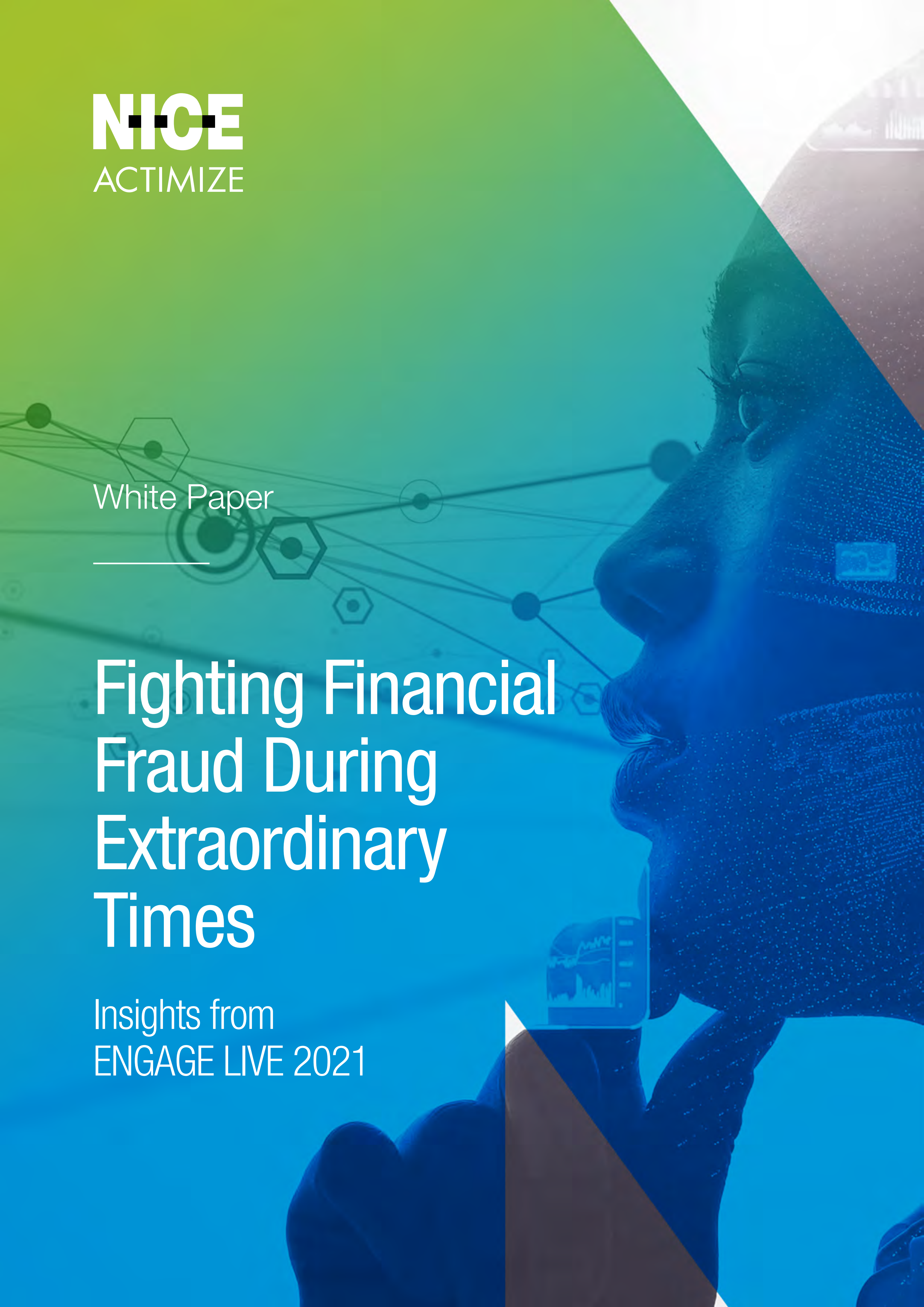
NICE
ACTIMIZE

White Paper

# Fighting Financial Fraud During Extraordinary Times

## Insights from ENGAGE LIVE 2021



# Contents

# Executive Summary

## 2020 was unlike any other...

Faster payments, new customer demands, shifting behaviors, pervasive digitization, and regulatory changes.

These disruptions have resulted in an unprecedented paradox for financial services organizations (FSOs): a once-in-a-generation opportunity and a perfect storm of risk.

**NICE Actimize ENGAGE LIVE 2021** brought together leading fraud experts, industry thought leaders and practitioners to explore the changes that emerged over the past 18 months, the challenges facing FSOs today, and the imperatives of the future.

Fraud moves quickly, and fraudsters are constantly attempting to exploit vulnerabilities. Digitization and faster payments have compounded the challenges surrounding real-time fraud detection and prevention, and put new stressors on fraud risk and operations teams. To remain agile in today's environment, FSOs need the power of AI, the scalability of the cloud, and the actionable insights of fraud data.

Across the globe, and the continued transition to digital and instant payments usher in fundamental changes to fraud strategies and controls. In the U.S., there are sharp rises in identity and new account fraud and increased focus on mule activity. In Europe, there's focus on robust customer authentication and liability shifts surrounding authorized push payments and social engineering scams. In APAC, fraudsters are targeting new and emerging digital payments as use of cash diminishes.

