



FINANCIAL
INSTITUTIONS
**REVAMPING
TECHNOLOGIES**
TO FIGHT
FINANCIAL CRIMES

December 2023 Report

PYMNTS
INTELLIGENCE

HAWK

FINANCIAL INSTITUTIONS REVAMPING TECHNOLOGIES TO FIGHT FINANCIAL CRIMES

TABLE OF CONTENTS

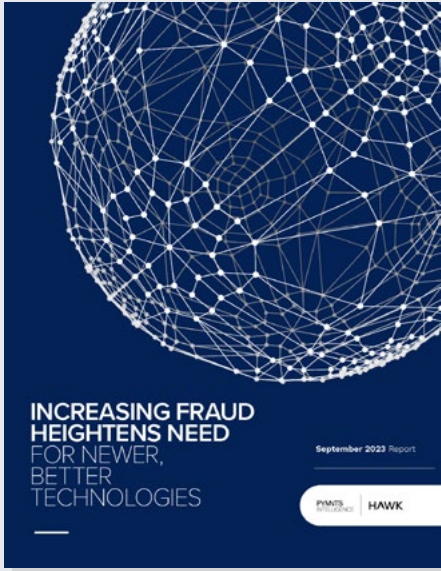
Introduction 04

Key Findings 06

Conclusion 20

Methodology 21

READ MORE _____



September 2023

The State of Fraud and Financial Crime in the U.S. 2023

PYMNTS INTELLIGENCE | HAWK

Financial Institutions Revamping Technologies to Fight Financial Crimes was produced in collaboration with Hawk, and PYMNTS Intelligence is grateful for the company’s support and insight. [PYMNTS Intelligence](#) retains full editorial control over the following findings, methodology and data analysis.

INTRODUCTION

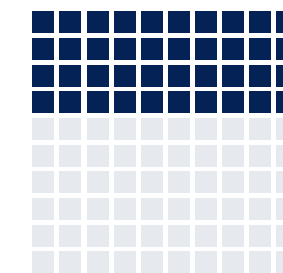
More than 40% of financial institutions (FIs) are seeing increasing volumes of fraud and financial crime, according to a recent PYMNTS Intelligence report, and this advancing wave likely poses a significant threat to the financial services industry.¹ Security is a top concern, particularly for financial services firms, as one of the industry's selling points is the security its firms provide customers on digital platforms. Consumers reported losing approximately \$8.8 billion to fraud in 2022; bank fraud cases grew 25% from 2021 to 2022.^{2,3} In this landscape, FIs need cutting-edge tools to fight the rising tide of fraud and financial crime.

¹ The State of Fraud and Financial Crime in the U.S. 2023. PYMNTS Intelligence. 2023. <https://www.pymnts.com/study/increasing-fraud-heightens-need-for-newer-better-technologies/>. Accessed December 2023.

² Author unknown. New FTC Data Show Consumers Reported Losing Nearly \$8.8 Billion to Scams in 2022. Federal Trade Commission. 2023. <https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022>. Accessed December 2023.

³ Caporal, J. Identity Theft and Credit Card Fraud Statistics for 2023. The Ascent. 2023. <https://www.fool.com/the-ascent/research/identity-theft-credit-card-fraud-statistics/>. Accessed December 2023.

40%



Share of FIs that are seeing **increasing volumes** of fraud and financial crime

Survey data shows that FIs typically use a combination of current technology solutions to address the myriad security issues in the industry. For example, FIs use internal artificial intelligence (AI) and machine learning (ML) and cloud-based, third-party solutions for fraud-fighting, and each approach poses specific challenges for innovation and integration. Third-party providers are an essential piece in the puzzle,

Financial Institutions Revamping Technologies to Fight Financial Crimes, a PYMNTS Intelligence and Hawk collaboration, explores the technological solutions FIs currently use to detect and combat financial crimes, as well as the technology they plan to use in the future. We surveyed 10 FIs in North America between Oct. 10 and Oct. 13 to examine their choices and behavior pertaining to technological solutions to improve their fraud and financial crime prevention operations.

This is what we learned.

While many FIs develop tools to combat fraud in-house, just 14% rely exclusively on in-house AI and ML fraud-fighting tools.

