Primetime Account IQ: Product Brochure

Identify Password Sharing with High Confidence

Video streaming continues to hit new highs in revenue and subscribers, but these aren't the only metrics on the rise. Illicit password sharing remains a growing problem, resulting in lost revenue for MVPDs and programmers, and necessitating an ongoing effort to educate their subscribers on what is permissible sharing.

Primetime Account IQ helps MVPDs and programmers identify account sharing with a high level of confidence, enabling them to deliver better business outcomes while providing improved viewing experiences for subscribers.

The Growing Risk of Password Sharing

According to eMarketer, U.S. video subscription revenues (pay TV and OTT) will grow by 3.6% YoY and reach $119.69 billion by end of 2021[1].

While the future certainly looks bright for online video consumption, an issue constantly plaguing the industry is password sharing by subscribers. A Parks Associates study says this problem costs the industry billions in lost revenue every year[2].

How widespread is password sharing? A LendingTree survey found that nearly 40% of Americans borrow someone else's streaming account[3]. Many subscribers don't even realize that password sharing isn't allowed. According to a CTAM report, only 27% of TVE users say they have a very clear idea of what is and isn't permissible when it comes to TVE password sharing[4].

Challenges to Identifying Password Sharing

For MVPDs and programmers, the big question has become: What is illicit password sharing costing my business? They face three key challenges to answering that question:

No industrywide alignment on password sharing: No uniform definition of it, and no common methodology on how to identify behaviors that constitute unallowed password sharing.

Uncertainty about what actions to take about password sharing: MVPDs and programmers are deeply concerned about wrongly penalizing legitimate users and possibly losing them.

Complexity of understanding user behavior: With millions of devices and locations, differentiating between legitimate activity and illicit password sharing can be challenging — especially in complex instances, such as distinguishing a vacationing subscriber from someone borrowing credentials in another location.

Identifying Password Sharing with High Confidence

What's needed is a solution that can deeply analyze the long, winding trail of data left behind by each subscriber and identify password sharing with a greater degree of certainty. One that can help MVPDs and programmers understand the risks to their revenue and business operations, and determine the most effective actions to take to mitigate the impacts of credential fraud.

Primetime Account IQ helps MVPDs and programmers uncover password sharing with a high level of confidence, enabling them deliver better business outcomes and provide better viewing experiences for subscribers.

Leveraging Real-World TVE Data and Advanced Machine Learning

Adobe Primetime's years of experience in managing TVE authentication, access to an extensive set of subscriber data, and a proprietary machine-learning model combine to provide an unequalled capability to cut through the challenges of accurately identifying illicit password sharing.

Primetime Account IQ pinpoints instances of password sharing by analyzing the wide array of subscriber data available in Adobe Primetime Authentication, which spans more than 600 Adobe-powered TVE apps and nearly 700 MVPDs. Using sophisticated machine-learning capabilities trained with real-world TVE user data, Primetime Account IQ is uniquely positioned to distinguish legitimate subscriber activity from illicit password sharing with high confidence.

To help MVPDs and programmers better understand password sharing within their businesses, Primetime Account IQ determines a **password sharing risk index** that rates every subscriber on their likelihood of sharing account credentials or subscription passwords, from very low to very high.

Primetime Account IQ's machine-learning model applies an innovative method to identify and estimate password sharing. Using a more stringent and conservative approach to interpreting data, the model segments subscribers into categories based on their viewing behaviors, resulting in increased accuracy, fewer false positives, and a higher degree in certainty in uncovering password sharing.

