



# AiteNovarica

FEBRUARY 2023

## RISK INSIGHTS AND ADVISORY FINTECH SPOTLIGHT

Q1 2023

—

TRACE FOOSHEE

This excerpt provided compliments of:



# IMPACT REPORT

# TABLE OF CONTENTS

INTRODUCTION.....2

    METHODOLOGY .....2

ENTERSEKT .....6

CONCLUSION ..... 11

ABOUT AITE-NOVARICA GROUP..... 12

    CONTACT..... 12

    AUTHOR INFORMATION ..... 12

## LIST OF FIGURES

FIGURE 1: RISK INSIGHTS AND ADVISORY FINTECH  
SPOTLIGHT SOLUTION DOMAINS.....3

FIGURE 2: RISK INSIGHTS AND ADVISORY FINTECH  
CATEGORY .....4

## LIST OF TABLES

TABLE A: Q1 2023 PROFILED FINTECH FIRMS.....4

TABLE B: ENTERSEKT SUMMARY.....6

TABLE C: ENTERSEKT PRODUCT ROADMAP .....9

IMPACT REPORT

FEBRUARY 2023

# RISK INSIGHTS AND ADVISORY FINTECH SPOTLIGHT

Q1 2023

—  
TRACE FOOSHEE

## INTRODUCTION

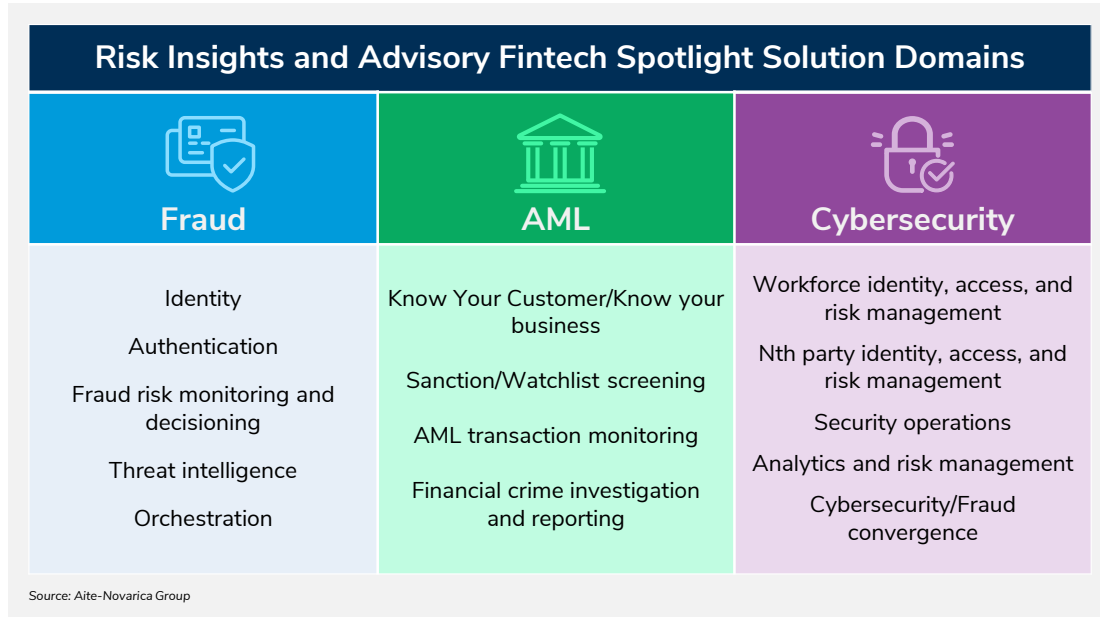
As financial crime soars, emerging technologies gain ground, the regulatory landscape continues to shift, and the fintech sector rapidly expands. Novel products addressing fraud prevention, AML, and cybersecurity are transforming how risk management professionals achieve their objectives. These innovations leverage emerging technologies, data, and techniques to tackle evolving security threats, rising fraud losses, economic uncertainty, the advent of emerging technologies, and intensifying compliance requirements.