To keep up with the ever-changing landscape of fraud prevention, FSOs have to leverage an effective and adaptive fraud program driven by the rapid acquisition and operationalization of new data and intelligence throughout fraud management.

**— Yuval Marco**
General Manager, Fraud & Authentication Management

# 2021: The Year of Intelligence-Driven Fraud Prevention

## Evolving Fraud Threats Demand Evolving Fraud Prevention

Trusted by the world's leading FSOs, NICE Actimize helps you acquire, retain and grow your customers safely with the next generation of enterprise fraud management - **IFM-X**. Providing end-to-end fraud protection and the ability to adapt to new and emerging fraud threats, **IFM-X** protects every touchpoint across the customer lifecycle.

At NICE Actimize, we believe that fraud prevention is not a destination, but a journey. Our innovative focus revolves around this perspective and is reflected in our dedication to continuous investment and development in the advanced analytics and artificial intelligence-fueled capabilities necessary to meet extremely demanding modern risk management requirements.

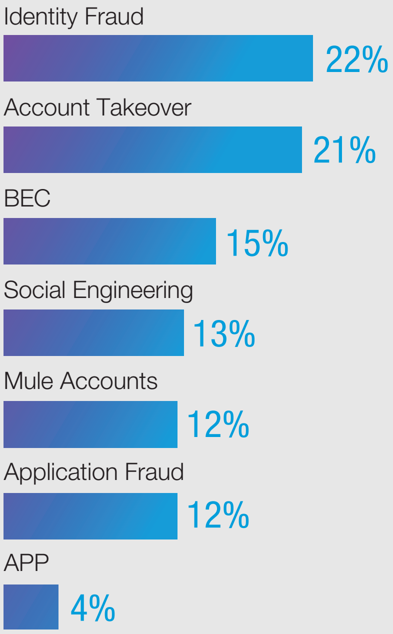
To win the fight against fraud in the long run, firms must come together and leverage data and insights from across the industry - not just from the limited view of the individual organization. This Collective Intelligence will be an integral aspect of every FSO's fraud prevention strategy in the future, alongside analytics accuracy and agility to constantly improve fraud detection.

These are extraordinary times to fight financial fraud, and ENGAGE LIVE explored the foremost concerns for fraud and cybersecurity teams and the areas that will impact fraud management today, and in the coming years.

We hope this white paper will serve as a valuable resource for FSOs as they advance and scale their fraud prevention strategies and agendas in a rapidly evolving threat environment.

## Voice of the Client:

### Top fraud concerns for 2021



# Instant Payments Ramp Up Fraud

In the financial services space, 2020 was the year of the great digital adoption, particularly in real-time payments.

> **Technology is reshaping how both consumers and organizations perceive instant payments and leading to a profound generational change that's accelerated by the pandemic.**

Consumers want the convenience of making payments from their own devices and they want to be paid faster. More consumers are using mobile banking, real-time, and P2P solutions, such as Zelle and Venmo, as virtual banking becomes mainstream.

The shift to digital banking is further evident in the growth of real-time payments transaction volumes. The RTP system from the Clearing House is experiencing substantial growth and currently running approximately 10 million transactions per month, with volumes further doubling every six to ten months.[1]

But consumers and businesses aren't the only ones embracing new technologies - fraudsters are also early adopters.

The pervasive adoption of instant payment channels and networks has opened the doors to more fraud while simultaneously making fraud prevention more difficult.

- **FSOs are opening up their infrastructures to third-party applications** to enable payment initiations from various instant applications.
- **Fraudsters manipulate customers into using new platforms** where transactions are authenticated or initiated in the third-party application that the bank doesn't control.
- **Organizations struggle with lack of end-point detection** when customers use third-party applications.
- **Institutions face barriers to obtaining enough data and information** to ensure risk engines can work as effectively as possible with the institution's systems.

> "What we see now with instant payments is that fraud is going faster… and we need to rethink a lot of our actions to potentially be able to prevent fraud with instant payments."
>
> **— Terje Fjeldvaer**
> Head of Financial Crime Centre, DNB Bank

[1] Lee Kyriacou, VP, Real-Time Payments, The Clearing House. Lee Kyriacou, VP, Real-Time Payments, The Clearing House. "Securing Existing and Future Real-Time Payments with AI." Engage Live, session 4.

> “I think it’s about being prepared for the shift to instant payments and not having fraud as a second thought. You’ve got to make it part of your plan.”
>
> **— Michael Timoney**
> Vice President, Secure Payments, Federal Reserve Bank of Boston

# Instant Payments Drives New Fraud Trends

Instant payments offer a number of attractive incentives for fraudsters, who can use real-time payments to get their cash instantly to anyone, anywhere. Criminals use this opportunity to perpetrate a number of devastating scams on consumers, which is shaping fraud trends in the instant payments world.

### Account takeover (ATO)

On the unauthorized side, fraud is emerging as **ATO** issues, where the user issuing the instructions to the bank to make a payment is not authorized.

