THE STATE OF FRAUD AND FINANCIAL CRIME IN THE U.S.

SEPTEMBER 2022

PYMNTS

FEATURE SPACE

OUTSMART RISK

THE STATE OF FRAUD AND FINANCIAL CRIME IN THE U.S.

TABLE OF CONTENTS

PYMNTS | FEATURE SPACE

The State Of Fraud And Financial Crime In The U.S. was produced in collaboration with Featurespace, and PYMNTS is grateful for the company's support and insight. PYMNTS retains full editorial control over the following findings, methodology and data analysis.

INTRODUCTION

Fraud attacks on financial institutions (FIs) are commonplace. Their frequency and intensity are on the rise to such an extent that some executives have become hesitant to innovate. The problem is not passivity but rather a pervasive sense of being overwhelmed at the scale of demands and complexity of the challenge.

PYMNTS' research found that 66% of respondents cited complex regulatory requirements as a challenge preventing executives from trying new technical options to protect their organizations. Additionally, 40% of all executives cited concerns over the potential complexity involved in using new technologies, and the same percentage also cited the presumed complexity of integrating new technologies with existing systems as factors inhibiting innovation to combat fraud.

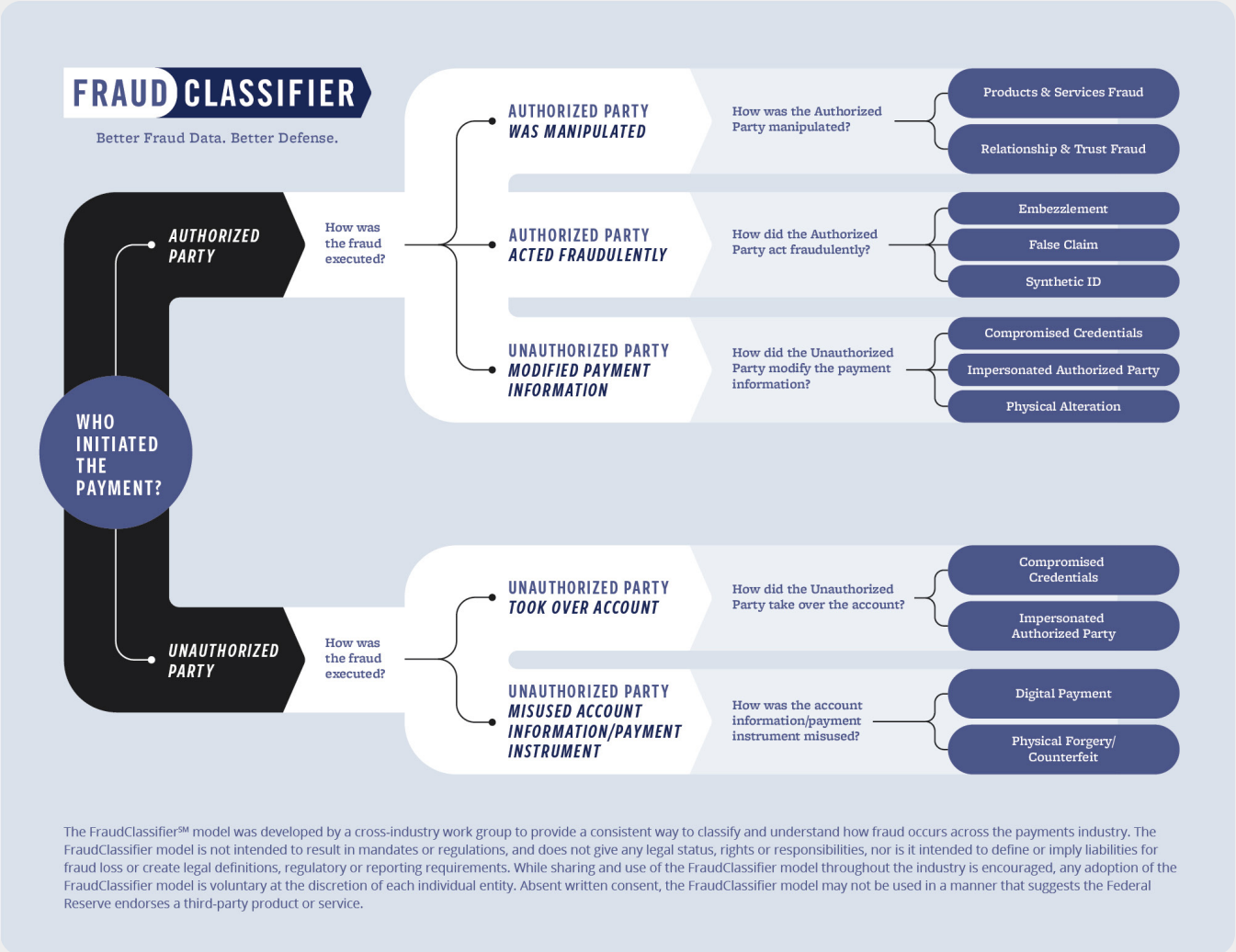
This hesitance to adopt modern tools due to a concern over possible difficulties in making them work leaves many FIs vulnerable at a time when fraud is rampant. Because criminals are ramping up the intensity and scale of their financial attacks — and in some cases targeting consumers directly — many FIs, even those with comprehensive anti-fraud and anti-money laundering strategies, may struggle to avoid pervasive losses without modern technology solutions. Although the most modern forms of financial crime, which include scams presenting as authorized payments or new money-laundering methods, often elude traditional protections, data shows that these strikes can be successfully thwarted with the use of real-time data and analytics powered by machine learning (ML).

A recent survey by PYMNTS finds that FIs using artificial intelligence (AI) and ML report the lowest levels of financial crimes, including fraud. Though the majority of FIs indicated that they wish to invest in new, AI-powered tools to block fraud and identify suspected money laundering, a key problem stands in their way: complexity. In particular, the complexity of implementation — especially regarding regulatory compliance — can impede adoption.

These findings and more suggest that taking a new approach to fighting fraud and financial crime may be wise for FIs seeking to protect both their clients and their ability to scale.

