THOMSON REUTERS®

AI Versus Financial Fraud:
The Next Frontier of Protection

AI Versus Financial Fraud: The Next Frontier of Protection

Financial fraud, thanks to the pandemic, is booming. Lockdowns drove financial institutions and customers en masse into the digital world, which has exposed them to new dangers. The rapid growth of online banking and the increased use of remote payment functions, remote notarization, and other aspects of digital finance have created a wide-open field for fraudsters.

Current aspects of digital finance have created a wide-open field for fraudsters.

Recent fraud statistics tell a harsh story:

- The 2021 Association of Professionals (AFP) Payments Fraud and Control Survey of over 500 treasury/finance professionals found that 65% believe the COVID-19 pandemic is to blame for some of the rise in payment fraud at their companies and that last year, 74% of respondents' organizations were targets of payment scams.
- In the United Kingdom alone, criminals stole $1 billion via bank fraud in the first-half of 2021, a 30% year-over-year increase, while authorized push payment (APP) fraud was up 71% in the same period.
- As per Feedzai's Third Quarter 2021 Financial Crime Report, the dollar amount of bank fraud in the second quarter of 2021 rose 23% compared to the same quarter in 2020.
- The amount of digital fraud attempts against financial services companies shot up 109% in the U.S. in the first 4 months of 2021, compared to the last 4 months of 2020. Globally, fraud attempts rose by nearly 50% in this period.
- The sheer volume, frequency, and variety of financial fraud stand to overwhelm traditional fraud prevention strategies. Further, it increases the likelihood of more legislative and regulatory initiatives on fraud protection that financial institutions must comply with.

Given this situation, financial firms should consider using AI applications as a key piece of their fraud protection strategy. Essentially, by using their own automated systems wisely, a firm can counter many of the downsides of greater financial automation.

Financial firms should consider using AI applications as a key piece of their fraud protection strategy.

Growing crisis, growing regulations

Fraudsters are hitting on multiple fronts; customer impersonations, account takeover scams, and "smishing" (the text equivalent of phishing, in which fraudsters seek to get personal information via phone contacts) among their most popular means of attack. The common goal is to access, control, and/or spoof a customer's digital identity to commit financial fraud.

In response, a variety of new regulations are being proposed.

In response to new fraudulent practices, a variety of new regulations are being proposed.

Greater identity protection measures. The Improving Digital Identity Act of 2021, introduced in Congress, would create an executive-level task force that would coordinate with federal, state and local authorities (including the Social Security Administration (SSA) and state-level Departments of Motor Vehicles) to enforce stricter digital identity verification standards.

The SSA, for one, recently launched a Consent Based Social Security Number Verification (eCBSV) service that’s meant to cut down on identity fraud for new customer accounts.

There’s also the proposed National Biometric Information Privacy Act, which could require companies to safeguard customer biometric identifiers (such as thumbprint or retinal scans) as they currently do for Social Security numbers, with substantial penalties for breaches due to inadequate safeguards.

Greater data protection obligations. Congress could also enact the equivalent of the European Union's General Data Protection Regulation. The Data Protection Act of 2021, introduced in the Senate, creates a federal-level data protection agency that would levy fines against companies that don't adequately protect consumer data. The Department of Justice also recently launched a Civil Cyber-Fraud Initiative to enforce cybersecurity compliance more strictly — particularly reporting requirements — in federal contracts and grants by invoking the False Claims Act's civil fraud and whistleblower provisions.

The Department of Justice recently launched a Civil Cyber-Fraud Initiative to enforce cybersecurity compliance more strictly.