### Authorized Push Payment (APP) scams

Authorized fraud is increasingly manifesting as **APP scams**. The sender is manipulated into authorizing a payment that they don’t actually want once they understand the circumstances.

### Peer-to-Peer (P2P) fraud

In 2021, P2P fraud losses will be at their highest level as instant payment apps continue to emerge. P2P fraud will only grow because unlike wire transfers, for example, which are often manually reviewed and require multiple verifications to complete, P2P represents an ideal vehicle for a fraudster to get paid.

# Changing the Game for Fraud Management

The adoption of faster payments is a game changer when it comes to fraud management. FSOs must examine their strategies around risk appetite vs. the customer experience, and reevaluate how to strike an optimal balance.

> **FSOs are exploring the potential of technology beyond an instrument for reducing fraud losses and operational costs, and as an enabler for digital banking and differentiating customer experiences.**

To secure instant payment channels while maintaining momentum of real-time and faster payments, the approach to enterprise fraud management (EFM) has to be improved.

To secure instant payment channels while maintaining momentum of real-time and faster payments, the approach to enterprise fraud management (EFM) has to be improved.

### Continuous model optimization

Monitoring only money movement is often too late given the shift to real time. All events that lead to money movement must be monitored, which drives the need for more accurate models that are continuously optimized to prevent the model degradation that happens over time.

### Enhance fraud analyst efficiency

Many of the faster payments networks come with a 24/7 requirement for transactioning, which introduces substantial stress on fraud operations teams. There's a need for smarter automation, and more accurate, faster decisioning on the fraud operations side to equip fraud analysts to work more efficiently while the window of investigation is dramatically shortened.

### Educate customers

FSOs need to emphasize education on phishing schemes to increase consumer awareness regarding use of instant payment apps. Consumers must understand where their payment is going and how the application works to better protect themselves and play an active role in fraud prevention.

### Balance risk and the customer experience

Optimal friction levels differ between customer segments and the customer's respective digital maturity. FSOs must adopt the appropriate risk-based approach, supported by data and advanced analytics, to identify behavioral patterns and optimize customer friction during instant payment transactions according to risk levels.

> "Fraud is now fought and won in data and analytics through big data early and often. The more information that you know as that entrant is coming into your site, as that payment is being made, the more that you can do to prevent fraud."
>
> **— Jen Martin**
> Head of Enterprise Fraud, Keybank

# The Threat of Identity Theft & Synthetic Identity Casts a Shadow Over Fraud Prevention

Other escalating fraud trends, such as identity theft and synthetic identity fraud, present unique challenges.

Data breaches, the increasing availability of intelligent technology and compute power, and the volume of personally identifiable information (PII) available through online sources has created a playground for bad actors to conduct fraud at scale.

> **In 2020, identity fraud cost American victims approximately $56 billion, $13 billion of which was attributed to traditional identity fraud, and $43 billion was due to identity theft scams.[2]**
>
> **In the U.S., synthetic identity fraud cost an estimated $1.8 billion in 2021, and is projected to jump to $2.4 billion for credit products.[3]**

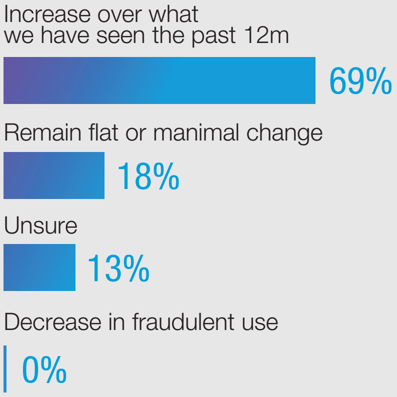
This fraud trend has quickly evolved as consumers adopted instant and digital payment methods during the pandemic, and shifted the way they shop and interact online. Around 18 million people were targeted by fraudsters through P2P payments systems and digital wallets last year. [4]

### Traditional identity fraud

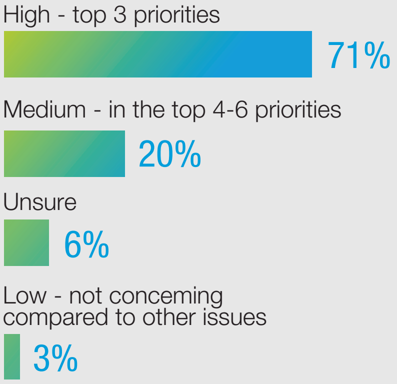
Fraudsters or cybercriminals steal PPI via data breaches or by appropriating a driver's license, for example, and use the information to commit fraud. Essentially, they're posing as another real person to use his or her credit.

## Voice of the Client:

### How will identity fraud impact your organization over the next 12 months?



### Identity fraud prioritization over the next 12 months



[2] https://www.businesswire.com/news/home/20210323005370/en/Total-Identity-Fraud-Losses-Soar-to-56-Billion-in-2020

[3] Fooshée, T. (n.d.). Application Fraud: Accelerating Attacks and Compelling Investment Opportunities (2020 ed., Vol. November, Rep.). Aite Group.