Much of the financial industry still utilizes in-house teams to develop fraud prevention tools, but the next wave of technologies has pushed many to consider external providers. FIs develop 48% of the technologies and 57% of the processes they use to combat fraud in-house, on average. For example, all FI respondents in our survey use customer transaction alerts, but the mix of these tools developed in-house or via a third party varies. While half of the FIs surveyed said they developed 50% or less of this customer transaction alert technology in-house, 30% developed more than 50% in-house and 20% developed these tools solely in-house. This pattern is relatively common across different fraud-fighting technologies, with most being a fairly fluid mix of in-house and third-party development. (Exceptions include call center-based multi-factor authentication, which FIs mostly outsource.)

FIGURE 1:
Fraud-fighting tool development

Share of FIs that use select technologies to detect and address fraud and financial crimes, by who developed the technology

	Use only third-party solutions	Use mostly third-party solutions	Use a roughly equal mix	Use mostly in-house solutions	Use only in-house solutions
• Consumer transaction alerts/SMS alerts	0.0%	40.0%	10.0%	30.0%	20.0%
• Fraud prevention APIs	22.2%	22.2%	22.2%	22.2%	11.1%
• Web-based multi-factor authentication	12.5%	37.5%	0.0%	25.0%	25.0%
• Adaptive authentication	12.5%	25.0%	12.5%	25.0%	25.0%
• AI/ML	28.6%	0.0%	0.0%	57.1%	14.3%
• Biometric authentication	28.6%	14.3%	0.0%	42.9%	14.3%
• Call center-based multi-factor authentication	71.4%	28.6%	0.0%	0.0%	0.0%
• Dynamic passcodes	14.3%	14.3%	14.3%	57.1%	0.0%
• Fraud scores provided by payments processor	33.3%	0.0%	50.0%	16.7%	0.0%
• Real-time data enrichment tools	0.0%	50.0%	0.0%	33.3%	16.7%
• Account takeover tools	20.0%	60.0%	0.0%	20.0%	0.0%
• Geolocation	0.0%	0.0%	50.0%	50.0%	0.0%
• Enhanced knowledge-based authentication	0.0%	33.3%	0.0%	0.0%	66.7%
• Data encryption	50.0%	0.0%	0.0%	50.0%	0.0%
• Address verification service	0.0%	100.0%	0.0%	0.0%	0.0%

FIs have widely adopted some of these tools. Data shows that 71% of FIs use both AI and ML to combat fraud. Another tool FIs commonly rely on to combat fraud is an application programming interface (API). Survey data shows that 90% of FIs use fraud prevention APIs. Adaptive authentication and web-based multi-factor authentication are also fairly ubiquitous, with 80% of FIs having adopted each.

Source: PYMNTS Intelligence

Financial Institutions Revamping Technologies to Fight Financial Crimes, December 2023
N varies by the technology FIs used, fielded Oct. 10, 2023 – Oct. 13, 2023