THE FRAUDCLASSIFIER℠ MODEL FROM THE FEDERAL RESERVE

This model offers a standardized reporting format for fraud typologies, and it was used to frame this report and research. See **table 3** on page 23.



The FraudClassifier℠ model was developed by a cross-industry work group to provide a consistent way to classify and understand how fraud occurs across the payments industry. The FraudClassifier model is not intended to result in mandates or regulations, and does not give any legal status, rights or responsibilities, nor is it intended to define or imply liabilities for fraud loss or create legal definitions, regulatory or reporting requirements. While sharing and use of the FraudClassifier model throughout the industry is encouraged, any adoption of the FraudClassifier model is voluntary at the discretion of each individual entity. Absent written consent, the FraudClassifier model may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.

The State Of Fraud And Financial Crime In The U.S., a PYMNTS and Featurespace collaboration, is based on a survey of 200 executives working at FIs with assets of at least $5 billion. The survey was conducted between April 29, 2022, and June 3, 2022. Surveyed executives held leadership responsibilities in fraud and risk operations, money laundering, fraud strategy, fraud analysis, technology and data science; 177 of our respondents held responsibilities in fraud management, 39 had responsibilities in data science and technology and 20 led anti-money laundering (AML) efforts, with some executives responsible for a combination of the above.

This is what we learned.

01 TWO-THIRDS OF FIs HAVE EXPERIENCED AN INCREASE IN THE VOLUME OF FINANCIAL ATTACKS, WITH SMALLER FIs GETTING ATTACKED MOST.

We found that 62% of all FIs experienced an increase in financial crime, and an even greater share of smaller FIs — those with between $5 billion and $25 billion in assets — experienced such an increase. Smaller FIs were also most likely to have faced an increase in the dollar value of fraudulent transactions.

02 FRAUD RATES INCREASED FOR ALMOST ALL PAYMENT METHODS, ESPECIALLY CREDIT CARDS.

Fraudsters especially targeted credit cards: 64% of FIs reported an increase in fraud attacks using them. For comparison, 52% of FIs noticed attacks on debit or prepaid cards increased. In addition, we found that 32% of firms saw an increase in fraud rates related to payments made with Venmo and 51% of firms saw an increase in fraud rates related to payments made with Zelle.

03 CRIMINALS' APPROACHES ARE BECOMING MORE SOPHISTICATED, AND MOST FIs CONSIDER THIS TO BE A PROBLEM.

Our research showed that a majority of FIs saw criminals' increasing use of sophisticated methods to target their organizations and their clients as a significant problem in their efforts to fight financial crime. Approximately one-quarter of the largest FIs by asset size consider this to be the most important challenge they face, leading all others.

04 NEARLY ALL AML EXECUTIVES ARE HIGHLY MOTIVATED TO FIGHT FINANCIAL CRIME AND FIND NEW METHODS TO MAINTAIN AML COMPLIANCE.

Our research reveals that 95% of AML executives consider it a high priority to use innovative solutions to improve fraud detection and AML compliance. That said, 85% of these executives are concerned about the complexity of integrating new technologies to help their organizations fight financial crimes.

05 THE COMPLEXITY OF COMPLIANCE AND THE CHALLENGE OF INTEGRATING NEW SOLUTIONS ARE BARRIERS IMPEDING THE PREVENTION OF FUTURE ATTACKS.

Our research revealed that 52% of FIs that experienced a high rate of relationship scams found the complexity of regulatory compliance a hindrance to adopting new solutions to fight financial crime. In addition, 40% of FIs found new technology integration as a challenge that slowed or halted their efforts to implement innovative solutions to mitigate financial crime risk.

06 AI- AND ML-BASED SOLUTIONS ARE PROVING TO BE EFFECTIVE: FIs DEPLOYING THEM REPORTED THE LOWEST LEVELS OF FRAUD AND FINANCIAL CRIME.

FIs that employ ML-, AI- or cloud-based platforms to mitigate fraud risk had the smallest shares of transactions lead to fraud losses among respondents to our survey. Overcoming implementation challenges can thus make a sizable impact in overall fraud-fighting effectiveness.

FRAUD'S RISING TIDE

Fraud attacks are becoming more commonplace among FIs, and the FIs least capable of absorbing these losses experienced the highest rates of fraud.

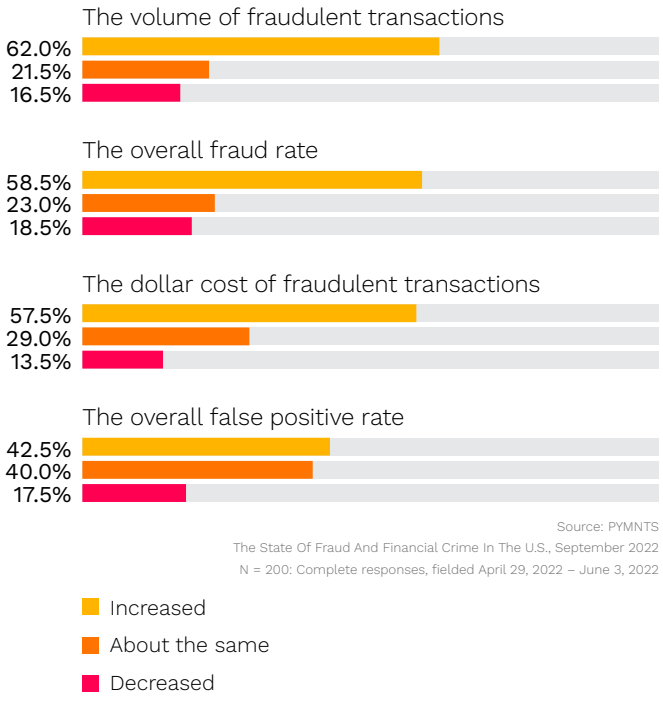
Our research revealed that 59% of FIs experienced an increase in overall fraud rates in the past year, with fraud loss rates averaging 1.29 basis points per transaction. Smaller FIs were hit especially hard, with 71% of these FIs reporting increased fraud rates and an average loss of 1.75 basis points per transaction. In addition, 77% of sampled firms that had fraud losses between $2.5 and $5 million — which we deem to be relatively high — experienced an increase in overall fraud rates.