[4] https://www.businesswire.com/news/home/20210323005370/en/Total-Identity-Fraud-Losses-Soar-to-56-Billion-in-2020

### Identity theft scams

A bad actor targets a consumer directly using techniques like phishing emails, skimming, or robocalls to steal sensitive information.

### Synthetic fraud

Usually includes two main categories: *manipulated*, where minimal alterations are made to a legitimate identity, and *manufactured*, where data is pieced together from multiple real identities to create a new false identity. The main targets are vulnerable demographics that represent identity groups who are challenging to authenticate, like young adults, the homeless, the elderly, and divorced women.

## Automatic Synthetic Fraud at Scale

Cybercriminals and fraudsters go to extreme lengths, deploying sophisticated techniques and practices to collect information and elude detection. They build systems and processes to do this automatically and at scale, and even familiarize themselves with the authentication controls and technologies used by FSOs so that they can more easily bypass these deterrents.

First, the fraudster compiles as much data about an individual identity as possible through a combination of widely available online sources, primarily the dark web. Here they can inexpensively purchase PII about an individual, including addresses, mother's maiden name, and phone numbers. Underground services are often used to augment the synthetic identity further, such as virtual phone numbers to help fraudsters get through application processes that require tokens by phone.

The criminal is then able to start applying for accounts at multiple FSOs by using tools and browsers that emulate the characteristics expected to be associated with that identity, adding a convincing level of authenticity to the synthetic identity.

> "At the community bank and credit union level, the best practice that you can have is taking a holistic approach. Your authentication strategy shouldn't be something that just the product team figures out or just your risk team figures out. To strike that balance, to provide the experience that you want but also the security, it has to be holistic."
>
> **— John Garette**
>
> Product Strategy & Innovation, PSCU

> “You need to keep your fingers on the pulse on what these bad guys are doing and then you can proactively put in place controls to mitigate or really preempt fraud when it does come in.”
>
> **— Eli Dominitz**
> Founder & CEO, Q6 Cyber

## Identifying Legitimate Customers vs. Synthetics

FSOs are leveraging advanced analytics-based tools to detect fraud early on. Fraud identification processes have to be predictive using machine learning (ML) models that are trained on comprehensive data sets to discern behavioral patterns. Fraud teams can then understand and identify the types of fraud being perpetrated against the organization and make accurate, data-driven decisions.

> **Organizations are exploring the potential of technology beyond an instrument for reducing fraud losses and operational costs, and as an enabler for digital banking and differentiating customer experiences.**

## Keeping a Watchful Eye on Dark Web Activity

Another key element in the fight against synthetics and stolen identities is tracking activity on the dark web, deep web and other underground communities, forms, apps and platforms used by cybercriminals and fraudsters.

This can provide organizations with the intelligence to stay ahead of criminals and fraudsters:

- Critical trends and popular tactics and tools used to commit fraud and financial crimes, like how to effectively compromise PII.
- Schemes and techniques that have been adapted over time, are being currently planned, or in the initial stages of activation.
- Pinpoint specific campaigns that are targeting certain types of FSOs or regions.

## Delivering Stellar Customer Experiences that Align with Risk

When addressing identity fraud and synthetic identity fraud, organizations are focusing on data collection, data integration, and data enrichment to add value for passive authentication solutions. This approach helps organizations deliver the right amount of friction based on customer risk level while simultaneously securing channels.

Passively collecting data and building digital identity profiles around the data points of every good interaction, and using this as a baseline to verify against, can mitigate the need for cumbersome friction touchpoints across every transaction - which ultimately results in a poor user experience.

Instead, FSOs should be smoothly ushering customer's along to the application page or product and provide an experience that aligns with that customer risk level.

## Growing Identity Risk Programs

The key to deploying a tailored degree of friction per individual customer is by using abundant quantities of data to authenticate identities and augment any missing information, and advanced analytics to recognize and manage risk across the customer lifecycle. FSOs can then mitigate fraud based on a holistic view of risk and identify legitimate customers to streamline conversion.

When layered with dark web monitoring, FSOs can **transform from reactive to proactive fraud prevention** and put the right controls in place to render identity fraud and synthetic identity fraud threats ineffective.

Many organizations, such as those at the community bank and credit union level, aren't in a position to use resources to build these capabilities themselves. Partnering with industry leaders in the fraud prevention domain can provide these institutions with the guidance and capabilities to leverage advanced analytics-powered fraud prevention at scale.

> "Right now so many of the customers we're working with are making that leap from using static data to employing their own data science and machine learning so that they can start having more predictive approaches and pattern matching to identify this more sophisticated fraud."
>
> **— Kurt Weiss**
> Director of Financial Services, Ekata

# Unlocking the Value of Data for Actionable Intelligence

The proliferation of digital channels has given organizations access to massive amounts of data that can be used to attract and retain customers, and mitigate risk.

But understanding what to look for and how to interpret it is another challenge.

## Data-Driven Insights

Deriving insights from data requires specific capabilities, tools and skill sets. FSOs need fraud data management experts who understand what data to look for, which data points are worth spending time on, and which data points are less relevant.