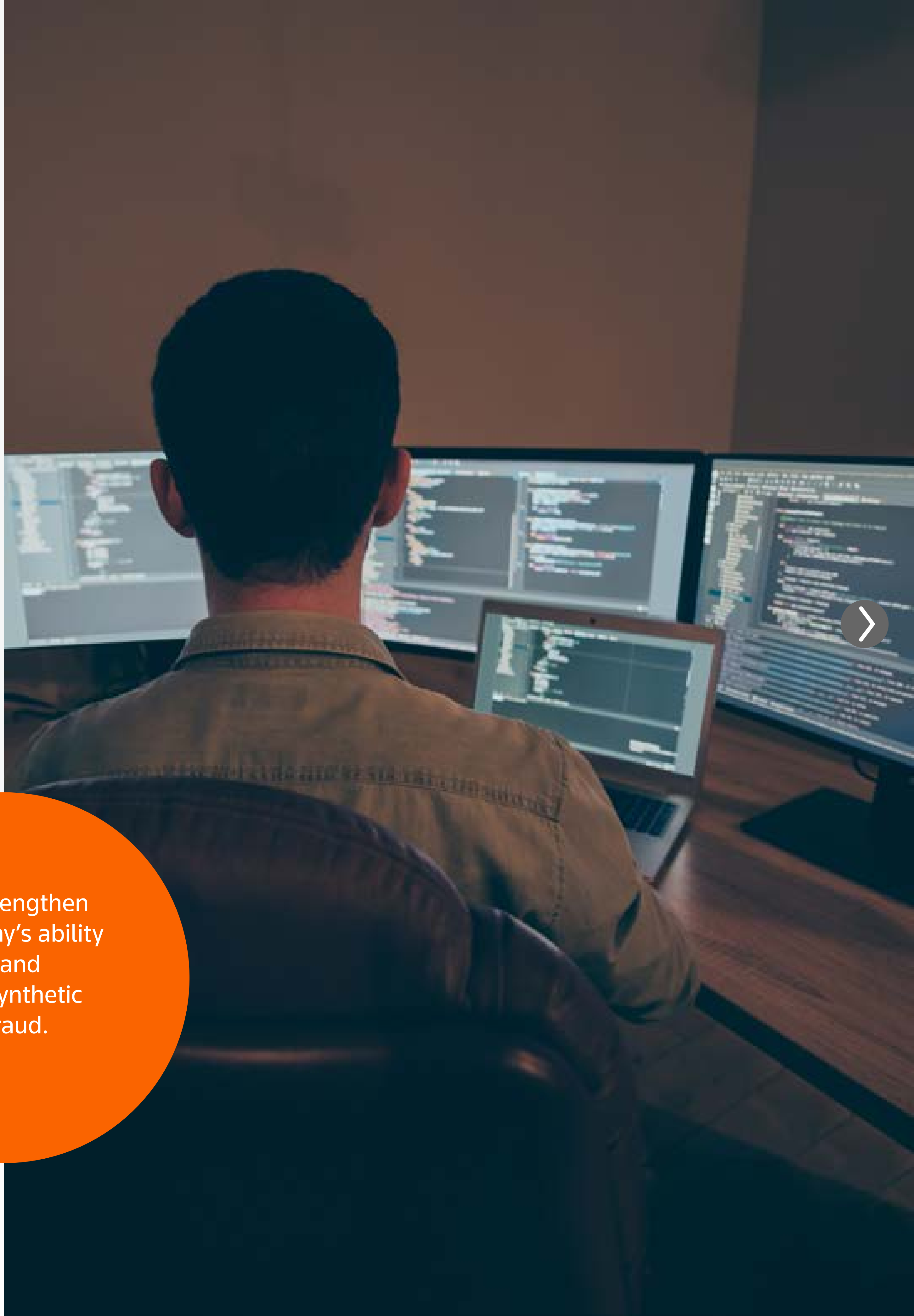
AI as next-generation weapon

The prospect of more government-mandated compliance is a compelling incentive for financial companies to make AI central to their fraud protection strategy. For some risk managers, AI is now nothing less "than the future of fraud management, irrespective of the system you are using," said Svetlana Belyalova, head of operational risk management at Rosbank, Societe Generale Group, in an early 2021 webinar.

For example, AI can strengthen a company's ability to detect and prevent synthetic identity fraud. In the latter, fraudsters typically will purchase a set of stolen identities and then mix and match them to forge a new identity. Thus, a fraudulent synthetic ID could be composed of one person's Social Security number, another's date of birth, another's home address, and so on. Estimates in 2020 found that synthetic identity fraud already had cost U.S. lenders nearly $6 billion; that volume certainly increased in 2021.

Automated technology, powered by advanced artificial intelligence and machine learning, can combat synthetic ID fraud, in part by streamlining and giving better protections to a company's Know Your Customer (KYC) /Anti-Money Laundering (AML) processes.

AI can strengthen a company's ability to detect and prevent synthetic identity fraud.



