451 Research

S&P Global
Market Intelligence

Enzoic aims to prevent fraud with payment card Bank Identification Number monitoring service

Analysts - Garrett Bekker

Publication date: Thursday, October 26 2023

Introduction

Like them or not, passwords will be with us in some fashion for the foreseeable future — survey data from 451 Research's Voice of the Enterprise service shows that passwords are still the most-used form of authentication, by a wide margin. In our initial report on Enzoic, we highlighted the vendor's ability to scan for and discover weak and compromised passwords across the public internet and dark web. Its goal is to help avoid account takeover and credential-stuffing attacks. The startup has added new services to its portfolio, the most recent being one that uses Enzoic's dark web database for monitoring payment card Bank Identification Numbers (BINs) to help prevent fraud associated with cards that have been exposed in data breaches.

The Take

While many security practitioners are looking forward to the day when passwords are completely obsolete, if the past 20 years are a guide, they will likely stick around longer than most of us would like. To the extent that passwords remain part of most firms' access control infrastructure, Enzoic offers a relatively straightforward approach that can help reduce the risks of using them, while requiring few changes to user workflows or business processes. The addition of BIN monitoring seems like a logical extension that should provide upselling and cross-selling opportunities, as well as an entrance into the financial services sector.

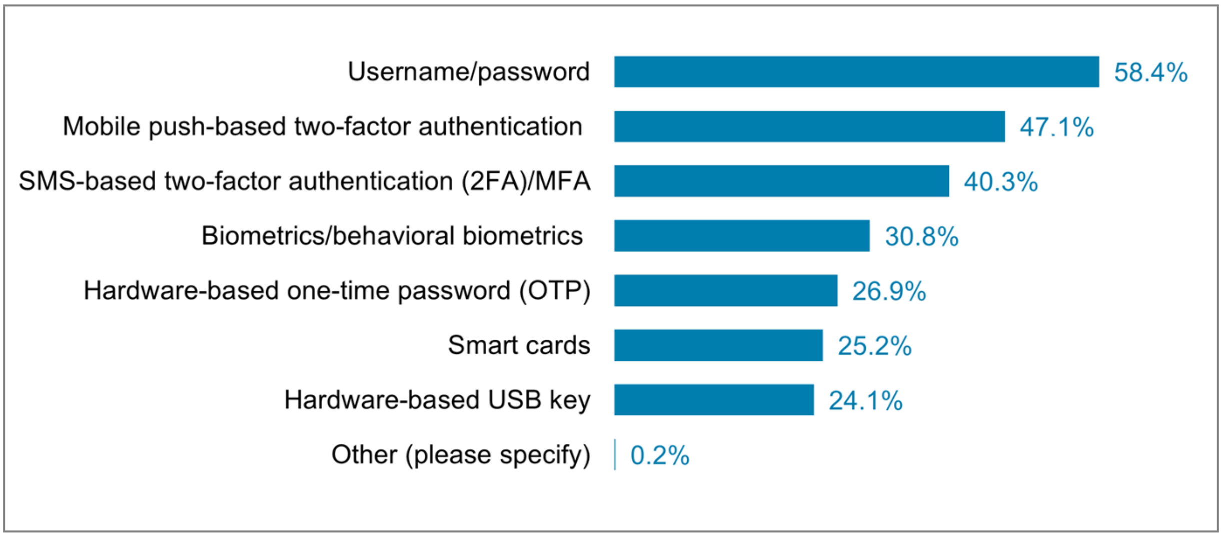
Details

The Bank Identification Number, also referred to as the Issuer Identification Number, comprises the initial four to six digits of a payment card number. These numbers are standardized and designate the issuing bank or credit union, meaning that cards from the same issuer will share the same starting digits. Enzoic's research team gathers data such as compromised credentials and payment card details that have been exposed and subsequently traded on the dark web.

Enzoic's new service will allow organizations to subscribe their institution's BIN to the service and receive alerts when it detects an exposure. Financial institutions can opt to receive alerts in several ways. One method is by email, which will include the full card number and any associated data that was leaked, such as CVV numbers or cardholder name and address, to allow the organization to remediate the exposed card.

Enzoic can also give the financial institution an API key and secret that can be integrated into existing systems, like a customer communications management system that will automatically prompt a mailer or email to users when their card is exposed, or into a card issuing platform to automatically issue a new card, or even into custom software or prop systems that handle their banking. Banks can then disable or remediate exposed cards before they are used for fraud.

Passwords remain the most-used form of authentication



Source: 451 Research's Voice of the Enterprise: Information Security, Identity Management 2022.
Q. Which of the following authentication form factors does your organization currently use? Please select all that apply.
Base: All respondents (n=461).
© 2023 S&P Global.