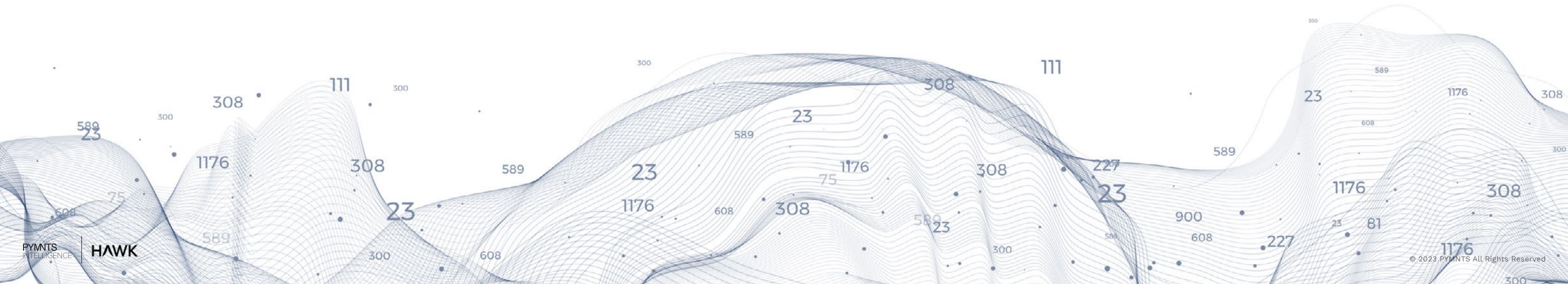
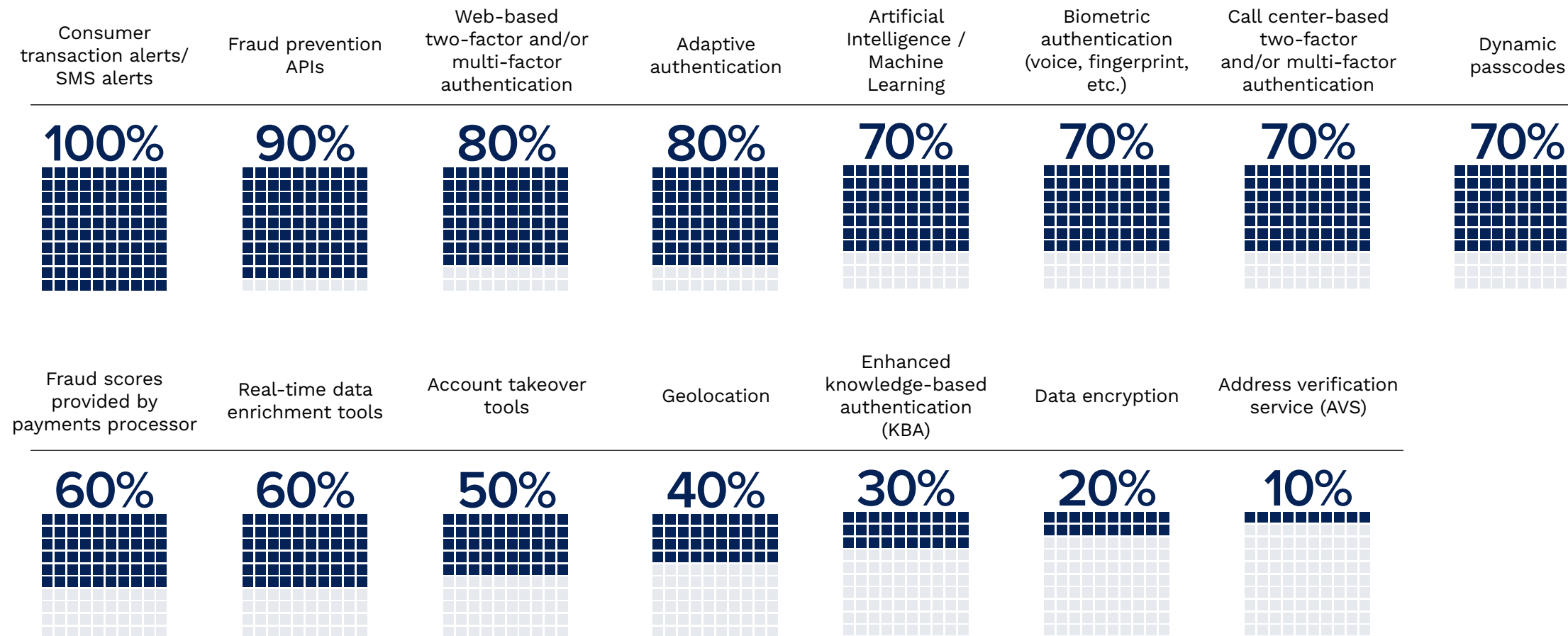
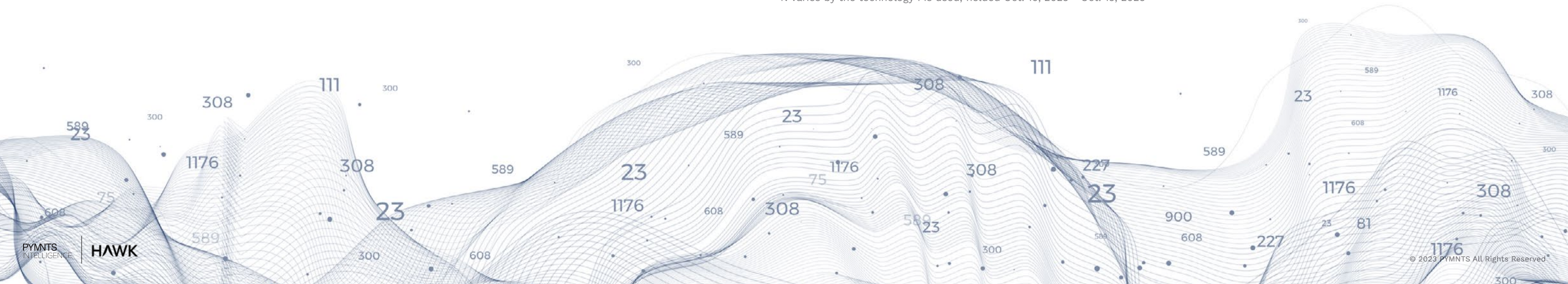


FIGURE 2:
Technologies FIs use to combat financial crimes
 Share of FIs that currently use select technologies to detect and address fraud and financial crimes



Returning to the issue of development, just 14% of FIs developed all fraud-fighting AI and ML technology in-house, and 29% rely entirely on third parties to provide these tools. In-house development of AI and ML tools requires substantial costs, which can help explain why this share is low. Just 11% of FIs use APIs developed entirely in-house, while 22% rely entirely on third-party API solutions. These figures highlight a key aspect of modern-day fraud-fighting for FIs: that third-party technologies are paramount.