Among the benefits that AI offers include:

- **Better, faster data collection and analysis**. AI authenticates identities by drawing upon a wide range of sources, such as credit bureaus, government license bureaus, sanctions lists, law enforcement records, phone records, DMV information, court records, and business data. AI systems can then swiftly flag any contradictory information, such as conflicting data sources for a particular ID.
- **More accurate, time-sensitive risk assessments**. Along with being reactive and searching for potential identity fraud, AI-driven behavioral models are also predictive as to when and how fraudsters may strike.
- **Mapping fraudsters' historical behavior**. Considering the latest warnings from law enforcement and government, such models can determine where a firm should focus its efforts at any given time — for instance, geographically. Via AI, a firm will receive real-time risk assessments to determine if, for example, a suspicious one-off transaction is more likely to have been an error or if it's seemingly part of a broader fraud effort.
- **Enabling customers to create stronger digital identities**. A critical piece of the anti-fraud puzzle is for customers to have easy-to-create and fully secure digital identities. Here, the use of application programming interfaces (APIs) automates this process, enabling customers to create a secure digital identity that financial institutions can verify instantly upon being established.
- **Improving the quality of audits**. Third-party auditors determine if a financial institution has met regulatory requirements. Given the amount of potential new legislation in the works, they'll likely be even more of a presence going forward. Automating the digital identity creation process doubles as a heightened audit protection: it creates a real-time accounting of client onboarding, with all data stored in a central, secure location.

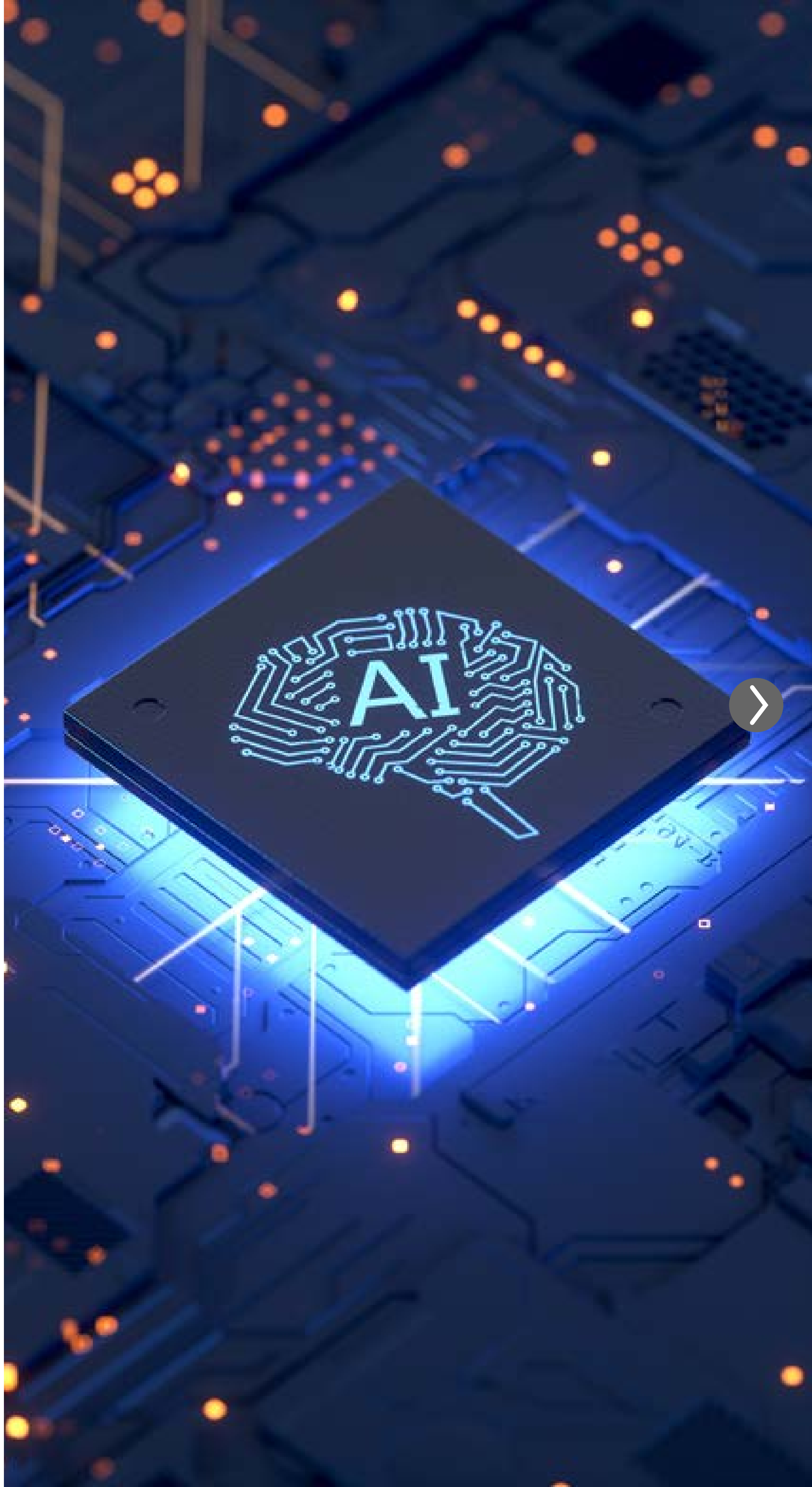
(continued on next page)