59%

OF FIs EXPERIENCED AN INCREASE IN **OVERALL FRAUD RATES** IN THE PAST YEAR.

FIGURE 1:

FRAUD AND FINANCIAL CRIME MEASURES
Share of FIs that measured select changes in fraud and financial crime measures year over year

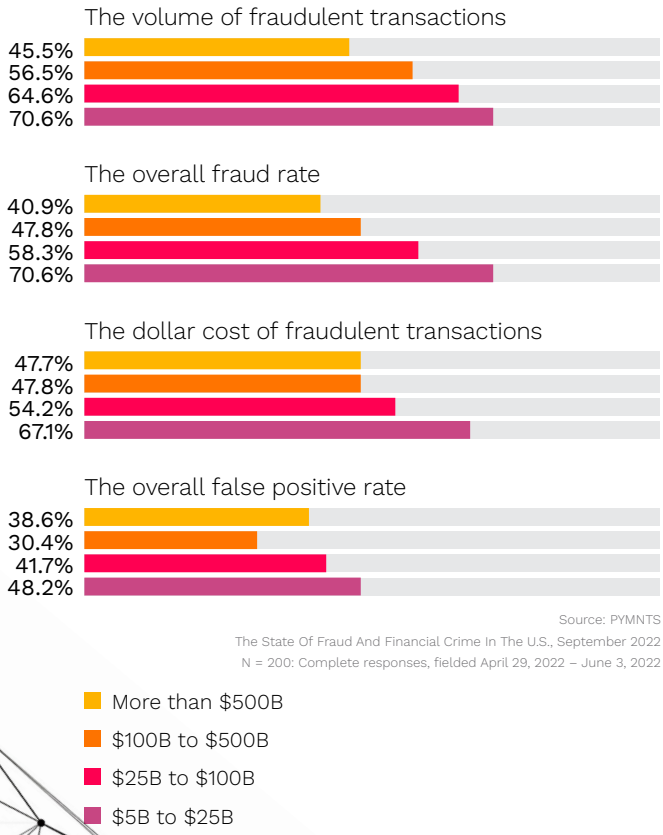


Source: PYMNTS
The State Of Fraud And Financial Crime In The U.S., September 2022
N = 200: Complete responses, fielded April 29, 2022 – June 3, 2022

Our research found that the increase in fraud encompassed most payment methods issued by FIs, although credit cards were especially targeted. Fraud rates related to credit cards increased year over year for 64% of FIs, whereas 51% of FIs reported an increase in fraud related to Zelle and 32% related to Venmo. Nonetheless, our research did not find that Zelle, Venmo or other real-time payments systems posed elevated risk for FIs.

FIGURE 2:

INCREASES IN FRAUD AND FINANCIAL CRIME
Share of FIs that measured increases in fraud and financial crime, by asset size



Source: PYMNTS
The State Of Fraud And Financial Crime In The U.S., September 2022
N = 200: Complete responses, fielded April 29, 2022 – June 3, 2022

There were also differences in the rates of fraud attacks experienced by FIs with various asset classes with respect to specific payment methods. Smaller FIs had the highest rates of increased fraud attacks in credit cards, with 66% reporting increased attacks on that payment method, and prepaid or debit cards, with 61% reporting increases. Smaller FIs also saw the highest rates of increased rates of fraud among peer-to-peer (P2P) and rapid payment methods: 56% reported increased fraud attacks using Venmo in the past year, 51% reported increases using Zelle, 48% saw increases using PayPal and 42% saw more fraud attacks using instant and real-time payment rails. Among the largest FIs, 63% reported increased fraud attacks via wire, 44% cited increases among buy now, pay later (BNPL) options and 38% saw increases in cash-based fraud.

TABLE 1:

INCREASES IN FRAUD RATES IN THE LAST YEAR

Share of executives citing increases in fraud rates across payment methods in the last 12 months compared to the prior 12-month period, by asset size

	ASSET SIZE			
	$5B to $25B	**$25B to $100B**	**$100B to $500B**	**More than $500B**
• Credit card or purchasing card	66.2%	65.9%	**65.2%**	56.8%
• Another digital wallet	55.6%	63.3%	52.6%	58.8%
• Another P2P app	**72.7%**	53.8%	55.6%	52.2%
• Prepaid or debit card	61.0%	46.8%	28.6%	53.7%
• Zelle	51.2%	68.2%	57.1%	33.3%
• Wire	39.7%	33.3%	50.0%	**63.2%**
• Cryptocurrency	60.0%	**75.0%**	50.0%	0.0%
• Bank account transfer	37.8%	31.8%	33.3%	38.2%
• Check	31.0%	50.0%	41.2%	35.3%
• Instant or real-time payments	42.3%	23.1%	44.4%	29.2%
• BNPL	40.0%	25.0%	40.0%	44.4%
• Venmo	55.6%	25.0%	42.9%	17.6%
• Cash	30.0%	32.5%	28.6%	37.9%
• Apple Pay	31.3%	40.6%	44.4%	22.2%
• PayPal	48.3%	24.1%	26.7%	30.6%
• Google Play	23.5%	28.1%	42.9%	16.0%
• Samsung Pay	35.5%	21.2%	20.0%	19.2%
• Regular ACH	27.5%	15.6%	11.1%	21.4%
• Same-day ACH	7.9%	18.5%	25.0%	17.2%

Source: PYMNTS
The State Of Fraud And Financial Crime In The U.S., September 2022
N = 200: Complete responses, fielded April 29, 2022 – June 3, 2022

TABLE 2:

FRAUD RATES ACROSS PAYMENT METHODS

Share of FIs that noticed changes in fraud rates in select payment methods in the last 12 months compared to the prior 12-month period