Aite-Novarica Group's Fraud & AML and Cybersecurity teams have profiled six vendors in this quarterly edition of the Risk Insights and Advisory Fintech Spotlight report. This report's featured vendors are active across a range of product categories and services aimed at financial institutions (FIs) and other fintech firms, specifically in the fraud, AML, and cybersecurity areas. Major areas of focus include authentication, AML compliance, ransomware protection, fraud detection, and robocall mitigation.

## METHODOLOGY

The Risk Insights and Advisory Fintech Spotlight is a quarterly series of reports that looks at select emerging fintech vendors active in the fraud prevention, AML, and cybersecurity spaces. With the vendor landscape increasingly crowded, and banks and their clients facing a growing array of choices, the Fintech Spotlight series aims to provide insight on interesting vendors that offer a strong unique selling point and an innovative approach as either partners or competitors. The vendors are classified by the nature of their solutions' functionality in fraud prevention, AML, and cybersecurity (Figure 1).

FIGURE 1: RISK INSIGHTS AND ADVISORY FINTECH SPOTLIGHT SOLUTION DOMAINS



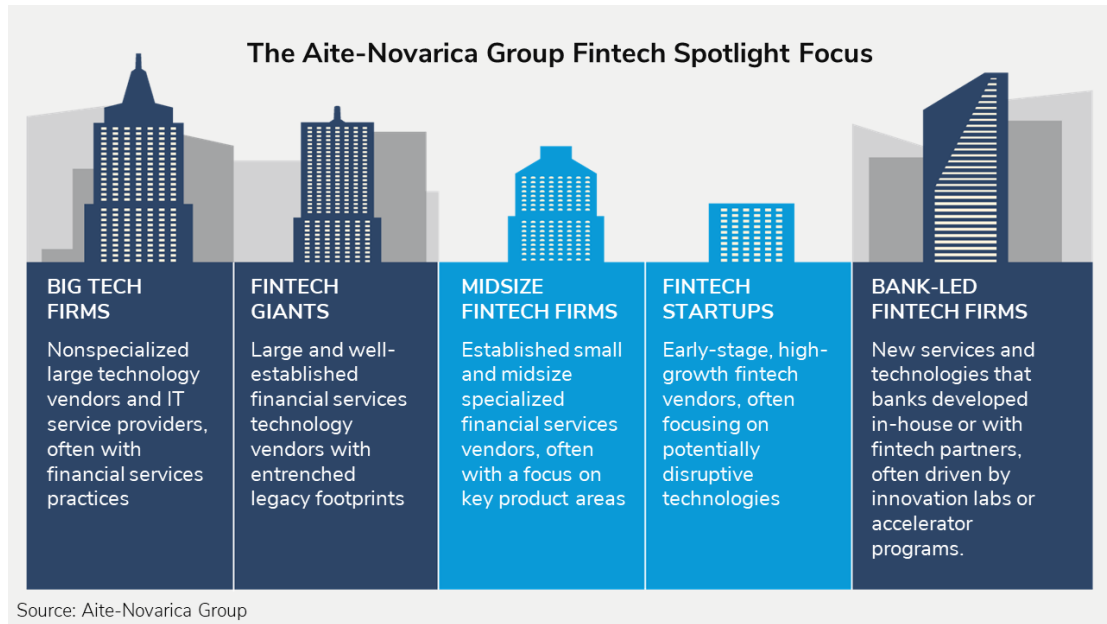
The fintech vendors included must have at least one financial services client with a solution in production and hold annual revenue of less than US\$75 million. Advisors select featured fintech vendors exclusively based on their level of innovation and their interesting approaches to wider business challenges facing the fraud and AML, and cybersecurity markets from both bank and customer perspectives. No featured vendors have paid for their inclusion in this report.