Among the benefits that AI offers include: (continued)

- **Strengthening biometric authentication**. Customer IDs are increasingly becoming biometric, whether it's a thumbprint scan to unlock a phone or a voice authentication test before being able to remotely access one's account. AI systems will be critical to keeping these processes safe and accurate. Firms may soon be required to adhere to more frameworks established by governing bodies, such as the Federal Financial Institutions Examination Council (FFIEC), which is reported to be considering stronger guidance on biometric authentication.

In voice biometrics, an automated system could require a user to say a randomly-generated phrase, drawing upon pre-established analyses of a customer's voice — its tone, its phrasing, and potentially accent, for example — to verify the customer's identity.

While this is a strong weapon against fraud, the system must have very accurate, up-to-date parameters as to a customer's voice patterns. Otherwise, a company will contend with irate customers being unable to access their accounts.



Challenges of AI

Implementing AI programs isn't the end of the story, by any means. Financial institutions need to ensure that all their AI applications fit well into their overall fraud prevention strategy. Without proper training and education as to how the systems work, the complexity of AI models may seem impenetrable to a company's risk prevention staff.

Another issue is that companies will need to establish parameters for the use of data in AI systems. AI uses vast amounts of data to power its algorithms. To make these processes more effective, it's important that a firm has strong protocols for standardizing, classifying (such as assigning data as structural, client or book data, among other categories) and, most importantly, verifying data, regularly pruning databases to eliminate duplications or inaccuracies.

The concept of "garbage in, garbage out," in terms of how poor-quality data affects predictive tools, is far from being obsolete.

(continued on next page)

Challenges of AI (continued)

Further, a company needs to ensure that it's legally able to access and exploit any data, particularly if such data has been derived from third parties. The EU's General Data Protection Act, for example, has strict parameters as to data usage. It's likely that any U.S. equivalent will have beefed-up protections as to how client data can be used by private companies.

One way to contend with data usage prohibitions is to have systems work on an aggregated level — searching for common behavioral patterns from, for example, clients making online payments or establishing digital IDs. Systems may use "metadata" — components of data inputted into various strategic models.

There's also the concept of Federated Learning, a type of machine learning in which algorithms don't exchange data from individual servers but instead rely on decentralized datasets or data samples.