	CHANGES IN FRAUD RATES		
	Increased	**About the same**	**Decreased**
• Credit card or purchasing card	**63.8%**	26.5%	9.7%
• Another digital wallet	57.7%	31.4%	10.9%
• Another P2P app	57.1%	32.1%	10.7%
• Prepaid or debit card	52.4%	26.2%	21.5%
• Zelle	50.5%	33.9%	15.6%
• Wire	44.8%	36.4%	18.8%
• Cryptocurrency	33.3%	33.3%	33.3%
• Bank account transfer	35.9%	42.5%	21.6%
• Check	37.8%	42.1%	20.1%
• Instant or real-time payments	32.9%	48.2%	18.8%
• BNPL	39.1%	17.4%	**43.5%**
• Venmo	31.7%	41.5%	26.8%
• Cash	32.0%	39.9%	28.1%
• Apple Pay	33.0%	40.0%	27.0%
• PayPal	33.0%	37.6%	29.4%
• Google Play	25.7%	56.2%	18.1%
• Samsung Pay	25.0%	57.0%	18.0%
• Regular ACH	21.7%	59.2%	19.2%
• Same-day ACH	15.1%	**64.2%**	20.8%

Source: PYMNTS
The State Of Fraud And Financial Crime In The U.S., September 2022
N = 200: Complete responses, fielded April 29, 2022 – June 3, 2022

COMPLEXITY IMPACTS FIs' AML EFFORTS

Executives responsible for AML strategy and operations highly value innovation and are proactive in their pursuit of solutions to fight financial crimes. However, despite their interest in new risk-mitigation strategies, most survey respondents showed concern over the complexity of the solutions that they found.

THE WAIT AND SEE PARADOX:

WHY THE PERCEPTION OF COMPLEXITY HINDERS INNOVATION

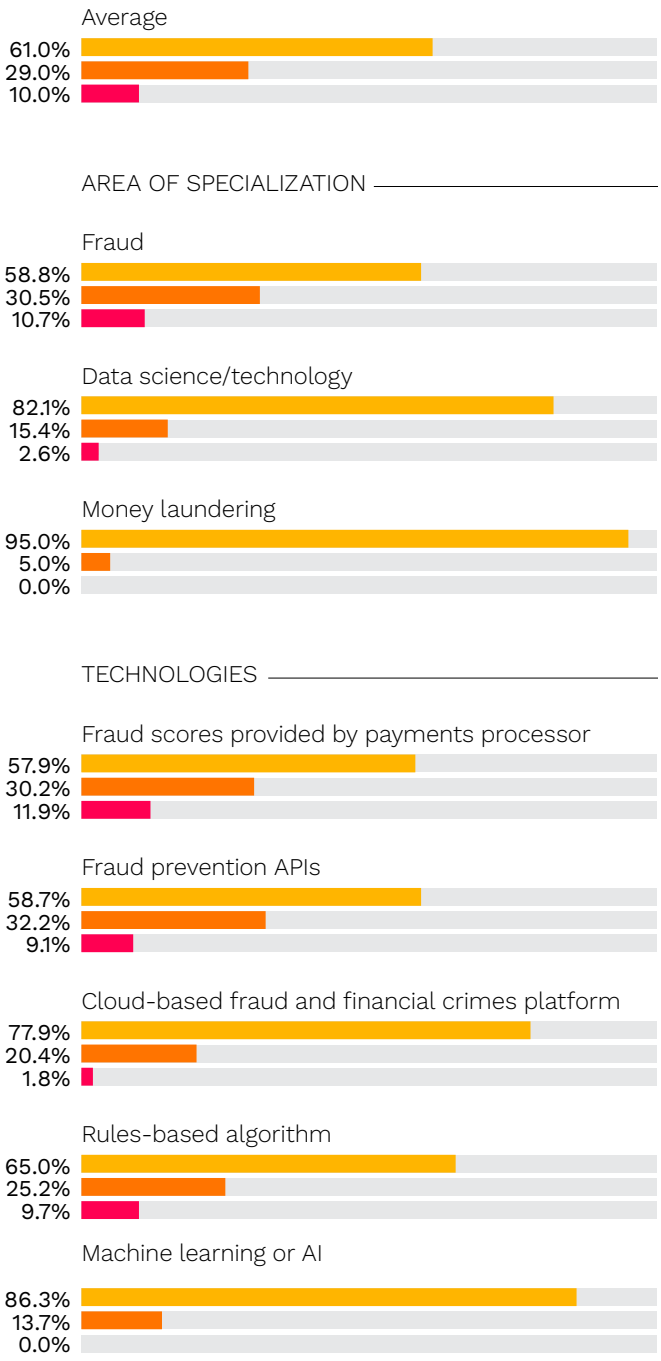
For FIs that have not yet integrated new anti-fraud and AML solutions, the perception of the potential complexity is a significant hindrance to modernization. The executives surveyed who did not adopt modern AML and anti-fraud strategies did so not because there were no available technical solutions that could be integrated with their existing technology stacks or strategies, but because they were convinced that doing so would be too difficult. We found that 66% of executives expressed concern that regulatory standards are too complex and their solution might not manage all of their compliance needs, 58% thought that modern fraud schemes were too sophisticated and no solution could be effective and 49% worried that the increasing rates of fraud would somehow overwhelm any system that they would adopt.

This suggests that executives are simply waiting for the right battle-tested solution, rather than passively standing aside as fraud rates climb. This also falls in line with findings that show that 59% of executives wait until they believe that technical solutions are well developed, widely accepted or both before looking for alternatives to or technical solutions for their existing AML and anti-fraud approaches. However, those who wait at all end up reporting significantly higher fraud losses than those who are brave enough to be first movers.

FIGURE 3:

PERCEIVED IMPORTANCE OF INNOVATION AND IMPROVEMENT

Share of executives who place select levels of priority on innovating new solutions or improving detection and prevention systems to combat fraud and financial crimes, by area of specialization and technologies used to combat fraud and financial crimes



