The Latest in Fraud Detection and Prevention

NICE ACTIMIZE

Using Advanced Fraud Technology for Frictionless Customer Experience

eBook

NICE · ACTIMIZE

Strengthening your fraud strategy is no easy task, with rapidly changing threats and new options for advanced technology. Read on to discover the latest fraud fighting trends to enhance fraud prevention.

Access our recent ENGAGE Fraud & Authentication Management track sessions to hear about the latest trends and best practices to address your toughest challenges.

Watch Now

Table of Contents

The Journey to Autonomous Fraud Management

When the journey to autonomous fraud management began, the goal was for a paradigm shift from machines assisting humans, to humans assisting machines. To achieve this ambitious goal, significant investment was required in:

- **Data Acquisition & Management:** With increasingly fragmented and siloed data growing, more data sources than ever, and the proliferation of point solutions for additional risk intelligence, FIs must be able to acquire, integrate and operationalize data quickly to create valuable insights.

- **Agile Analytics & Decisioning:** The introduction of tools and automation to accelerate the overall model optimization and delivery cycle helps FIs develop better and faster risk models – as well as automate their decisioning and policy management.
- **Holistic Fraud Risk:** Accelerating into a digital-first world requires expanding the coverage to achieve a holistic and cross-channel view of fraud risk.

NICE · ACTIMIZE

When the journey to autonomous fraud management began, the goal was for a paradigm shift from machines assisting humans, to humans assisting machines.

Watch Now

Immediate Action Required! Detecting Authorized Fraud

NICE · ACTIMIZE

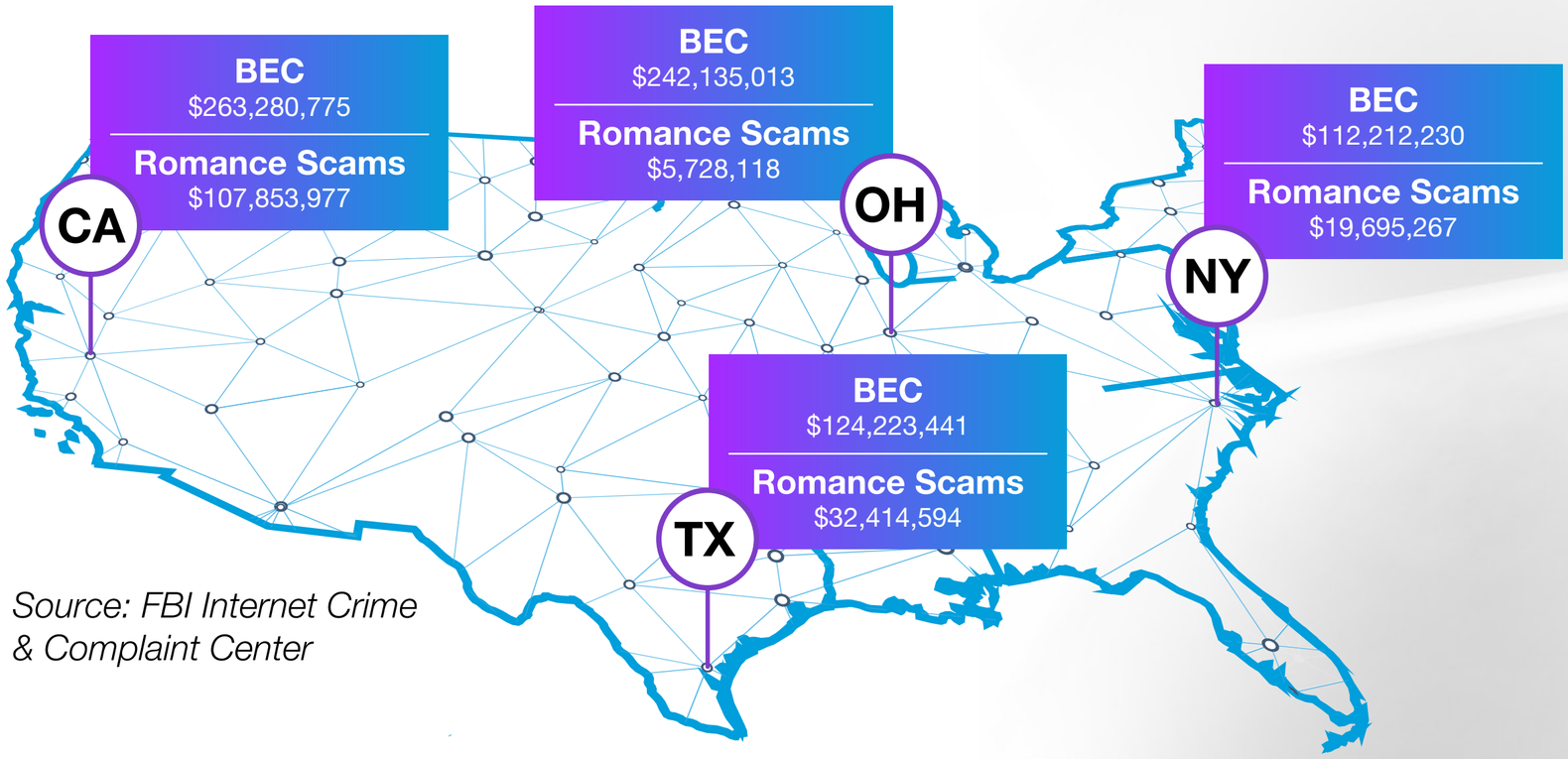
Authorized Fraud, or Authorized Push Payment Fraud, is a broad classification for a type of fraud where the customer is deceived into making a fraudulent payment.

