FRAUD DETECTION AND PREVENTION

HOW IT CAN WORK **AND WHY YOU NEED** TO CONSIDER IT

A GUIDE TO FRAUD-DETECTION SOLUTIONS AND BEST PRACTICES

EQUIFAX®

By now, most organizations know they need some form of fraud detection to help protect themselves and their customers from fraudulent activity during and after account opening.

While your business may have many security options to choose from, knowing the best way to combat fraud can be complicated. Generally, to select an effective approach, your organization needs to first understand the threats it faces and then balance security without sacrificing customer experience.

Unnecessary or overly stringent controls can put you at a competitive disadvantage or, worse, could drive away customers, leading to lost business. However, if controls are not tough enough, you could incur large operational losses from fraud.

This best-practices guide explores the most common identity fraud threats and several effective, customer-friendly ways to combat them.

UNDERSTANDING THE THREATS

Organizations typically deal with two main types of identity threats:

- New account fraud, which occurs when fraudsters use a stolen or synthetic identity to open a new account and engage in fraudulent activity
- Account takeover fraud, which happens when fraudsters use identity theft to pose as someone else to access existing funds, lines of credit, or other resources

Those committing fraud use various entry points and tactics to establish accounts or assume identities for their crimes. Some of the most common include:

Online or mobile applications. Using online or mobile interfaces, fraudsters attempt to open new accounts or take over existing accounts. They may use records of information gathered about a person to successfully answer common security questions, such as an applicant's parent's birthplace or the name of a pet. When opening new accounts, they may use another person's Social Security number or account number to gain unauthorized access to a new account or line of credit.

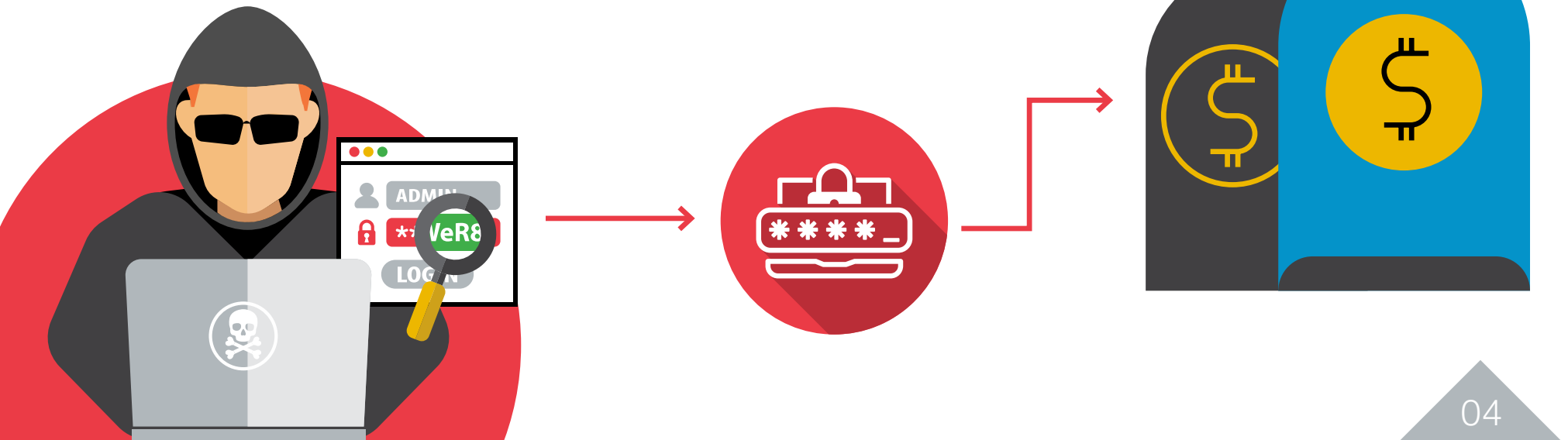
Contact centers. Contact centers tend to be a popular target for fraud perpetrators because they attempt to "trick" employees into revealing information or believing that the fraudster is the person he or she is claiming to be. Contact-center employees are generally focused on providing good customer service and may not be trained to identify a fraudulent caller. In addition, fraudsters may initiate a distributed denial of service attack against the organization's website, driving more call volume to the contact center, thus increasing the likelihood that a fraudulent interaction will go unnoticed.

"Bust outs." This can be a long-term tactic whereby a fraudster opens an account, perhaps even in his or her own name. He or she uses the account responsibly to build up access to greater lines of credit. Then, the fraudster either takes out a large cash advance or makes significant charges on the line of credit and never pays back the account.