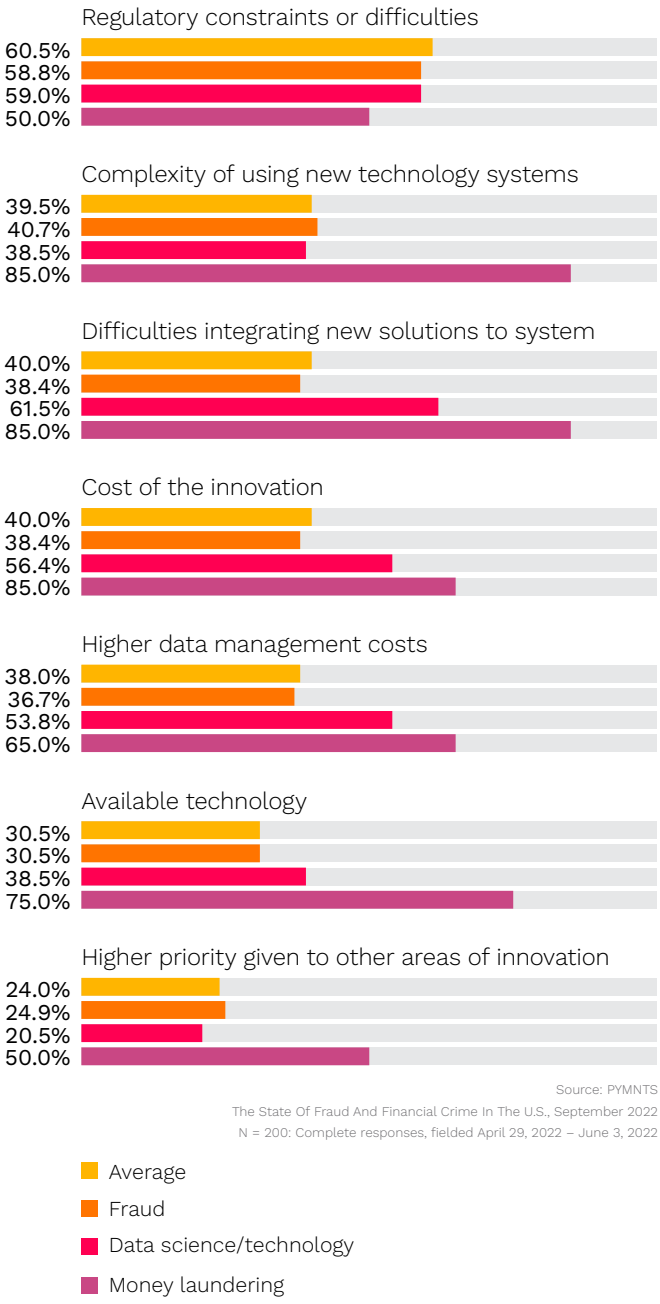
Source: PYMNTS
The State Of Fraud And Financial Crime In The U.S., September 2022
N = 200: Complete responses, fielded April 29, 2022 – June 3, 2022

AML executives are on the front lines of the fight against money launderers, and their day-to-day view of their organizations' risks likely influences their openness to new technical options. PYMNTS' data reveals that 95% of AML executives view the use of innovative solutions to fight money laundering risk and improving fraud detection as high priority, exceeding the 82% of data science executives and 59% of fraud executives that share that view. There were institutional differences as well: FIs already using modern technologies tended to prioritize the integration and use of modern AML and anti-fraud techniques. Our research also found that 86% of institutions that use ML or AI give high priority to innovative AML and anti-fraud solutions and 78% of those that use cloud-based fraud platforms do as well.

FIGURE 4:

KEY INHIBITING FACTORS

Share of executives citing select factors that inhibit innovation or adding new features to existing solutions, by area of specialization

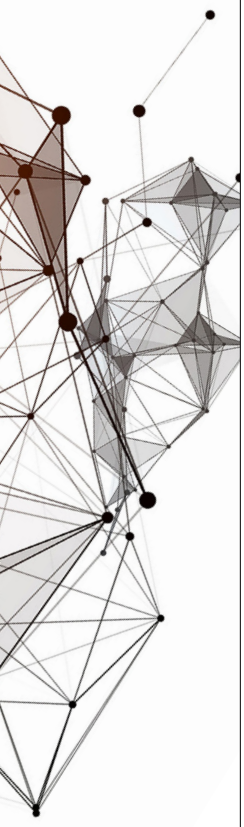


Source: PYMNTS
The State Of Fraud And Financial Crime In The U.S., September 2022
N = 200: Complete responses, fielded April 29, 2022 – June 3, 2022

In addition, our research showed that AML executives are worried about making modern AML and anti-fraud solutions feasible for their organizations. We found that 85% expressed concern over the complexity of new technology systems, the cost of innovations and integrating new solutions with existing systems. Executives in the areas of fraud and data science are far less likely to be concerned, with only 39% of data science executives viewing the complexity of using new systems as inhibiting innovation and 41% of anti-fraud executives sharing this view.

95%

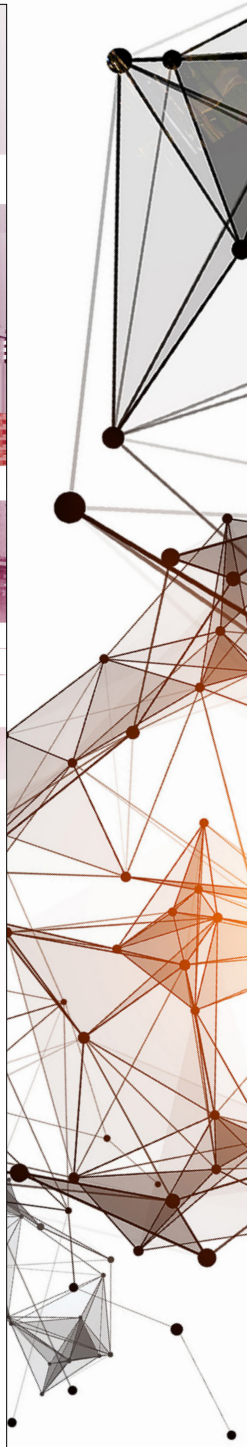
OF AML EXECUTIVES VIEW **IMPROVING FRAUD DETECTION** AND THE USE OF INNOVATIVE SOLUTIONS **TO FIGHT MONEY LAUNDERING** AS HIGH PRIORITY.



FINANCIAL CRIME AND FRAUD:

INCREASINGLY SOPHISTICATED, DIGITAL AND COSTLY

Criminals' use of sophisticated digital methods to commit financial crimes, including fraud, is a key challenge facing FIs, especially those with assets over $500 billion. That sophistication is causing executives concern. Our research revealed that 58% of FIs noticed increasing sophistication in the financial crimes they experienced and saw this change as a challenge to protecting the organization, with 16% identifying it as their biggest challenge. PYMNTS' data finds that 25% of institutions with assets in excess of $500 billion mentioned the increasing sophistication of fraud as the most important challenge, implying that the issue is most pressing for FIs with greater resources.