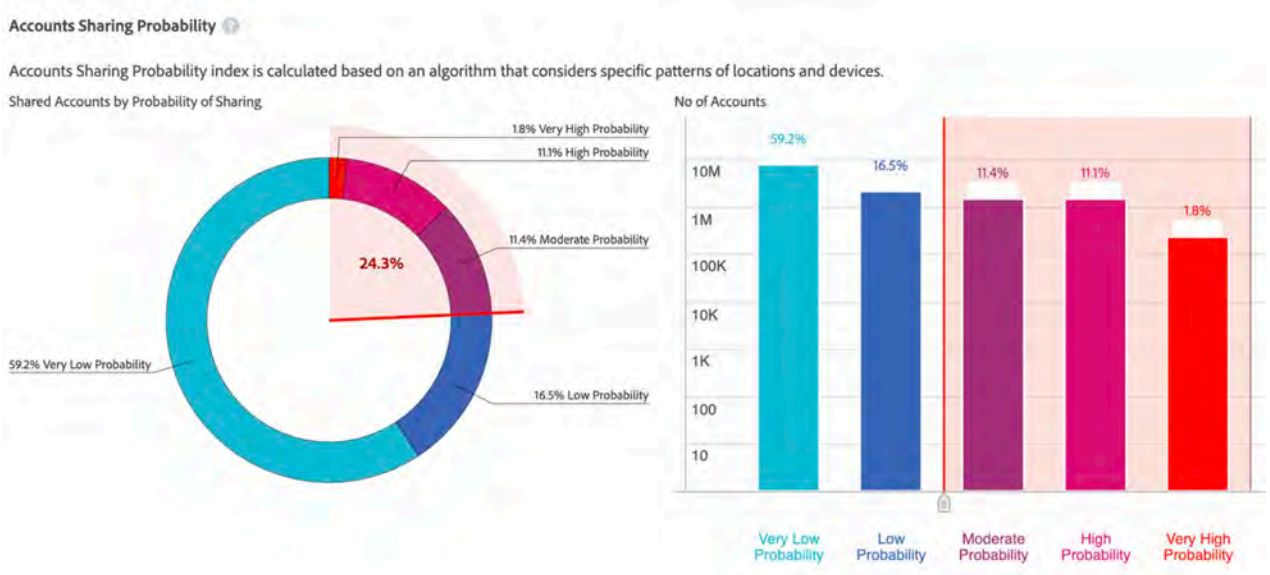

Figure 1: Primetime Account IQ Sharing View

Primetime Account IQ: Key Business Benefits

- **High accuracy in identifying password sharing**: Innovative multi-layer machine-learning approach increases certainty in pinpointing password sharing and reducing false positives.
- **Greater confidence in detecting bad actors**: Accurate analysis of user behavior reduces concerns associated with identifying instances of password sharing.
- **Improved tracking of user devices and locations**: Precise and conservative identification of individual devices increases the accuracy of estimating the number of unique devices used by a single subscriber. Advanced latitude- and longitude-based location tracking combined with accurate device insights help define clusters of legitimate and suspicious user behaviors.
- **Granular analytical tools and reporting**: Deeper reports on user behavior metrics and viewer segmentation provide more detailed insights into patterns of password sharing.
- **Unified and seamless user experience**: A simple and streamlined user interface offers greater synergy with other Adobe Experience Cloud solutions