Fraud rings. In this scenario, fraud perpetrators gather groups of people to carry out a coordinated fraud — either by allowing their real identities to be used to open accounts or by working together to create synthetic identities. Many gangs are now running fraud rings.

Fraudsters have various methods of committing their crimes and are getting more sophisticated as information resources, technology and tactics evolve. Understanding these common threats is the first step to preventing them.

Clearly, fraudsters have various methods of committing their crimes and are getting more sophisticated as information resources, technology and tactics evolve. Understanding these common threats is the first step to preventing them.



FINDING THE RIGHT FRAUD-PREVENTION SOLUTIONS

As organizations work to find solutions to help prevent fraud losses, they also face unprecedented consumer demand for technology-driven interfaces and convenience. Stringent identity verification may cost business — something no business wants.

However, just as fraud perpetrators are evolving, so are fraud-detection solutions. Organizations are using these and other methods, both internally and in conjunction with third parties, to help stop a wide variety of fraud types and tactics with as little inconvenience to the customer as possible.

Detecting fraud schemes based on synthetic or made-up identities means knowing what a real customer looks like. Your business can use high-quality, diverse data — including personally identifiable information and financial information, as well as sources such as residence, employment and utilities information — with smart analytics to help quickly separate a legitimate customer from a fraud. You must first start with good data. Primary ways you can help to boost data quality include:

Sharing fraud data. Some industries, such as financial institutions, contribute valuable information about potential fraud, collections risks, and even cyber threats to central repositories. These repositories can capture petabytes of data from consortium members and make the information available to authorized parties. Data from just one company or division will have blind spots, but the power of a network of fraud-detection information can mean that

Detecting fraud schemes based on synthetic or made-up identities means knowing what a real customer looks like.

fraudsters might not easily move their scam from one company to the next. Another benefit of sharing data in exchanges is that it might help give a window into what's new in fraud techniques, tactics and patterns. This preventive and detective system may help organizations act proactively instead of reactively.

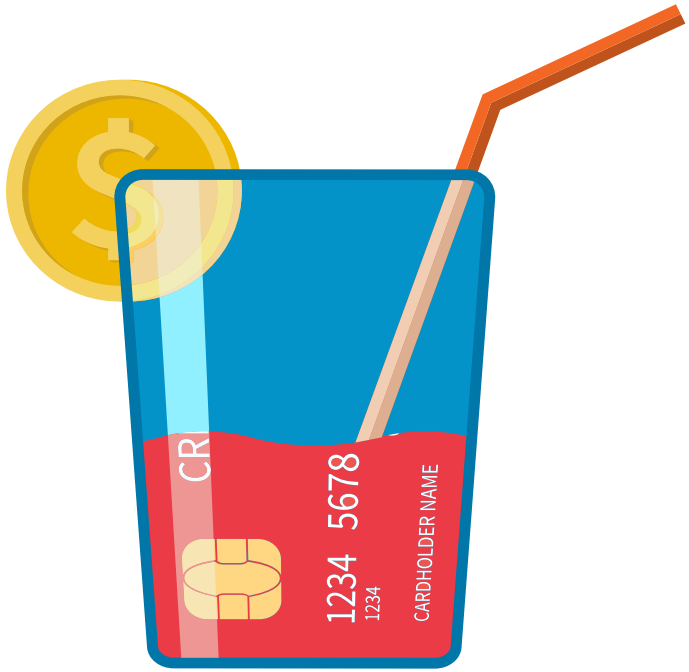
Reviewing data for patterns and developing analytics to anticipate those patterns can be very helpful. Examining patterns or commonalities in actual or attempted fraudulent activity helps show where such issues could be prevented in the future.

Building on data with good analytics.

Reviewing data for patterns and developing analytics to anticipate those patterns can be very helpful. Examining patterns or commonalities in actual or attempted fraudulent activity helps show where such issues could be prevented in the future. Your business also should examine existing cases of fraud and ask important questions to help prevent future attempts. For example, what information could we have required to detect that a transaction was fraudulent? What signs could have triggered an escalation in authentication? What clues, such as atypical customer behavior or access from a new location, did the fraudster leave behind that could help improve security practices in the future? By examining fraud attempts and fraudulent transaction patterns, you can continue to develop systems and security measures that aid in protecting your organization and your customers from future fraud.

Analyzing customer behavior.

Comparing individual and typical behavior patterns can also lead to fraud indicators. For example, if a small-business account holder typically accesses an account from the office between 8 a.m. and 6 p.m., an attempted access at midnight from an overseas computer could indicate an unauthorized attempt. Of course, it could also mean



that the owner is overseas on vacation and needed to pay a bill or transfer funds, but that type of atypical behavior is a good reason to escalate authentication to perhaps prevent unauthorized account access.

