital profiling is a regulatory requirement [see appendix].

We hope that browsers will adopt standards that balance the need for consent-driven privacy measures against the need for trust in high-risk contexts such as account creation.

The proposals so far have not struck an adequate balance in this regard.

Recommendations

We are in favor of carve-outs or exemptions for companies with an exclusive focus on fraud-detection or account security.

Presumably this would require browsers to maintain safelists for certified parties who meet rigorous ethical standards. Browser and IP data would be visible to these parties, but only in high-risk contexts. Users would then have the ability to add or remove organizations from the safelist.

This approach would enable high-trust interactions while respecting consent and protecting against ubiquitous surveillance mechanisms.

Appendix: Digital Signals and NIST 800.63.3A

Digital signals are effectively mandatory across a variety of government agencies and initiatives.

For example, NIST guidelines for fraud prevention during onboarding (800.63.3A) state:

“The CSP SHOULD obtain additional confidence in identity proofing using fraud mitigation measures (e.g., inspecting geolocation, examining the device characteristics of the applicant, evaluating behavioral characteristics, checking vital statistic repositories such as the Death Master File [DMF], so long as any additional mitigations do not substitute for the mandatory requirements contained herein.”