The FBI reports that between June 2016 and July 2019, there were 166,000 victim reports that the IC3 were made aware of, totaling $26 billion USD, from 177 countries.

Customers are often the weakest link in cases of authorized party fraud, because they are trusting and can be manipulated. Often, many fraud schemes are not overly sophisticated but can still snare customers who may be less savvy or in a vulnerable position. 2019 was been a perfect storm with data breaches hitting records, and now the surge of digital payments accelerated by the 2020 global pandemic.

If a fraudster has access to identity and account numbers, all first line of defenses are breached and “authorized fraud” will be the preferred method of transferring our money.

BEC & Romance Scams in the U.S. Totaling over $2 Billion in 2019



Source: FBI Internet Crime & Complaint Center

Catch Me If You Can - Digital Identity Challenges

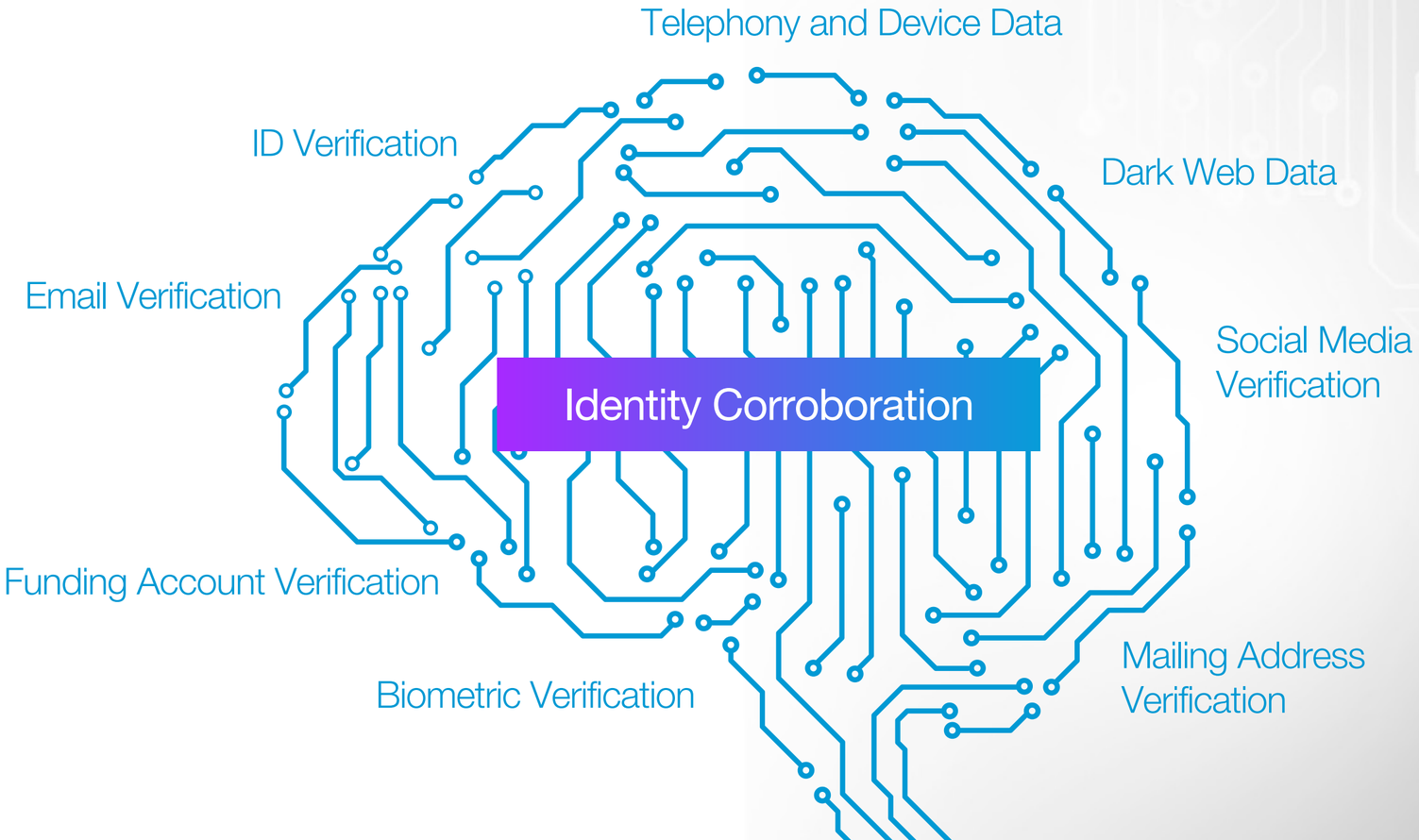
NICE · ACTIMIZE

The growth of digital services is growing exponentially, and COVID-19 has only accelerated that pace of adoption. As new products and services come online, it also increases the responsibility of financial institution to verify identities of their customers.

This raises the question – can FSOs detect and defend against synthetic IDs and new account fraud, without hindering the customer experience?

Compromised accounts are used by criminals for both direct fraud, as well as part of more complicated, somewhat indirect schemes that circuitously move and pull money.

