Risk, Rage and Revenue Loss: New Study Offers Key Insights into Consumers' and Small- to Mid-Sized Business Owners' Password-Related Practices and Attitudes

Executive Summary: For years, the industry has been well aware of the limitations of traditional passwords - they are prone to theft and loss, weak and costly, with Gartner estimating that 20-50 percent of all help desk calls are related to password resets. While the industry has been conscious of consumers' growing frustration with passwords, a new survey commissioned by Aware, a leading authentication company, and Pollfish highlights a new level of urgency to replace passwords - underscored by chronically poor password management, heightened consumer grievances and businesses realizing the need for change.

Risk: Despite efforts to educate consumers on proper password hygiene, poor password management practices are a perpetual problem - with more than half of consumers using the same passwords across multiple accounts; staying logged into accounts as a means of avoiding having to re-enter a password; and picking easy to remember passwords or writing them down on paper. This leaves consumers, and the services they use, exposed to considerable risk.

Rage: About half of consumers have experienced 'password rage,' or what happens after someone has too much password stress/password fatigue. Common reactions include yelling at loved ones; taking a nap or binge eating or drinking. Tolerance for password-related obstacles is exceedingly low, with the vast majority of consumers having experienced account lock-out and resulting frustration. Interestingly, the survey revealed some generational differences, including older generations being less comfortable using advanced authentication methods like biometrics than younger generations.

Revenue Loss: Small to mid-sized business (SMB) owners are acutely aware of the damage password friction can inflict on their revenues. Perhaps most telling, 95 percent of SMB owners consider delivering an easy, seamless authentication experience as an important competitive differentiator. This is because more than half of consumers will give up on purchasing a product or using a service because they do not remember a password, and a substantial amount will not sign up for companies, products or services if they are required to even create a new password. Well over half of SMB owners believe that advanced authentication methods like biometrics can deliver the holy grail of a better user experience combined with better data protection; and would consider allowing customers and/or employees to replace passwords with biometrics.

The full survey results can be found below.

Methodology: For the consumer portion of the survey, for a period of several days in late August 2022, Pollfish polled 1,000 consumers from across the United States, representing both males and females (49% and 51% respectively) as well as various age groups including 18-24 (11.8%), 25-34 (17.8%), 35-44 (16.1%), 45-54 (16.1%) and >54 (38.2%). For the SMB owner portion of the survey, for a period of several days in early September 2022, Pollfish polled owners of 420 SMBs (500 or fewer employees) from across the United States that need to authenticate customers, clients and/or employees.

FULL SURVEY RESULTS:

Consumer Questions:

1. I am concerned that my accounts may be accessed by an unauthorized individual (hacked):

- Strongly Agree: 24.2%
- Agree: 36.8%
- Neither Agree or Disagree: 23.8%
- Disagree: 11.3%
- Strongly Disagree: 3.9%

2. My experience with password-related authentication services has been frustrating:

- Strongly Agree: 14.9%
- Agree: 31.0%
- Neither Agree or Disagree: 29.8%
- Disagree: 19.7%
- Strongly Disagree: 4.6%

3. Having to go through a password reset process has negatively impacted my mood/day:

- Strongly Agree: 16.9%
- Agree: 35.3%
- Neither Agree or Disagree: 22.5%
- Disagree: 19.2%
- Strongly Disagree: 6.1%

4. Length and complexity requirements for passwords makes me feel frustrated:

- Strongly Agree: 22.3%
- Agree: 37.6%
- Neither Agree or Disagree: 20.5%
- Disagree: 15.2%
- Strongly Disagree: 4.4%

5. Do you use the same passwords across multiple accounts?

- Yes: 53.6%
- No: 46.4%

6. Do you avoid or dread the password reset process?

- Yes: 66.6%
- No: 34.4%

7. Do you know anyone personally who has been victim to someone hacking one or more of their accounts?

- Yes: 66.9%
- No: 33.1%

8. Have you ever given up on purchasing a product or using a service because you do not remember the password?

- Yes: 52.9%
- No: 47.1%

9. Have you ever been locked out of a service from too many password attempts?

- Yes: 79.2%
- No: 20.8%

10. Have you decided not to sign up for companies, products or services because they require you to create a new password?