NICE Actimize applies our fraud expertise toward generating actionable information to share with clients for fraud detection.

Fraud is dynamic and trends migrate; being plugged into the industry via collective intelligence helps organizations balance fraud processes and the customer experience, and proactively anticipate some of the challenges that other institutions are experiencing.

## Data Segmentation and Categorization

There are different types of data that are particularly relevant for detecting fraud risks:

### Transactional data

Encompasses both monetary and nonmonetary transactions, and includes all of the events that an FSO processes through their various banking channels. Information might include the transaction amount, login, timestamp and the event types, like loan application, card application or wire transfer.

### Channel data

This covers information such as the type of device or communication in which the account holder is interacting with the bank, bank system, bank application or bank website. If it's a web-based event, for example, this would include the IP address and browser information. If it's a mobile device, then the information would include the mobile brand and mobile app version.

### Customer and account data

Includes customer and account information as it is represented in the bank's CLM system, which might include names, addresses, phone numbers and account balances.

These categories are important as organizations accelerate enterprise-wide digital transformation. Risk complexity, velocity and intensity necessitates that this data be captured, contextualized and leveraged to efficiently combat first and third-party fraud.

To understand the context of different threats, FSOs need the advanced analytics capabilities of an integrated fraud management platform that has the compute power and data availability to accurately contextualize risk and provide a single view of the customer across different risk types.

> "To get the context of these types of threats we're dealing with, you have to work across AML, cyber and fraud, and get that richness of information and bring it together and contextualize it based on a device and a customer."
>
> **— Ian Mitchel**
>
> Global Fraud and Financial Crime Executive

## A Bigger Picture of Fraud

A common thread throughout fraud prevention and detection capabilities and best practices is the importance of data and collective intelligence.

> **Organizations need high quality, relevant, actionable data to help ensure success, as well as an industry-wide view of fraud trends and patterns defining the threat landscape in order to sharpen their approach to financial crime risk management.**

## Cross-Industry Insights Sharing is the Future

Considering the shift to instant and faster payments, the rise of identity theft and synthetics, and the breadth of other fraud threats and digital disruption, cooperation across FSOs will play a crucial role in the future of financial crime risk management.

Many European banks currently use a model of cooperation and data sharing. In Scandinavia and Nordic countries, financial integration and cooperation is facilitated via the Nordic Financial SUERF community. Member banks share non-sensitive data, like mule accounts and login data, and other information that is critical to preventing attacks and promoting better financial crime risk management.

However, in the U.S., there are thousands of banking institutions, fintechs and community banks, and fraud is frequently addressed differently per institution. While common standards on fraud are continuing to be defined, many FSOs in the U.S. are eager to explore potential connectivity initiatives between institutions to communicate fraud trends and events more seamlessly than is currently possible.

NICE Actimize views cross-industry insight sharing as a strategic direction for the industry and shares aggregated trends and benchmarking data via **ActimizeWatch**. Sharing aggregated, anonymized data has been helpful in informing fraud strategies and priorities for participating institutions, and new solutions are in development to leverage this collective intelligence even further while maintaining the required privacy, security and compliance standards.

> "We have to keep up with that speed of fraud. I think where the industry is with the massive amount of data - not just data that can be breached, but just the sheer massive amount of data that's available - that creates this perfect situation for identity fraud, account takeovers and synthetic identities."
>
> **— Naureen Ali**
> Senior Vice President Fraud,
> Deposits & Payments,
> PenFed Credit Union

## Accelerate Fraud Fighting in a Perfect Storm of Risk

Collective intelligence for financial crime management uses the power of many to transfer learnings and insights to fight crime faster than ever before.

It gives fraud fighters a distinct advantage in staying a step ahead of the speed of fraud. For example, a specific fraud threat may be impacting the industry but may not yet have hit a particular FSO. Because the models are already included in the collective intelligence network, this threat is already accounted for.

This is a potent asset in an environment of exacerbated fraud. Today, the speed at which high performing models detect aberrant or deviant behaviors matters and significantly impacts the ability to keep up with the rate and complexity of fraud. The more sophisticated, targeted and differentiated the models, the better situated an organization is in mitigating some of the most complex types of fraud.

> "The ever-evolving dynamics of opportunities and threats don't leave any room for firms to take a wait and see approach – those that do, risk falling behind the competition or failing outright.
>
> The same goes for financial service organizations when it comes to financial crime. In this climate, it's critical to move faster than the speed of crime. Failure to innovate and comply puts firms at risk for heavy penalties, reputational damage and dissatisfied customers."
>
> **— Craig Costigan**
> CEO, NICE Actimize

**Fraud is not always an isolated event; fraud types slide across all channels and products, and FSOs can no longer take a singular view of fraud.**

Fraud truly personifies a perfect storm, including ATO, card breaches, skimming, synthetic identity fraud, APP fraud, identity scams, P2P fraud, and digital currencies.

Fraud fighters must equip themselves to contend with this storm and leverage the cloud and advanced ML to effectively protect their institutions against numerous fraud typologies – all while enhancing the customer experience.