Source: PYMNTS Intelligence
 Financial Institutions Revamping Technologies to Fight Financial Crimes, December 2023
 N varies by the technology FIs used, fielded Oct. 10, 2023 - Oct. 13, 2023



FIs seek to leverage third-party providers to revamp their financial crime technology.

Financial crimes' constant evolution forces FIs to revamp their efforts in the next three years. While 80% of FIs will rely on a mix of third-party providers and their own technology, the remaining 20% say that instead of developing their own technologies, they will integrate third-party technologies into their existing systems, which could suggest that costs are driving this decision. Ultimately, 70% of FIs will rely on third-party solutions to use ML, AI and fraud scores provided by payment processors.

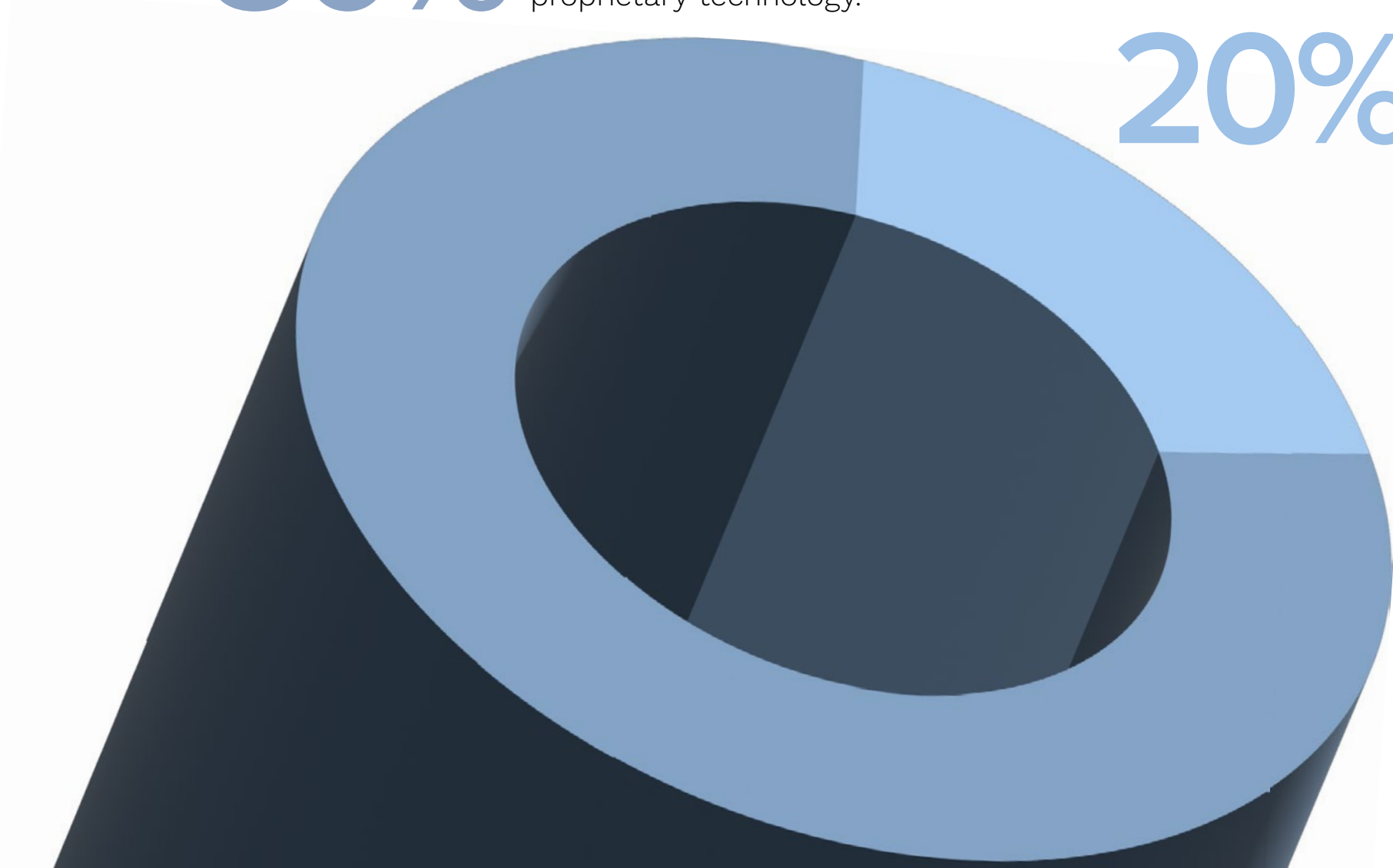
Sixty percent of FIs say they want to rely on third parties to incorporate a cloud-based fraud platform and fraud prevention APIs — cloud-based solutions not only offer the theoretical advantages of distributed computing but also remove the heavy structural and financial burden of developing systems in-house. As for behavioral analysis, 30% of FIs use it to detect fraud — and of these FIs, 66% use procedures developed by third parties.