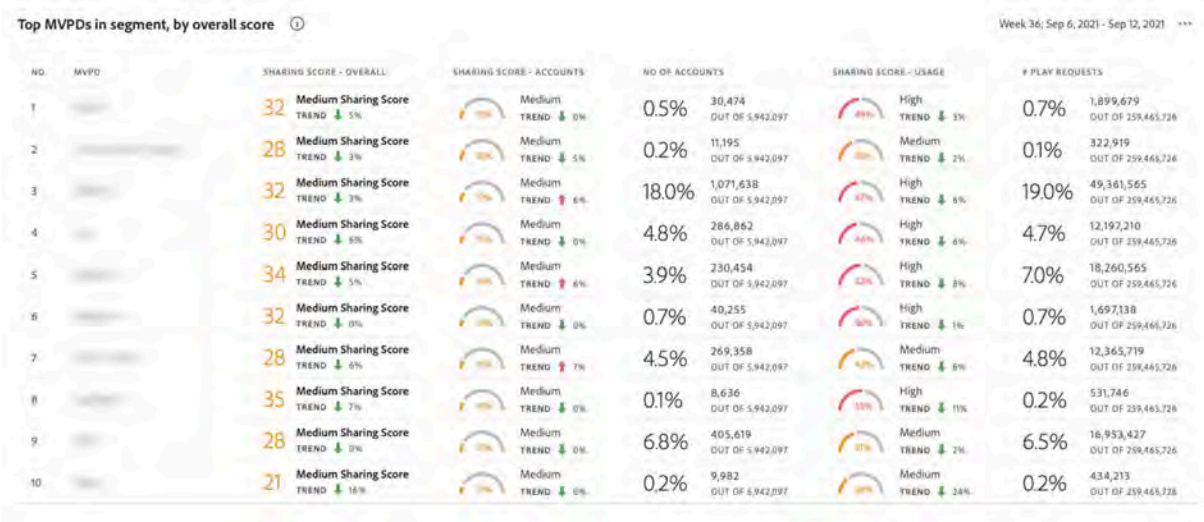

Figure 2: Granular Reporting in Primetime Account IQ

Primetime Account IQ: Key Features

Sharper insights into subscriber behavior

Primetime Account IQ combines an innovative multi-level machine learning approach with more stringent data interpretation to deliver sharper insights into user behavior. The machine learning model is trained using real-world TVE activity and provides greater certainty in accurately identifying password sharing with fewer false positives.

Detailed data segmentation

MVPDs and programmers can segment user data in new ways to help guide their decisions on mitigating password sharing and providing better experiences to legitimate users. For example, programmer and channel-level data segmentation offers detailed insights that enable a wider range of comparisons, such as partner performance and patterns of password sharing, to help uncover issues and take more targeted actions to resolve them.

Detailed data reporting

Primetime Account IQ provides new reports on user data tailored to meet the specific needs of customers. For example, reports that compare user data from MVPDs, programmers, and channels to highlight shared risk, and reports on password-sharing behaviors that can help businesses see the impact of sharing on revenue and user experience.

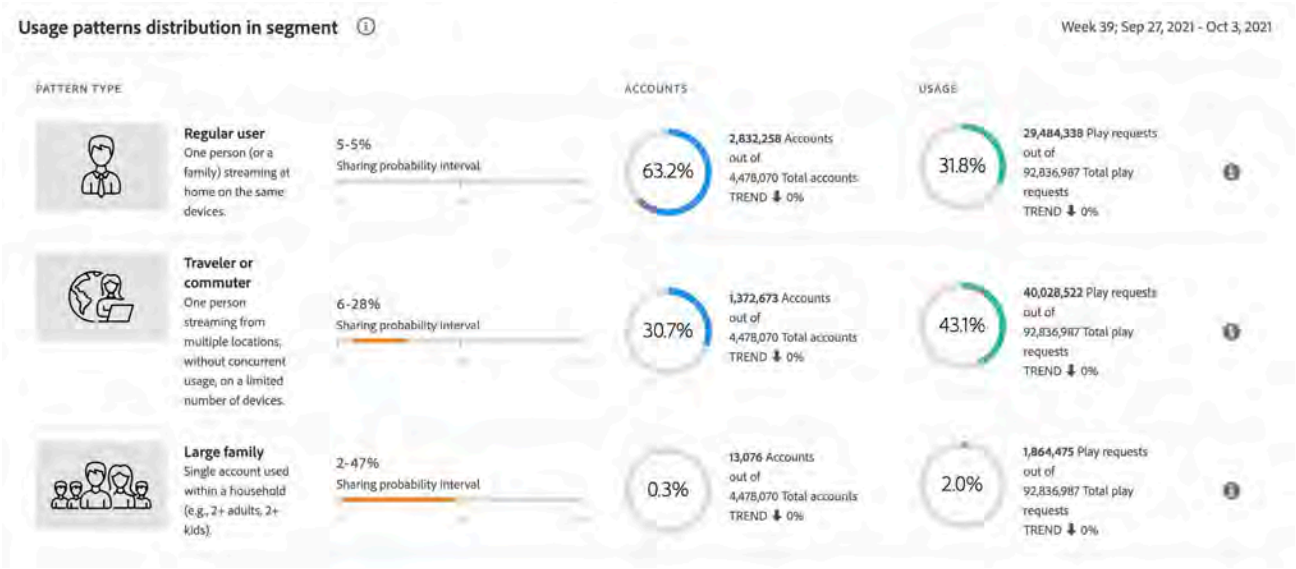

Figure 3: Subscriber Segmentation in Account IQ

Acting Against Password Sharing

The industry is going strong, but the market is also maturing. With growth rates flattening, competition increasing, and production costs skyrocketing, losing revenue to fraudulent password sharing becomes ever more serious. Every player in the TVE industry is somehow impacted by password sharing. Left unchecked, the problem seems sure to keep growing.