# Advanced AI & Machine Learning Revolutionizes Fraud Fighting

Advanced artificial intelligence (AI) and ML in fraud prevention is a key focus of NICE Actimize's analytical vision and a vital component in addressing the range of challenges surrounding fraud prevention.

We recently introduced a new federated learning technique that is uniquely suited for the continuous changes associated with fraud detection.

## What is Federated Transfer Learning?

Federated Transfer Learning is an ML technique that trains algorithms across multiple distributed machines that are holding local data samples - without exchanging or sharing data. Conversely, traditional approaches involve a centralized ML algorithm running on one server where all of the data samples are stored.

> **A recent NICE Actimize case study using this technique resulted in a 20 percent improvement in fraud model performance. The model was documented with a richer set of detection features leveraging federated transfer learning.**

The goal during the development of this technique was to use segregated data repositories and avoid data sharing between FSOs. Numerous models are trained on segregated data sets separately, but the learnings are transferred and used as detection features for new fraud models.

# What is Online Incremental Machine Learning?

This technique solves the problem of automation in the scalable production of ML models. An important challenge is ongoing maintenance of huge amounts of models, which includes monitoring models for performance, tracking degradation over time, periodically retraining the models and redeploying models.

Online incremental machine learning eliminates the manual model training stage; instead, the models are trained online because they run on streaming data. This approach enables real, continuous and incremental model learning without the need to worry about performance degradation or model retraining.

# Client Impact

- Impacts the entire model production by simultaneously increasing production scalability and reducing maintenance costs and the amount of data scientists needed to provide solutions at scale.
- The models capture data trends and patterns almost instantaneously, drastically reducing time-to-insights and time-to-business-impact.
- Fraudulent activities can be detected in real time the moment fraud happens.

# New Applications of Deep Neural Networks

Applying deep learning methods into fraud prevention is another primary focus for NICE Actimize. Deep learning solves one of the most difficult problems with feature development by allowing features to be enriched to increase model accuracy and precision.

Indicative features are engineered by analysts and reflect a more complicated meaning behind the data. They are representative features that depict the domain knowledge well.

Indicative features are representative features that depict the domain knowledge well. They’re stand-alone features that are non-redundant, don’t overlap with each other and ensure top model performance. Because so many features are fed into fraud prevention models, it’s important to have high quality features.

Deep learning automates feature engineering development and once this robust process of feature engineering is applied, indicative features can be enriched.

## Benefits of Deep Learning for Fraud Prevention

- **Improved incremental data quality** for training models.
- **Automated feature engineering processes** to reduce cost maintenance and time-consumption of product or business analysts.
- **Development of robust, stable, accurate** machine learning models.
- **Alleviates imbalances in data** that can cause model drift.
- **Generate synthetic data** that preserves the privacy of the initial data.

## Why Deep Learning Now?

Applications of deep learning require intensive resources, strong hardware and huge amounts of data. With the move to the cloud, NICE Actimize had the opportunity to realize the power of deep learning technologies incorporating the cloud, and can support and deploy large amounts of data on a scalable production.

Furthermore, financial data differs from other types of data and domains; it has a special structure called tabular data and dedicated frameworks for applying deep learning on tabular data that have only recently been developed.

# Fraud Prevention in the Customer Experience Era

While FSOs aspire to prevent fraud losses, focusing on the customer is also critical.

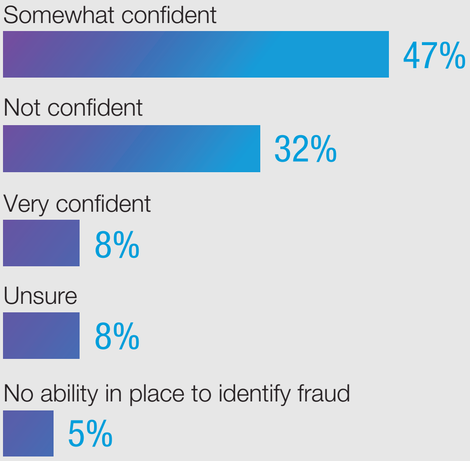
> **Do retail and corporate banking customers expect to experience a certain level of friction to validate the trust that they've placed in the FSO?**

One argument suggests that if friction is user-friendly, and the customer is able to quickly transition beyond that friction during a legitimate transaction, then many customers accept a certain degree of friction. Some customers want to opt-in and be alerted for every banking transaction, whether that's a debit payment, wire transfer or ACH. Others only want to be alerted if a transaction is truly suspicious, and FSOs should have the data and analytics tools in place to support customers and their preferred level of fraud defense.

On the other hand, some customer segments, depending on their level of digital maturity for example, want less friction because they understand that they can have secure solutions with minimal friction. Given that FSOs are competing with fintechs and third parties that want to introduce transactions through their infrastructure, they need to address the desire for minimal customer friction during authentication while improving security.

## Voice of the Client:

### Level of confidence your organization can detect identity fraud



## Earlier Fraud Prevention

The industry is shifting their fraud prevention focus toward new clients earlier in the lifecycle to address fraud risk while optimizing the digital experience - either during the account origination process itself or immediately after account origination.