Identity fraud starts when criminals secure partial or complete identifying information. Sometimes access to this data is physical – stolen or copied documents – but more often this digital data is acquired through breaches, malware, social engineering and similar methods. In general, most types of identity fraud fall into three categories: Account Takeover, Identity Theft, and Synthetic identity.



NICE · ACTIMIZE

There is an increased responsibility for financial institutions to verify identities of their customers.

Watch Now

Fraud: AI in Action

NICE · ACTIMIZE

Effective Fraud Risk Management requires analytical tools, skills and capabilities to enable proper protection against constantly evolving and malicious fraud attacks. Advanced machine learning and AI are powerful on their own. When coupled with innovative analytic techniques to create valuable insights, these tools provide FIs with even stronger fraud models.

One example of data innovation is Federated Learning. Federated Learning is a machine learning technique that trains an algorithm across multiple distributed machines holding local data samples, without exchanging or sharing the data in any way.

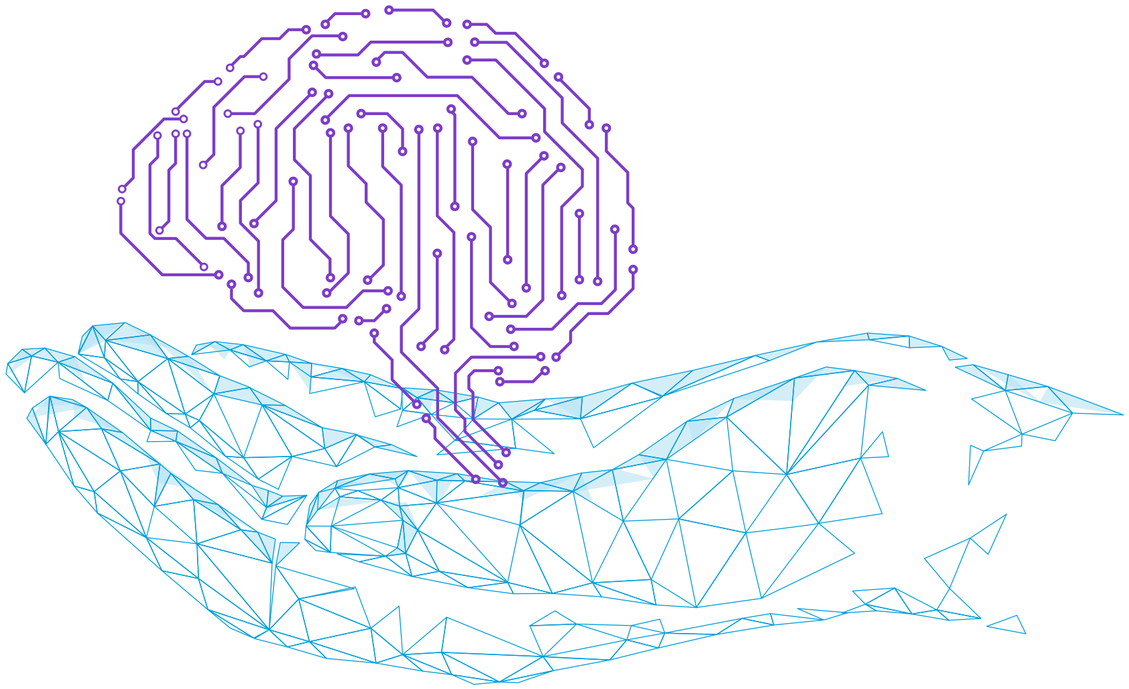
While machine learning and AI have greatly improved fraud detection capabilities, it's still a continuous journey. Operations teams, as well as regulators, need to be able to trust machine learning-based scores to properly use and evaluate these scores.