**How Aite-Novarica Group Defines Fintech**

Although popularly used as shorthand to refer to young and disruptive companies in the financial services technology space, “fintech” remains an ill-defined term meaning many things to many people. In an environment in which Tier-1 global banks, multibillion-dollar legacy vendors, and early-stage startups all refer to themselves as fintech firms, terminology remains critical in understanding the market. For purposes of clarity, Aite-Novarica Group defines fintech providers as technology vendors and service providers that aim to improve or automate financial services delivery, potentially disrupting legacy processes and business models in financial services.

While many types of firms can be categorized as fintech firms, the Risk Advisory and Insights Fintech Spotlight is intended to raise awareness of businesses that may have less market visibility than others. As such, Aite-Novarica Group is primarily focused on fintech startups and midsize fintech firms, as outlined in Figure 2.

FIGURE 2: RISK INSIGHTS AND ADVISORY FINTECH CATEGORY



The fintech firms profiled in this quarterly edition are summarized in Table A. Their trend-setting approaches to fraud, AML, and cybersecurity are broadening the tools and intelligence available to the industry.

TABLE A: Q1 2023 PROFILED FINTECH FIRMS

VENDOR	SOLUTION DESCRIPTION	SOLUTION DOMAIN
Entersekt	An authentication orchestration platform that unifies the consumer authentication experience across online, digital, and payment channels	Authentication

VENDOR	SOLUTION DESCRIPTION	SOLUTION DOMAIN
<b>Facctum</b>	A financial crime risk management platform that elevates watchlist management and client and transaction screening	AML
<b>Lucinity</b>	A financial crimes product suite that processes, organizes, and displays compliance data in context, enabling scalable, streamlined, and cost-effective end-to-end AML processes: transaction monitoring, actor intelligence, case manager, and SAR manager	AML
<b>NeuShield</b>	A data protection software that is designed to prevent data destruction and encryption of files resulting from a ransomware attack	Cybersecurity and ransomware protection
<b>Senzing</b>	An entity resolution API that delivers advanced data matching and relationship discovery capabilities without the need for experts in entity resolution	Fraud detection, Know Your Customer (KYC), and AML
<b>YouMail</b>	A suite of SaaS-based solutions that leverages AI, machine learning, and content-based analytics to differentiate legitimate and desired calls from unwanted and illegal robocalls, identify evidence of such threats, and algorithmically score telephone numbers and the service providers enabling those threats	Fraud

Source: Aite-Novarica Group

## ENTERSEKT

Entersekt is an authentication and payment security company. Founded in 2010, its Entersekt Secure Platform (ESP) enables customers to orchestrate consistent and personalized authentication across digital and payment channels. Entersekt enables its customers to expose a variety of active and passive strong authentication options that go beyond traditional SMS OTP methods. When leveraged with Entersekt's modularized 3-D Secure Access Control Server (ACS), customers can extend a robust set of authentication and orchestration capabilities into 3-D Secure (3DS) transactions.

The current relationship between digital channel and payment authentication is fraught with silos and a lack of contextual data flow. Bank customers who are familiar with an authentication journey when accessing their accounts are often faced with a different experience in e-commerce. This disconnectedness leads to frustrating, disjointed user experiences and subsequent cart abandonments when a consumer is attempting to shop online. One way for institutions to get around this is to offer a more integrated and holistic solution for consumers to engage across all of their channels.

Privately held, Entersekt recently partnered with Accel-KKR, a technology-focused private equity firm, to accelerate growth in the global market for authentication and payment security solutions.

Table B provides a high-level summary of Entersekt.

TABLE B: ENTERSEKT SUMMARY

CATEGORY	DESCRIPTION
Founded	2010
Number of employees	Over 200
HQ location	Atlanta and Stellenbosch, South Africa, with offices in London, Utrecht, Munich, Mauritius, and Johannesburg
Geographic coverage	Global

CATEGORY	DESCRIPTION
Key product/service offerings	ESP, customer authentication, 3-D Secure ACS
Ownership and key investors	Privately held; key investors include Accel-KKR, RMI, Nedbank CIB, Endeavor Catalyst, and PAPE Funds
Funding information	Recently partnered with Accel-KKR, a technology-focused private equity firm, to expand market share globally
Customers	Mastercard, Brex, Standard Bank, Capitec Bank, Plus Card, Investec, and First Bank of Colorado
Key partnerships	Mastercard, Onfido, Netcetera, Bonifii, Q2, Finastra, and Temenos
Website	<a href="http://www.entersekt.com">www.entersekt.com</a>