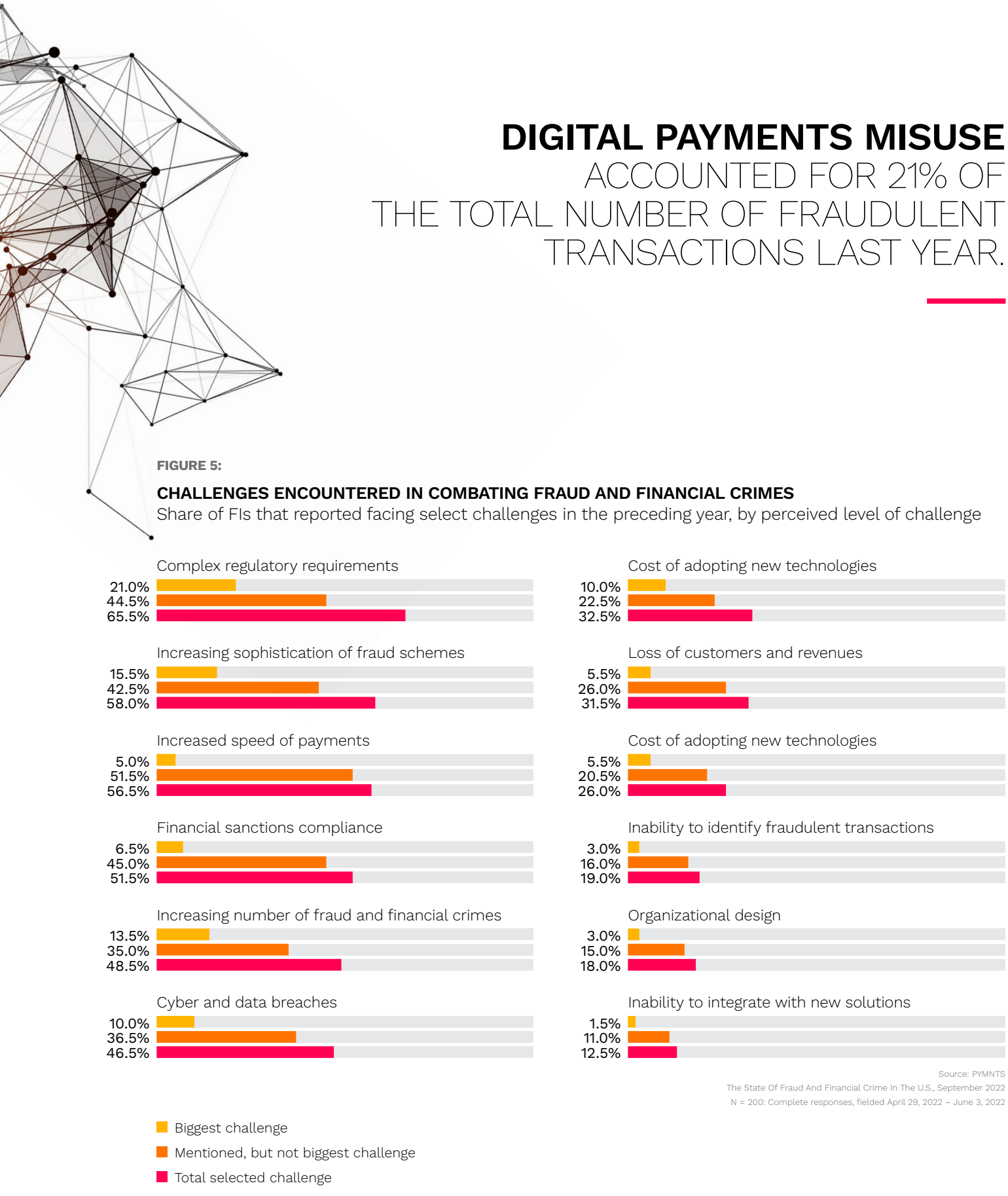
Digital payments are at the heart of FIs' innovation efforts, but such payments also present a challenge to organizations still struggling to find the right risk management solution. Digital payments misuse accounted for 21% of the total number of fraudulent transactions and cost FIs an average total of $120 million last year. Fraud resulting from relationship, product and service scams combined represented 22% of total fraud and cost FIs an average total of $102 million. Misusing digital payment account information is the single leading source of fraud and represents above average transaction values. Regardless of their size, all FIs we surveyed have been targets of these two types of fraud.

DIGITAL PAYMENTS MISUSE ACCOUNTED FOR 21% OF THE TOTAL NUMBER OF FRAUDULENT TRANSACTIONS LAST YEAR.

FIGURE 5:

CHALLENGES ENCOUNTERED IN COMBATING FRAUD AND FINANCIAL CRIMES

Share of FIs that reported facing select challenges in the preceding year, by perceived level of challenge



Source: PYMNTS
The State Of Fraud And Financial Crime In The U.S., September 2022
N = 200: Complete responses, fielded April 29, 2022 – June 3, 2022

TABLE 3:

FRAUDCLASSIFIER℠ MODEL

Share of transactions classified as specific types of fraud under the FraudClassifier℠ Model, as a percentage of total transactions and as a percentage of total dollar value, expressed as total losses in millions

	Total number of transactions	Total dollar value	Total losses
UNAUTHORIZED PARTY			
Misused account information			
• Physical forgery/counterfeit	6.9%	7.6%	41M
• Digital payment	**20.9%**	**22.4%**	**120M**
Account takeover			
• Impersonated authorized party	10.6%	11.5%	62M
• Compromised credentials	9.8%	10.1%	54M
AUTHORIZED PARTY			
Unauthorized party modified payment information			
• Physical alteration	3.4%	3.8%	21M
• Impersonate authorized party	7.3%	7.2%	39M
• Compromised credentials	8.5%	8.4%	45M
Authorized party acted fraudulently			
• Synthetic ID	4.6%	4.6%	25M
• False claim	2.4%	2.1%	11M
• Embezzlement	4.0%	3.3%	18M
Authorized party was manipulated			
• Relationship or trust fraud	**12.7%**	**11.7%**	**63M**
• Products or services fraud	8.9%	7.3%	39M

Source: PYMNTS
The State Of Fraud And Financial Crime In The U.S., September 2022
N = 200: Complete responses, fielded April 29, 2022 – June 3, 2022

A TRIPLE THREAT:

COMPLIANCE COMPLEXITY, FINANCIAL CRIME AND TECHNOLOGY INTEGRATION

Though FIs that have been victims of financial crimes would like to use innovation to combat scams, many cite regulatory requirements and difficulties integrating new solutions as barriers impeding them from doing so.