Machine Learning

Analytics

Data Science

Behavioral Analytics



NICE · ACTIMIZE

Effective Fraud Risk Management requires analytical tools, skills and capabilities to enable proper protection.

Watch Now

Future-Proofing Fraud with Advanced Technology

NICE · ACTIMIZE

The technological challenges for fighting fraud are growing daily with the advanced rate of digitalization. Financial institutions must ingest fragmented, siloed and complex data from numerous sources and specialty point solutions.

The two significant technology advances shaping fraud detection are:

- **Cloud Adoption:** Cloud is maturing as an architecture and is becoming a realistic option for FIs looking to deploy their next-generation applications. Fintechs and challenger banks are launching in the cloud. Many FIs are looking at moving all or part of their operations to the cloud. For their fraud solutions they are exploring a range of potential options to augment or replace on-premise solutions.

- **Data Integration Capabilities:** The fraud ecosystem has exploded over the past few years. Fraud systems are handling more transactions, more data and more point solutions. This creates the challenge of building an environment that can handle different asynchronous sources and combine them for risk decisioning.

New Technologies & Enhancements

IMPROVED PERFORMANCE & SCALABILITY • REDUCED TCO • LIMITLESS DATA & ANALYTICS

NICE · ACTIMIZE

Cloud is maturing as an architecture and is becoming a realistic option for FIs looking to deploy their next-generation applications.

Watch Now

Case Management to Combat Financial Crime

NICE · ACTIMIZE

Case management is the primary touch-point for financial crime operations. By connecting the dots across domains, it empowers teams to maximize their potential to fight more financial crime.

- **The Journey to the Next Level of Operational Excellence.** Learn how case management innovations are maximizing analysts' potential, and connecting organizational teams with greater collaboration and workflow consistency

NICE · ACTIMIZE

- **Making the Case for Case Management.** Industry leaders from NatWest Group and NICE Actimize come together to discuss how they are connecting disparate systems and processes
- **Connecting Across the Financial Crime Ecosystem.** The X-Sight Marketplace is the industry's single ecosystem to extend your financial crimes and compliance programs with innovative data and technologies covering the needs of AML, Markets Surveillance and Fraud managers.
- **From Fraud to SAR: The Value of Complete FinCrime Coverage.** Leaders from Alliant Credit Union, MSU Federal Credit Union, and NICE Actimize come together to discuss the lifecycle of how fraud and money laundering teams are converging and collaborating.

Watch Now >

The Changing Face of Fraud

NICE · ACTIMIZE

When it comes to scamming consumers, fraudsters tend to capitalize on the unknowns. Whether that be the learning curve of new technology, or the unknowns of a global pandemic – fraudsters will prey on these opportunities.

In 2020 we have seen a dramatic shift in the world of digitalization, especially when it comes to fighting fraud. Scams and first-party fraud are quickly emerging as vehicles of choice for bad actors. Unfortunately, most of this fraud is not traditionally managed by bank fraud departments. Therefore, many systems and tools aren't tuned to detect it, and verification methods are misaligned to the threat. Financial institutions need to step away from the siloed approaches of today's systems and move toward a more holistic approach to monitoring risk.

NICE · ACTIMIZE

Access our full ENGAGE track to discover more

Watch Now

Want to see our solutions in action?

Schedule a Demo

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.

www.niceactimize.com