Source: Aite-Novarica Group

### Entersekt Pitch

On the topic of consumer choice, Henry Ford famously said that a customer “can have a car painted any color that he wants, so long as it’s black.” A similar pattern has emerged when it comes to authenticating online, digital, and especially payment transactions. A contemporary Henry Ford might say that consumers today can authenticate any way they like, so long as it’s SMS. This is curious given that in a recent consumer survey, two-thirds of respondents indicated that they want a choice of authentication methods. Getting authentication wrong causes issues beyond consumer frustration. For example, poor payment authentication in e-commerce leads to higher rates of cart abandonment, false positives, and customer churn. It’s no wonder, therefore, that so many firms are seeking to make their authentication journeys more consistent and provide consumers with greater flexibility in terms of being able to choose from a more diverse variety of authentication methods.

As a FIDO Alliance member, Entersekt provides an authentication orchestration platform that includes a fully certified and integrated ACS to unify the consumer authentication experience across online, digital, and payment channels. The company’s ESP

orchestrates customer and payment authentication across several different consumer channels (browser and app, for example) using a diverse ecosystem of signal detection capabilities and authenticators. Entersekt's customers have a variety of ways to customize the authentication experience and tailor the mix and sequence of signals and authenticators and the conditions for triggering and segmenting them.

The benefits of this degree of control over customizing the authentication experience are well understood, but they are hardly unique to Entersekt. What differentiates Entersekt's platform from other authentication hubs is that it has fully integrated its authentication orchestration platform with payments channels, such as its ACS. This is done in such a way that enables Entersekt to not only extend the benefits of its robust ecosystem of orchestrated authentication capabilities to authenticating 3DS transactions, but also to exposing the same range of authentication choices to online and mobile banking users for other use cases, such as login or changing/adding payees, chat banking, and the call center.

Entersekt's ESP is designed as a cloud-based SaaS solution, though larger implementations with more than a million users can be deployed on client-hosted clouds.

### Primary Target Market and Clients

Entersekt started in South Africa and quickly grew market share in Europe before its global expansion was accelerated by the partnership with Accel-KKR, with a strong focus in the U.S. Entersekt primarily targets FIs and fintech firms in all major markets.

### Key Value Proposition and Market Challenges Addressed

Entersekt offers customers four important differentiators as the core of its value proposition:

- A robust, scalable, and flexible authentication orchestration service that works across both digital and payment channel use cases

- The ability of users to leverage Entersekt's ecosystem of signal detection (risk-based authentication for frictionless transactions) and step-up authentication capabilities for both PC/laptop and mobile sessions

- A modularized, stand-alone ACS that can leverage existing vendor capabilities together with all or parts of Entersekt's integrated authentication suite

The ability of users to choose from a variety of strong customer authentication (SCA)-compliant methods, including FIDO (e.g., biometric authentication, hard tokens, soft tokens, and browser ID, which is a browser-based “silent token”), SMS, and in-app push made possible through its software development kit (SDK) for online and mobile platforms.

### Product Roadmap

Entesekt’s strategic product roadmap is defined annually but is refined and executed on a quarterly cadence. Upcoming product releases are anticipated to address the initiatives as listed in Table C.