FIGURE 3:
FIs' fraud-fighting strategies

Share of FIs that use select technologies to detect and address fraud and financial crimes, by who developed the technology

80% We will rely on both third-party technology and our own proprietary technology.

20% We will integrate more third-party technology into our fraud and financial crimes technology stack instead of developing such solutions in-house.



Source: PYMNTS Intelligence
Financial Institutions Revamping Technologies to Fight
Financial Crimes, December 2023
N = 10: Whole sample,
fielded Oct. 10, 2023 - Oct. 13, 2023

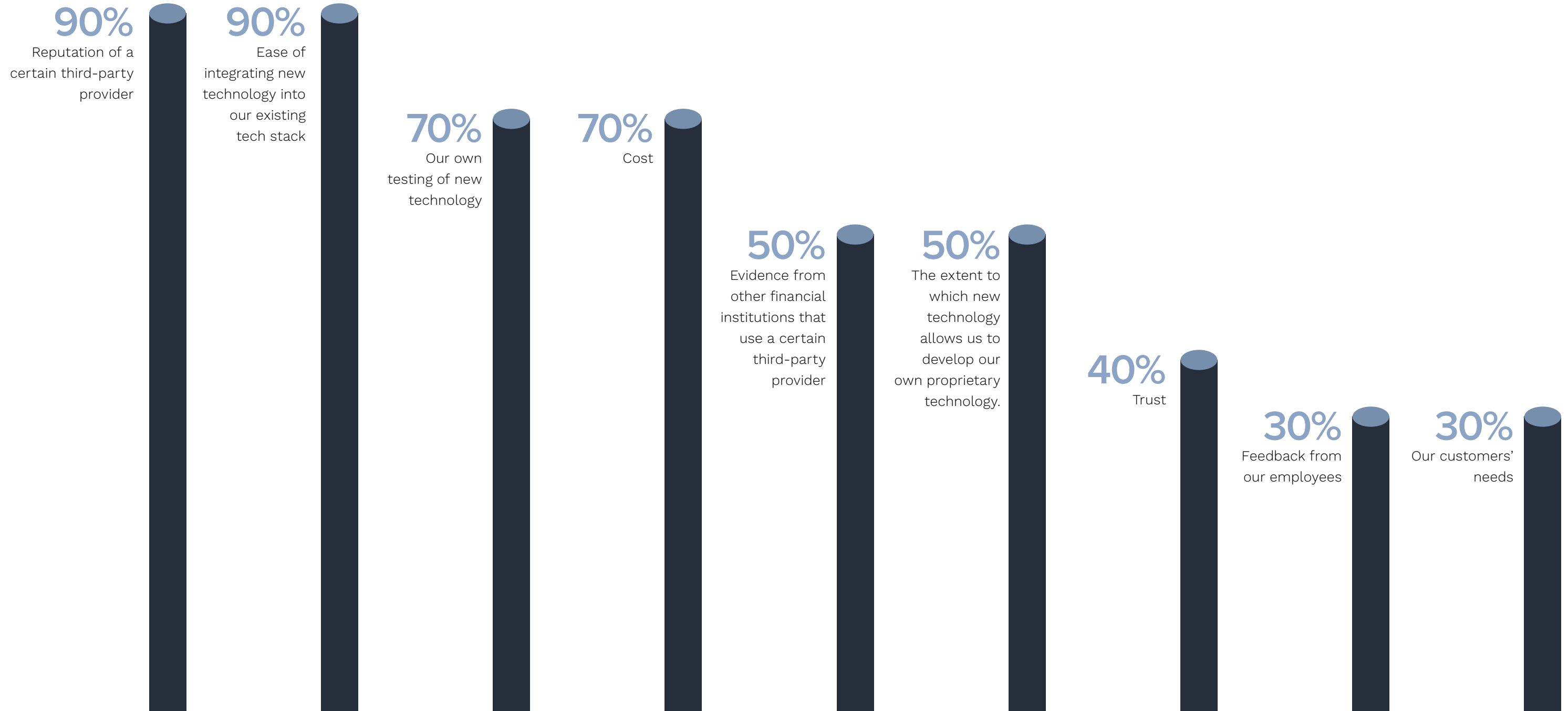
The reputation of a prospective provider and ease of integrating its third-party solution are crucial for FIs' decision-making, with 90% mentioning these as top reasons for choosing a particular third-party provider.