With the commoditization of PII on the dark web accelerating synthetic identity fraud, and the demand for near frictionless digital banking experiences, FSOs are under pressure to replace siloed approaches to fraud prevention that are easy for fraudsters to exploit.

NICE Actimize's **New Account Fraud** provides coverage earlier at the application stage and helps organizations optimize friction levels.

- **Advanced analytics connect existing identity verification data and tools** to provide a single identity risk score for efficient risk decisioning.
- **Seamlessly links application data and identity risk scores** into an early fraud monitoring system.
- **Accurately detects sophisticated fraud** stemming from stolen and synthetic identities, and mule activity.
- **Streamlined transition into ongoing monitoring phases,** supported by intelligence collected during both the application and early monitoring phases.
- **Zero-trust risk profiling fueled by advanced AI** to enable intelligent early account access and safeguard against fraudulent accounts at account origination.

## Transforming Fraud Prevention into Competitive Differentiation

A lucrative opportunity is available for FSOs to acquire, retain and grow their customers - if they can optimize how they work with customers and deliver a trusted, digital-first experience.

But emerging fraud patterns are straining the ability to execute effective fraud prevention while providing safe, enhanced customer experiences.

There's a meaningful generational shift surrounding purchasing power that not only impacts how customers engage with digital banking, but how fraudsters operate. Fraudsters are now adapting their tactics according to different generational personas, which is evident in the fraud schemes and typologies deployed against each generation.

## Generational Differences

Each generation interacts, understands and uses technology differently, and fraudsters trigger customers based on this knowledge.

- **Gen-Z:** This generation is entering into independence and spending their own money, and are typically targeted through chatbots and social media messages.
- **Millennials:** Targeted via text messages and other automated messages that promise rewards or shipment tracking, and are vulnerable to phishing attacks.
- **Gen-X:** As the generation between Millennials and Baby Boomers, this generation is often susceptible to the fraud schemes that attack the generations above and below them.
- **Baby Boomers:** Tend to be targeted through robocalls about healthcare, taxes or social security.

Gen-Z and Millennials are early digital adopters and represent emerging affluent generations. Because they will be experiencing significant life changes in the near future, including buying homes and cars, FSOs are looking to establish early relationships with these customers and provide excellent experiences to attract and retain them.

Gen-X and Baby Boomers tend to bank with the future in mind as they're already settled in life. Unlike younger generations, they're familiar with standard banking interactions but open to new ideas. For example, a decade ago it was a novelty to hear of grandparents texting their grandchildren, but this generation has adopted technology and now it's the norm. Baby Boomers mirror younger generations in their adoption of digital in their interactions, but generally do so at a slower pace.

> "The psychological aspects in which the fraudsters take into consideration is amazing, and if you understand that and apply that to your customers, you could not only protect them, and think like they do, but you could also identify where their vulnerabilities may be."
>
> **— Terje Fjeldvaer**
> Head of Financial Crime
> Centre, DNB Bank

> "We need to focus on a full level of input to our fraud prevention tools to appropriately segment the risk and give the friction where needed. Truly focus on thinking about the right segmentation and using all the data at hand across the board for the customer - a full customer experience, not just in silos or a single point."
>
> — **Ben Geertz**
> Senior VP Fraud and Claims Management, Detection Analytics, Wells Fargo

## Earlier Fraud Prevention

FSOs need to adopt a customer-centric approach to fighting fraud according to different generational vulnerabilities.

If customers understand various types of scams then they can better protect themselves. FSOs should take the opportunity to educate customers at every viable point in time so the customer is aware and able to judge for themselves as to what could potentially occur.

To grow more meaningful, impactful relationships with their customers and become trusted partners during uncertain circumstances when fraud does occur, organizations should:

- **Communicate and be transparent** regarding the levels of friction their customers are experiencing with access or transactions.
- **Continuously introduce new techniques** to educate and improve customer awareness of fraud at critical points in time.

## Personalizing Protection by Customer Persona

Understanding different customer personas and how they interact can drive organization-wide benefits, including fraud and operations teams.

> **Customer empowerment must be linked to fraud prevention processes, including enabling customers via digital tools and new interaction channels. This introduces cost optimization, customer stickiness, organization efficiency, and can result in new opportunities.**

- **Data and advanced analytics:** Data and advanced analytics helps secure the payment methods that newer generations are adopting, and helps organizations protect older generations that might not be familiar with some technologies. It further helps FSOs accelerate their digital-first, mobile-first presence.
- **Meaningful friction:** Customers expect 24/7, secure access to financial services. FSOs must develop segmented strategies that focus on the specific risk, and add targeted friction without making authentication overly challenging for their customers.
- **Deliberate segmentation:** Using multiple point solutions and alert systems prevents organizations from gaining a full picture of the customer. Focus on the right segmentation and utilize all available data to deliver a complete customer experience - not just in silos or a single point.

# Protecting the Entire Customer Risk Lifecycle from Fraud

Because FSOs are constantly exposed to new and emerging fraud vectors and complex fraud risks, they need end-to-end coverage against threats while enabling continual, safe account growth via superior digital banking experiences.