What can MVPDs and programmers do about password sharing? The first step is understanding the size of the problem in their subscriber base and how much it's costing their business. The second is to continue identifying and tracking password sharing in the base for deeper knowledge and more accurate identification. The third is to choose actions to mitigate sharing, guided by insights revealed by subscriber data analysis.

Actions could range from delivering onscreen messages to notify sharers of illicit usage to denying them playback.

According to a recent report by Cartesian, 56% of U.S. residents[5] who reported using shared credentials indicated they would be willing to pay for content if their free access no longer worked, so a little education regarding permissible sharing or even stronger actions might prompt them to sign up as new subscribers.

In addition to mitigating password sharing, Primetime Account IQ can help MVPDs and programmers provide better experiences for legitimate customers, such as offering higher concurrent stream limits or longer time to live authentications.

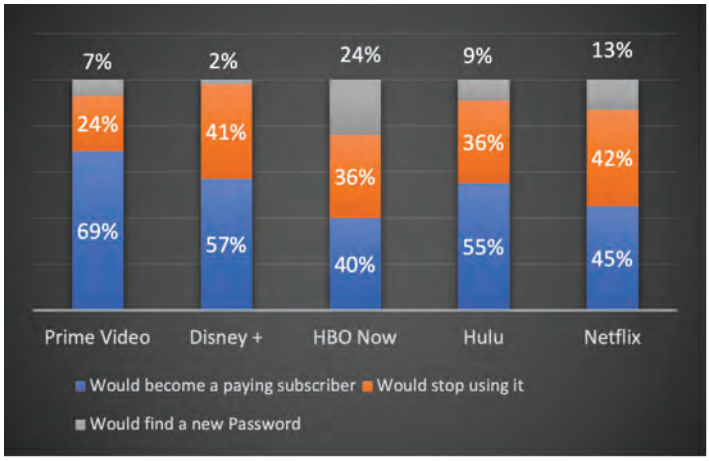

Figure 4: % who would pay if their shared credentials stopped working

By integrating Primetime Account IQ with external systems including Adobe Primetime Authentication and Adobe Concurrency Monitoring, MVPDs and programmers can use its password sharing risk index to interact with both password sharers and legitimate customers to perform the following actions at their end:

	For Programmers	For MVPDs
Adjust time to live for authentication or authorization		●
Send customizable onscreen messages	●	
Export account lists to send email or SMS		●
Change the number concurrent streams allowed	●	●
Change the ad load for an account	●	
Require multifactor authentication		●
Deny authorization and/or logout the user or device	●	●
Deny playback to the viewer	●	●

In all these scenarios, MVPDs and programmers can use Primetime Account IQ to track before-and-after user behaviors to determine if their actions have had the desired effect.

Extending Primetime Account IQ to More Business Cases

Primetime Account IQ's approach to identifying password sharing among massive amounts of complex, changing data can be extended to other subscription-based business models, such as direct-to-consumer streaming (D2C) apps and other emerging distribution channels in the media and entertainment industry.

Another use case is the booming software-as-a-service (SaaS) industry. According to BetterCloud, more than 70% of today's business apps are SaaS-based[6]. Many are sold via subscriptions, opening the door to password sharing. Primetime Account IQ's capabilities in fraud detection and subscriber experience can help manage credential-based fraud management in these industries and more.

To receive a free, customized Account IQ report for your subscriber base providing details on your Risk sharing index and password sharing pattern as well as to learn more about how Account IQ can help your business identify and take action against illicit password sharing, reach out to the Primetime Account IQ team: Sandeep Singh (sasin@adobe.com) or Brian Brinkmann (brianb@adobe.com).

Disclaimer: This marketing collateral contains forward-looking statements, including those related to Adobe's future product plans for Primetime Account IQ, which involve risks and uncertainties that could cause actual results to differ materially. Adobe does not undertake an obligation to update forward-looking statements.

References

1. US Subscription Video Revenues 2021 -- Insider Intelligence Report, eMarketer, March 2021
2. Video Piracy: Ecosystem, Risks, and Impact -- Parks Associates, January 2020
3. Nearly 4 in 10 Americans are Mooching Off Someone Else's Streaming Account -- LendingTree, March 2021
4. CTAM TVE Tracking: 2018 Highlights -- CTAM, March 2018
5. The Threat of Credential Sharing and Theft -- Cartesian, January 2020
6. 2020 State of SaaSOps -- Key Findings, BetterCloud, October 2020