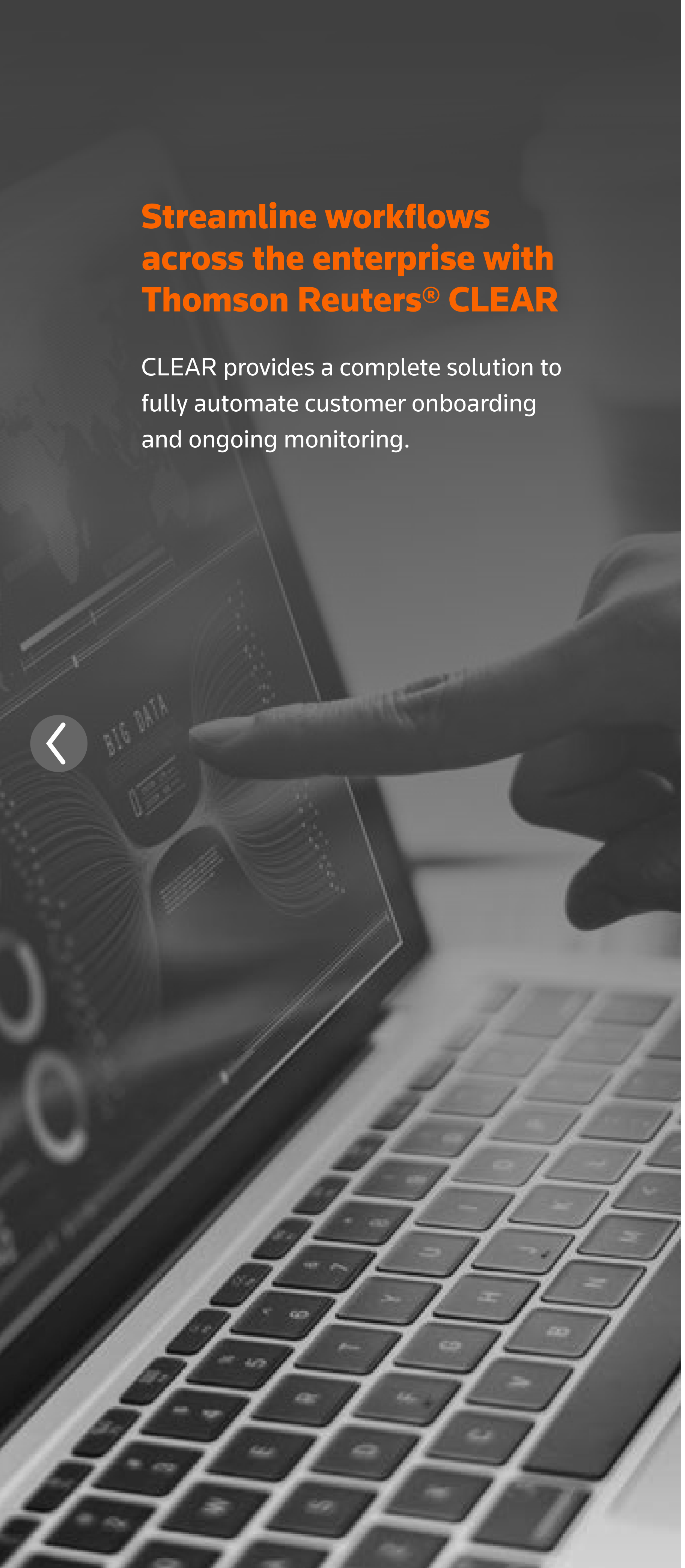
A continual evolution

There's no turning back from the digital finance boom of the past few years. An already-rising trend was given critical mass during the COVID era. Banking via phone or laptop, the growing use of biometric IDs, the ever-important need for database security — all of this will only progress throughout the decade. And this means that digital fraud is also going to be here to stay.

This rising digital financial fraud wave has one benefit — it can improve the accuracy of AI fraud models by giving them greater and more frequent sets of inputs.