**IFM-X**, the industry-leading intelligent fraud management platform, adapts to new and emerging fraud threats now and in the future. With agile advanced analytics and advanced AI, FSOs can holistically safeguard the customer lifecycle across all channels and payment types.

## Always on AI

Fueled by industry and behavioral intelligence, **Always on AI** understands customer patterns and continuously learns, discovers and adapts to rapidly detect anomalous activity and prevent sophisticated fraud attacks.

## More Advanced Analytics & Automation Capabilities

Supervised and unsupervised learning models with predictive capabilities, cross-enterprise model insights, and faster, streamlined model operationalization and governance processes allows for more AI, ML and automation capabilities to be continuously embedded in **IFM-X**.

## Proven Fraud Analytics

The entire fraud management ecosystem is connected by a single fraud prevention solution, which uses advanced AI to orchestrate data across all point solutions to create accurate fraud analytics. **IFM-X** quickly consumes data to detect and alert earlier, accelerating alert resolutions and centralizing all fraud prevention activities.

# Final Thoughts

If there's anything the past has taught us, it's that fraud prevention continues to be dynamic.

The risk landscape is growing more varied, complicated and automated. Just as FSOs rely on new technologies for digital transformation, fraud prevention and the customer experience, fraudsters and criminals rely on new technologies to exploit every available avenue to diversify their techniques and commit more complex fraud.

Traditional approaches to fraud prevention simply won't suffice in today's threat environment. FSOs must be future-facing in their approach to fraud prevention and fraud prevention and detection, and leverage high-quality data, next-generation advanced analytics and the cloud to protect their institution and customers from sophisticated fraud.

As a solution designed for future functionality and scalability at both the platform and solution level, **IFM-X** accelerates the journey to holistic fraud prevention and introduces new intelligence-driven innovation for fraud fighters. Complete, holistic and end-to-end fraud prevention optimized with continuous self-learning capabilities ensures that FSOs can evolve their approach to fraud prevention alongside constantly changing risks.

With the ability to develop and leverage more sophisticated analytics algorithms and more data, FSOs can put collective intelligence into action to stay ahead of the speed of fraud.

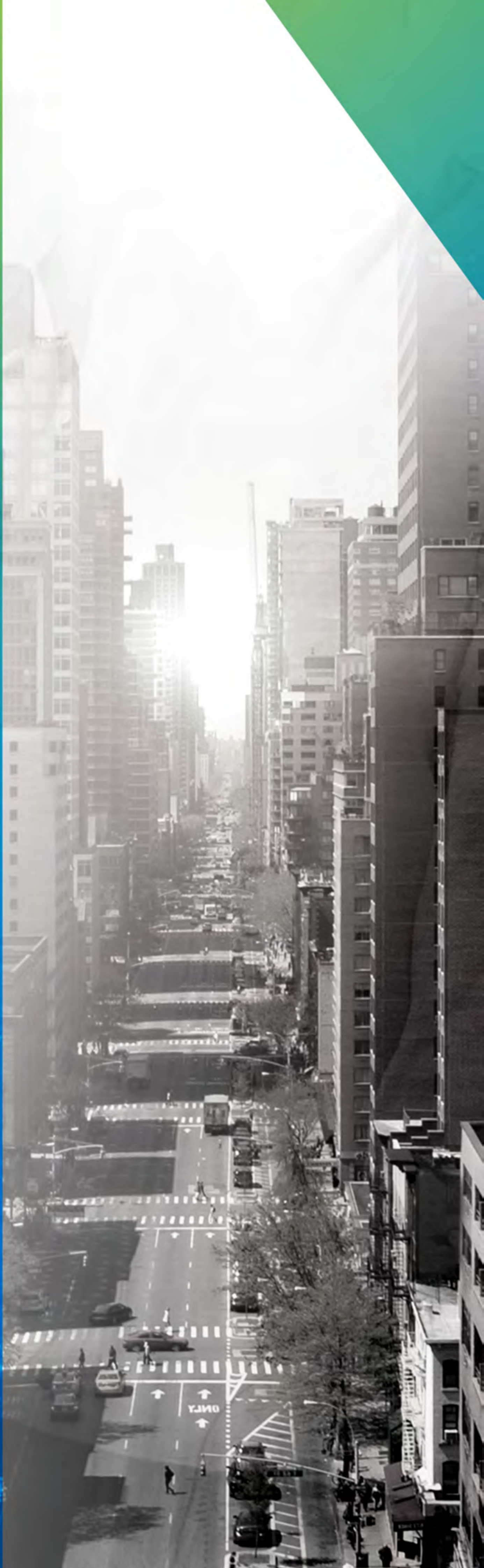
As we move forward, we remain committed to our evolving analytics vision and are excited to continuously share our ongoing developments with the industry.

Thanks for joining us and stay tuned for what's next.

**— Glenn Fratangelo**
Head of Strategy and Marketing
Fraud & Authentication Management

Get the latest NICE Actimize updates.

STAY IN TOUCH >



## About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance.

The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

Find us at www.niceactimize.com, @NICE_Actimize