Just as FIs aim to build a reputation to win over prospective account holders, public confidence is key when selecting a provider for this crucial technology. Nearly all FIs say they will choose a third-party provider based on its reputation in developing technologies to combat fraud, even exceeding the 90% of FIs that cited the ease and expertise with which they can integrate new technologies with existing ones as their reason for using a specific third-party provider. Seventy percent of FIs will choose providers based on their own testing of new technologies. Similarly, another 70% point to cost as a deciding factor when considering external providers. One surprising note: FIs seem disinterested in external viewpoints when making these decisions, as the least important factors considered by FIs are customer needs and employee feedback, with just 30% of FIs mentioning each as an influential factor.

FIGURE 4:
Fis' considerations when selecting third-party solutions

Share of Fis citing select factors as influential in their choice of third-party solution providers in the next three years

Source: PYMNTS Intelligence
 Financial Institutions Revamping Technologies to Fight
 Financial Crimes, December 2023
 N = 10: Whole sample, fielded Oct. 10, 2023 - Oct. 13, 2023



CONCLUSION

Fraud fighting in today's economy is a technological arms race, and FIs continue to adopt new technologies such as AI and ML to adapt to the evolving challenges of financial crime. While some FIs use systems and technologies developed in-house, most also leverage third-party solutions. This trend is slated to continue, as all respondents in our sample plan to use third-party technology in the future, with most planning to use outsourced AI and ML technology. Reputation and ease of integration will be critical decision-making criteria for banks as they evaluate third-party technology providers.

METHODOLOGY

Financial Institutions Revamping Technologies to Fight Financial Crimes, a PYMNTS Intelligence and Hawk collaboration, explores the type of technological solution FIs use to detect and combat financial crimes. We surveyed 10 financial institutions in North America between Oct. 10 and Oct. 13 to examine their choices and behavior pertaining to technological solutions they choose to improve their security systems.

THE PYMNTS INTELLIGENCE TEAM THAT PRODUCED THIS REPORT

Scott Murray
SVP and Head of Analytics

Yvonne Markaki, PhD
Senior Analyst

Harold Maldonado
Senior Writer

ABOUT

DISCLAIMER ■

PYMNTS
INTELLIGENCE

PYMNTS Intelligence is a leading global data and analytics platform that uses proprietary data and methods to provide actionable insights on what's now and what's next in payments, commerce and the digital economy. Its team of data scientists include leading economists, econometricians, survey experts, financial analysts and marketing scientists with deep experience in the application of data to the issues that define the future of the digital transformation of the global economy. This multi-lingual team has conducted original data collection and analysis in more than three dozen global markets for some of the world's leading publicly traded and privately held firms.

HAWK

Hawk is the leading provider of AI-supported anti-money laundering and fraud detection technology. Banks and payment providers globally are using Hawk's powerful combination of traditional rules and explainable AI to improve the effectiveness of their AML compliance and fraud prevention by identifying more crime, while maximizing efficiency by reducing false positives. Hawk's modular solution can either enhance or replace rules-based systems with AI-powered transaction monitoring, payment screening, pKYC and fraud prevention in real-time to deliver greater accuracy and reduced noise.

Financial Institutions Revamping Technologies to Fight Financial Crimes may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED "AS IS" AND ON AN "AS AVAILABLE" BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.

Components of the content original to and the compilation produced by PYMNTS is the property of PYMNTS and cannot be reproduced without its prior written permission.

We are interested in your feedback on this report. If you have questions, comments or would like to subscribe, please email us at feedback@pymnts.com.