Our research showed that 52% of FIs that experienced what we consider to be a high rate of relationship scams — impacting between 60% and 100% of their total number of transactions — reported that maintaining compliance with regulations was inhibiting innovation. We found that 41% of FIs that experienced scams involving products or trust impacting between 40% and 60% of the total number of transactions cited difficulties integrating new anti-crime solutions into existing systems.

Although 40% of FIs mentioned technological complexity as an inhibiting factor to innovation, that group is made up mainly of FIs that consider innovation to be a low priority.

TABLE 4:

INNOVATION STRATEGIES' EFFECTIVENESS ON FRAUD RATES

Share of FIs with select strategies when launching innovative solutions and average percentage of transactions in basis points that resulted in fraud losses for FIs that employed select strategies

	Share of FIs with select strategies	Average percentage of transactions
• Launch innovative solutions before others	10.0%	0.45
• Wait for evidence of emerging trends, then act quickly to launch	31.0%	1.20
• Wait until innovative solutions are well-developed, then integrate the most accepted solutions	21.0%	1.26
• No new solutions added until they are widely accepted in the marketplace	**38.0%**	**1.61**

Source: PYMNTS
The State Of Fraud And Financial Crime In The U.S., September 2022
N = 200: Complete responses, fielded April 29, 2022 – June 3, 2022

Overall, our data shows that FIs that place a high priority on innovative solutions are more likely to act quickly to launch new solutions to fight financial crime. Yet organizations that have experienced higher rates of transactions resulting in fraud losses show significant hesitance in trying anti-crime solutions before they have become widely accepted in the marketplace.

AI AND ML FIGHT FRAUD BEST

Financial institutions using AI and ML report lower levels of fraud and financial crime than those not using these solutions, and 71% of large FIs now plan to innovate new solutions or improve detection and prevention systems to better combat fraud and financial crimes.

Our research shows that 71% of FIs plan to improve their use of these solutions within the next six to 12 months. Smaller FIs are the most likely to be adding new technology in the next six months: 43% of these institutions plan to do so. This may reflect the fact that FIs already using ML and AI or cloud-based platforms to combat fraud report the lowest rates of transactions leading to fraud losses. Overall, ML and AI combined with other technologies are the most effective technologies FIs can use to combat fraud.

TABLE 5:

PLANS FOR IMPROVING EXISTING FRAUD- AND FINANCIAL CRIME–FIGHTING SOLUTIONS
Share of FIs that have planned select actions, and share of FIs planning to add new technologies, by asset size

	AVERAGE	ASSET SIZE			
		$5B-$25B	$25B-$100B	$100B-$500B	$500B+
ACTION					
• Improve communication with customers	**64.0%**	**61.2%**	**56.3%**	60.9%	**79.5%**
• Initiate/increase the use of ML/AI models	46.0%	38.8%	27.1%	**65.2%**	70.5%
• Initiate/increase the use of cloud-based platforms	44.0%	35.3%	45.8%	52.2%	54.5%
• Initiate/increase the use of deep learning systems	35.0%	18.8%	41.7%	47.8%	52.3%
• Develop new in-house systems for fraud and financial crimes	20.0%	8.2%	29.2%	30.4%	27.3%
• Outsource detection and prevention to a third party	17.0%	12.9%	16.7%	26.1%	20.5%
• No plan	18.0%	24.7%	20.8%	13.0%	4.5%
TIME PERIOD					
• Next two years	19.9%	31.4%	14.3%	10.0%	15.0%
• Next 12 months	**42.5%**	**52.9%**	34.3%	30.0%	**42.5%**
• Next six months	28.1%	9.8%	**42.9%**	**35.0%**	35.0%
• In the process	9.6%	5.9%	8.6%	25.0%	7.5%

Source: PYMNTS
Fraud And Financial Crimes In North America, September 2022
N = 200: FIs planning select actions; N = 146: FIs planning to add new technology, fielded April 29, 2022 – June 3, 2022

CONCLUSION

Financial institutions searching for ways to combat increasingly sophisticated forms of financial crime and fraud must also stay compliant with regulations when trying new technical solutions. This research reveals that FIs implementing AI- and ML-powered solutions have the greatest success in mitigating financial crime risk. However, the implementation of these new anti-crime solutions can be a challenge for FIs of any size.

This research also indicates how FIs of differing asset sizes can overcome these challenges and achieve simplicity. The relative cost and complexity of fighting modern fraud may lead smaller FIs to consider partnering with service providers who can deliver high-performing services at an economy of scale.

Mid-size FIs need to overcome their relatively high fraud rates and high total cost of fraud to release resources for innovation. To achieve this, they can invest in modern technologies, including AI and ML, to improve results and operational efficiencies.

Larger FIs are more likely to already have invested in modern technologies, but the high total cost of fraud among those larger FIs would indicate that technologies are not currently optimized. Exploring deep learning and other innovations could help them manage false positive ratios as fraud volumes keep rising, and support them as they tackle emerging fraud threats.

A self-learning anti-fraud and financial crime technology that offers advanced anti-fraud and compliance features and simple integration with existing technology will provide FIs and their customers with the best protection against financial crime and fraud loss.