- Yes: 44.2%
- No: 55.8%

11. Does signing up for a new service or product with your biometric identity (fingerprint, face, voice, iris) make you more likely to use the service or product versus implementing a password?

- Yes: 49.6%
- No: 50.4%

12. How many passwords do you feel like you have to remember?

- 20 or more: 15.6%
- 15-19: 9.1%
- 10-14: 21.5%
- 5-9: 31.1%
- 1-4: 22.7%

13. How many passwords do you actually remember?

- 20 or more: 6.0%
- 15-19: 4.9%
- 10-14: 12.9%
- 5-9: 31.6%
- 1-4: 44.6%

14. If you have experienced password rage, how have you reacted? (Password rage is what happens after someone has too much password stress/ password fatigue)

- Yell at partner/spouse/roommate/children: 12.4%
- Drink alcohol: 9.6%
- Binge eat: 10.5%
- Take a nap: 18.5%
- Take headache medication: 16.1%
- Other: 12.6%
- I've never experienced password rage: 50.4%

15. If you have been locked out of a service from too many password attempts, how did it make you feel about using the service?

- Extremely frustrated: 26.5%
- Frustrated: 43.7%
- Neutral: 12.2%
- Not frustrated: 4.8%
- I stopped using the service: 1.9%
- I've never been locked out for too many password attempts: 10.9%

16. Do you stay logged into your account(s) as a means of avoiding having to enter your password(s)?

- Yes, on devices that only I use: 57.2%
- Yes, on devices that I use but that are also sometimes used by family and friends: 11.3%
- Yes, on any device: 6.1%
- No: 25.4%

17. How do you remember your passwords?

- I use easy-to-remember passwords: 31.8%
- I write them down on paper (e.g. on sticky notes, in a notebook or planner, etc.): 37.1%
- I use a digital password manager (e.g. a mobile application on your smartphone, tablet, etc.): 21.0%
- I rely on the 'password hint' feature: 6.8%
- I don't seem to remember them: 3.3%

18. Please indicate your willingness to replace passwords with one or more of your biometric traits (face, voice, fingerprint, iris):

- Face: 50.8% yes; 49.2% no
- Voice: 39.6% yes; 60.4% no
- Fingerprint: 71.60% yes; 28.4% no
- Iris: 41.9% yes; 58.1% no

19. **Do you feel comfortable using biometrics for account login/access instead of a password for the following use cases?**

- Consumer-based digital properties (e.g. retail, online banking, social media, etc.): 54.8% of respondents said yes
- Citizen access to government services (e.g. states unemployment, departments of revenue/taxation, etc.): 43.6% of respondents said yes
- I do not feel comfortable using biometrics for account login/access at all: 31.4%

SMB Owner Questions

1. **Do you consider delivering an easy, seamless authentication experience an important competitive differentiator?**

- Yes: 94.4%
- No: 5.6%

2. **Are you getting feedback indicating frustration with your existing password-based authentication process?**

- Yes, from customers: 18.8%
- Yes, from employees: 17.0%
- Yes, from customers and employees: 30.6%
- No: 33.6%

3. **Are there advantages to using biometric authentication? Please select all that apply.**

- Better user experience: 57.4%
- Better data protection: 66.8%
- Peace of mind: 53%
- There are no advantages: 8.0%
- Other:1.0%

4. **Would you consider allowing customers and/or employees to replace their password(s) with an alternative like biometric authentication?**

- Yes, but only customers: 13.6%
- Yes, but only employees: 19.8%
- Yes, both customers AND employees: 57.8%
- No: 8.8%

5. **Why not? Please select all that apply.**

- Extensive development/implementation efforts internally: 13.6%
- Customer privacy concerns: 38.6%
- Data security/storage requirements: 45.5%
- Other: 13.6%

Aware is a leading global provider of software products and solutions for biometric identification and authentication. They are used for variety of applications including financial services, enterprise security, border management, and law enforcement. Aware is a publicly held company (NASDAQ: AWRE) based in Burlington, Massachusetts.