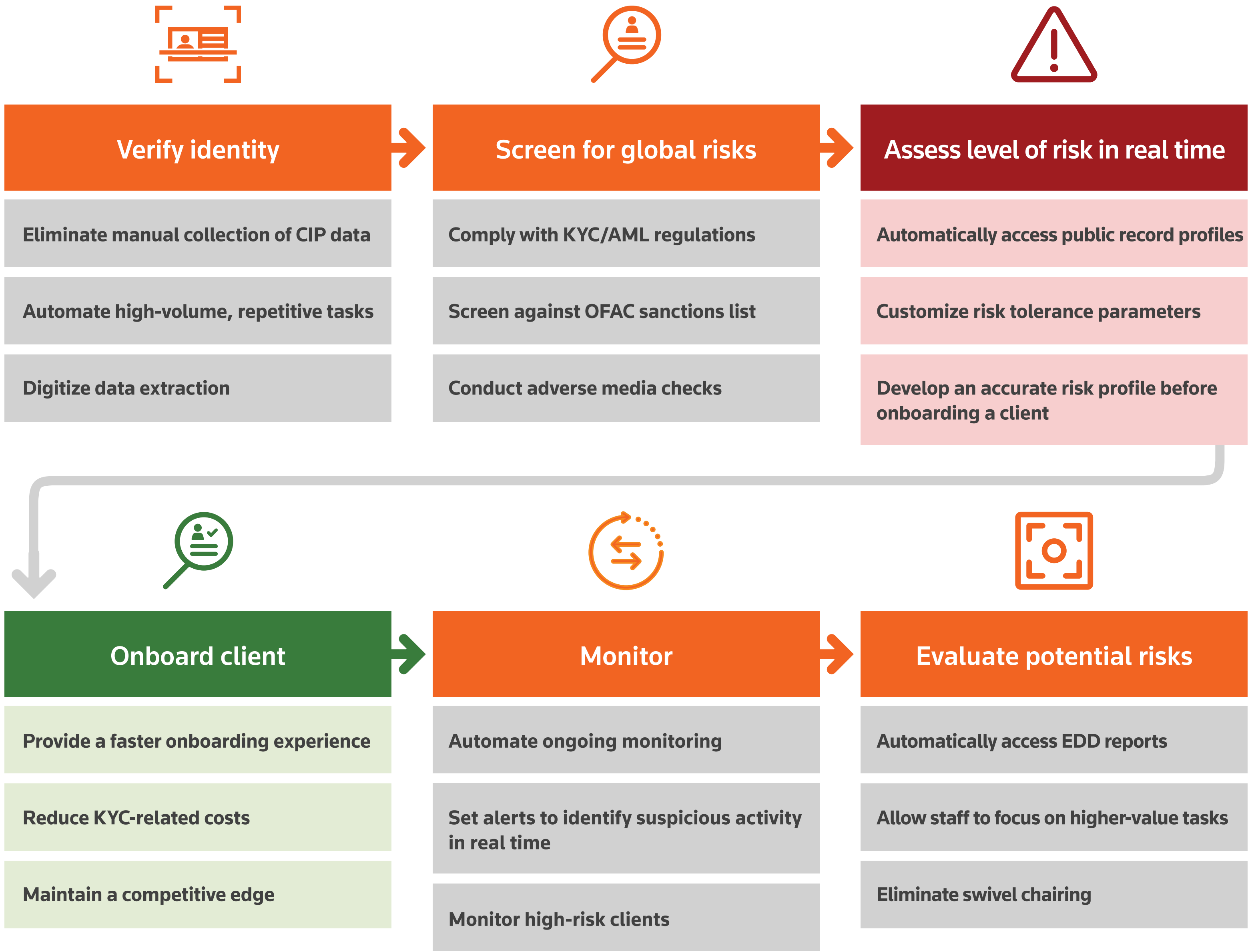
In the ongoing struggle between fraudsters and risk managers, companies need to be as strong and as nimble as possible.

Companies need to be as strong and as nimble as possible.



Streamline workflows across the enterprise with Thomson Reuters® CLEAR

CLEAR provides a complete solution to fully automate customer onboarding and ongoing monitoring.



Verify identity

- Eliminate manual collection of CIP data
- Automate high-volume, repetitive tasks
- Digitize data extraction

Screen for global risks

- Comply with KYC/AML regulations
- Screen against OFAC sanctions list
- Conduct adverse media checks

Assess level of risk in real time

- Automatically access public record profiles
- Customize risk tolerance parameters
- Develop an accurate risk profile before onboarding a client

Onboard client

- Provide a faster onboarding experience
- Reduce KYC-related costs
- Maintain a competitive edge

Monitor

- Automate ongoing monitoring
- Set alerts to identify suspicious activity in real time
- Monitor high-risk clients

Evaluate potential risks

- Automatically access EDD reports
- Allow staff to focus on higher-value tasks
- Eliminate swivel chairing

Thomson Reuters CLEAR includes:

CLEAR EDD
CLEAR ID Confirm
CLEAR Risk Inform
CLEAR Adverse Media

Thomson Reuters is not a consumer reporting agency and none of its services or the data contained therein constitute a 'consumer report' as such term is defined in the Federal Fair Credit Reporting Act (FCRA), 15 U.S.C. sec. 1681 et seq. The data provided to you may not be used as a factor in consumer debt collection decisioning, establishing a consumer's eligibility for credit, insurance, employment, government benefits, or housing, or for any other purpose authorized under the FCRA. By accessing one of our services, you agree not to use the service or data for any purpose authorized under the FCRA or in relation to taking an adverse action relating to a consumer application.

legal.thomsonreuters.com/en/c/clear-investigation-solution

THOMSON REUTERS®