RS:/0211 SEARCH... A01
RS:/0211 SEARCH... A01
SEARCH TR/01 03
SEARCH TR/01 03
SEARCH TR/01 03
SEARCH TR/01 03
RS:/011
RS:/011
RS:/0211TR /ON
RS:/0211TR /ON

METHODOLOGY

The State Of Fraud And Financial Crime In The U.S., a PYMNTS and Featurespace collaboration, provides the first comprehensive data and analysis on fraud and financial crime from the perspective of the largest FIs in North America. We conducted a survey of 200 executives at FIs with assets of at least $5 billion from April 29, 2022, to June 3, 2022, to uncover how FIs will adapt to the rising challenge of fraud and financial crimes. Of the firms surveyed, 43% had asset sizes between $5 billion and $24.9 billion, 24% between $25 billion and $99.9 billion, 12% between $100 billion and $499.9 billion, and 22% had assets greater than $500 billion.

ABOUT

PYMNTS

PYMNTS is where the best minds and the best content meet on the web to learn about "What's Next" in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

FEATURE SPACE
OUTSMART RISK

Featurespace is the world leader in enterprise grade technology that prevents fraud and financial crime. With a mission to make the world a safer place to transact, Featurespace helps banks and financial institutions protect customers, and reduce risk and business operating costs by providing industry-leading machine learning, financial crime prevention solutions.

Featurespace invented Adaptive Behavioral Analytics and Automated Deep Behavioral Networks and is the first to profile both genuine and fraudulent behavior to identify and block criminal activity in real time. Both are patent pending technologies that are central to Featurespace's award winning ARIC™ Risk Hub.

Over 70 direct customers and 100,000 financial institutions have put their trust in Featurespace's technology including HSBC, NatWest, TSYS, Worldpay, Marqeta, Contis, Danske Bank, Akbank, Edenred and Permanent TSB. Founded in 2008, and headquartered in Cambridge, UK Featurespace has a team of over 400, operating globally from seven locations.

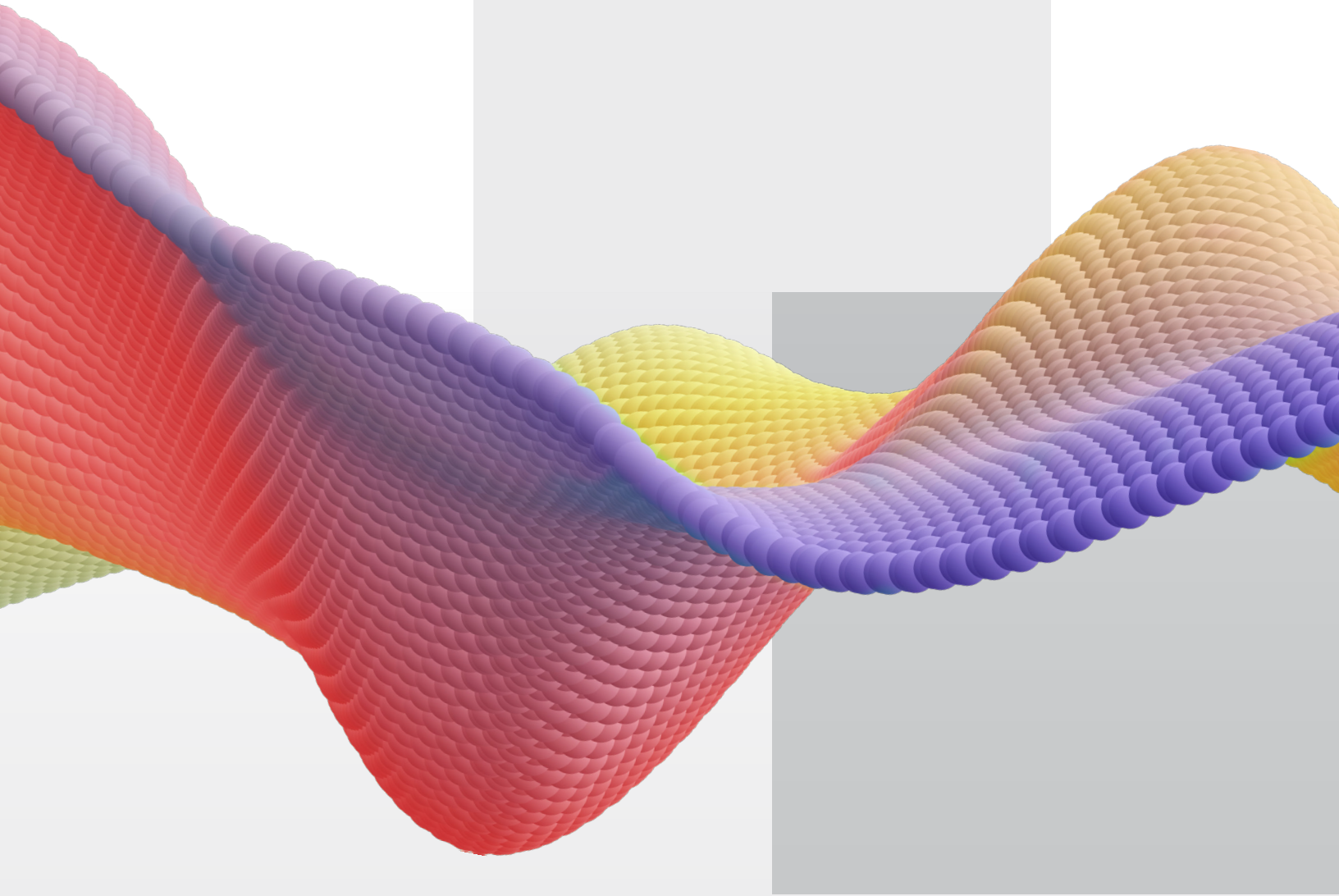
We are interested in your feedback on this report. If you have questions, comments or would like to subscribe, please email us at feedback@pymnts.com.

DISCLAIMER

The State Of Fraud And Financial Crime In The U.S. may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS.COM: 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.COM 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.COM 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.COM 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.COM 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.COM 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.



The State Of Fraud And Financial Crime In The U.S., a PYMNTS and Featurespace collaboration, is based on a survey of 200 executives working at FIs with assets of at least $5 billion. The survey was conducted between April 29, 2022, and June 3, 2022. Surveyed executives held leadership responsibilities in fraud and risk operations, money laundering, fraud strategy, fraud analysis, technology and data science; 177 of our respondents held responsibilities in fraud management, 39 had responsibilities in data science and technology and 20 led AML efforts, with some executives responsible for a combination of the above.