TABLE C: ENTERSEKT PRODUCT ROADMAP

TIME FRAME	FEATURE/ENHANCEMENT
<p>Near term</p>	<ul style="list-style-type: none"> <li>DAF support (Visa mandate)</li> <li>ID proofing (document and face scan/liveliness, and federated OpenID Connect)</li> <li>Sensitive transaction challenge with liveness</li> <li>SIM info check as a silent risk signal for additional countries, such as the U.S.</li> <li>Single API call for risk-based authentication score and optional challenge</li> <li>Magic links via SMS and email (to facilitate decoupled/delayed authentication)</li> <li>Integrated SDK offering for Q2 customers (browser authentication and white-labeled app already exists)</li> <li>Finastra and Temenos integrations</li> </ul>
<p>Long term</p>	<ul style="list-style-type: none"> <li>Secure payment authentication support for e-commerce transactions</li> <li>Further digital banking platform pre-integrations for turnkey authentication enablement on online and mobile banking</li> <li>Pre-integrations to major U.S. processors for turnkey 3DS enablement</li> </ul>

Source: Aite-Novarica Group

## Aite-Novarica Group's Perspective

Identity authentication has come a long way over the past decade, and innovation in this space has leapt forward particularly aggressively over recent years, as virtually every FI in the market competes to be the easiest FI to do business with. Fraud professionals have had to remake themselves into experts in how to optimize customer journeys in the interest of capturing expansive pools of capital that can be applied to improving the client experience while simultaneously enhancing security. Despite the frenetic pace of innovation in authentication controls, however, solution providers on the supply side of the market and, admittedly, many fraud executives on the demand side, have demonstrated a bias toward a fairly narrow range of options for authentication methods (think passwords and one-time passcodes). In the abstract, this makes a whole lot of sense. These methods are a known quantity, and despite some well-known security flaws, these are what most consumers and security professionals are comfortable with as the status quo. And that counts for a lot given that no one on either the fraud side of the house or on the customer experience side of the house wants to jeopardize security, nor do they want to create a confusing process for customers.

There are two challenges to this, however, that will eventually lead to the kind of disruption that solution providers such as Entersekt are positioned to benefit from:

The first challenge is the collection of security flaws alluded to earlier. To borrow a phrase from the contemporary vernacular, SMS is problematic as a means of authenticating users. As for the password, as one fraud executive said many years ago, "As a security precaution, the password has been dead for over a decade; we just haven't mourned its passing." In summary, these authentication methods are ready to be replaced by more robust methods that are at least as easy to use.

The second challenge is that consumers are very clear that they want more choice in how they authenticate. They prefer that these authentication methods be consistent across channels and use cases. Yes, many of them are exceedingly resistant to change: 'Twas always thus and always thus will be. Despite this, companies still have many appealing reasons to offer a variety of authentication methods for consumers within the constraint that deployment and management is facilitated by a capable and flexible platform.

## CONCLUSION

Fintech firms continue to develop innovative and disruptive approaches to an array of complex and ever-evolving challenges across the financial services industry.

Entersekt's ESP enables customers to orchestrate consistent and personalized authentication across digital and payment channels. This integrated approach to authentication can drive down customers' typically disjointed e-commerce experience, which can often end in frustration and shopping cart abandonment.

## ABOUT AITE-NOVARICA GROUP

Aite-Novarica Group is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

### CONTACT

**Research, consulting, and events:**

[sales@aite-novarica.com](mailto:sales@aite-novarica.com)

**Press inquiries:**

[pr@aite-novarica.com](mailto:pr@aite-novarica.com)

**All other inquiries:**

[info@aite-novarica.com](mailto:info@aite-novarica.com)

**Global headquarters:**

6 Liberty Square #2779

Boston, MA 02109

[www.aite-novarica.com](http://www.aite-novarica.com)

### AUTHOR INFORMATION

Trace Fooshee

[tfooshee@aite-novarica.com](mailto:tfooshee@aite-novarica.com)

**Contributing author:**

Gabrielle Inhofe

[ginhofe@aite-novarica.com](mailto:ginhofe@aite-novarica.com)

© 2023 Aite-Novarica Group. All rights reserved. Reproduction of this report by any means is strictly prohibited. Photocopying or electronic distribution of this document or any of its contents without prior written consent of the publisher violates U.S. copyright law, and is punishable by statutory damages of up to US\$150,000 per infringement, plus attorneys' fees (17 USC 504 et seq.). Without advance permission, illegal copying includes regular photocopying, faxing, excerpting, forwarding electronically, and sharing of online access.