By viewing data such as accelerated spending or unusual patterns in credit acquisition, you may be able to see if the change is an anomaly, an indicator of identity assumption or identity theft, or simply an isolated incident. For instance, if an identity receives credit inquiries from more than a dozen companies in less than a minute, that would likely indicate fraudulent activity. Likewise, multiple credit card transactions from different locations in a short timeframe would be considered another red flag.

Learning from future behavior. The schemes that fraudsters run are always changing. Being able to update screening mechanisms and incorporate new antifraud tools as needed is essential for staying on top of fraud. Incorporating tools such as machine-learning models can greatly shorten the time needed to update the model when facts on the ground change. This leads to less money and time spent on maintaining the fraud-catching efficiency of the model.

COMPLETE THE SOLUTION WITH THE RIGHT TECHNOLOGY

In addition to implementing practices that may help boost data quality, your organization must also embrace technology solutions to help mitigate fraud. By using a variety of tactics and tools, it's possible to verify low-risk transactions and prospects with minimal inconvenience, while flagging potentially risky situations for escalated means of verification. Verification tiers include:

Passive insights. Passive methods of verification generally just require customers to enter standard information about themselves, such as name, address, telephone number, email address, birth date, Social Security number or other information. Your organization then works with a third-party verification service to ensure that the individual is, in fact, a real person and not an alias or made-up identity. Passive checks can include looking at the velocity or frequency at which the consumer-identity elements are seen, either alone or in various combinations. High velocity may indicate a fraudster using a stolen identity or trying to open an account with a synthetic identity.

In some cases, such as when the customer is applying for credit, you may run a credit check to be sure the individual qualifies for the service for which he or she is applying. This is one of the most basic forms of defense but can also signal red flags, such as when addresses or other data don't match the individual's profile through the verification service. Such cases may mean that the account needs further verification.

Device authentication. Typically, users who access their accounts online or through mobile interfaces do so using the same device each time, whether it's a computer, smartphone or tablet. Organizations may use "cookies" installed on the device to determine that the individual is logging in from the same devices or applications.

Passive checks can include looking at the velocity or frequency at which the consumer-identity elements are seen, either alone or in various combinations.

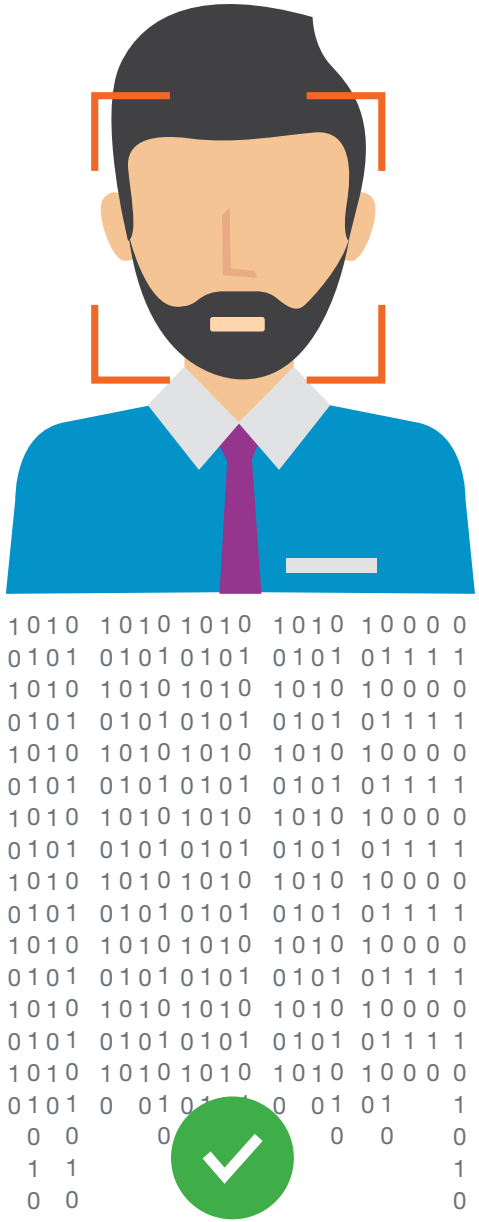
Your organization may also note internet protocol (IP) addresses. If the individual is logging in from a recognized device and IP address, the likelihood that the access is fraudulent is less than if an attempt is being made from an unrecognized device. Additional information about the device, such as anomalies in characteristics of the device, associations with other devices, or confirmation that the device has previously been used for fraudulent activity, may indicate that additional authentication is needed.

Risk-based user flows.

This anti-fraud tactic allows your business to apply progressive authentication strategies, escalating only when necessary, to help minimize customer friction. For example, if passive insights show that the information given matches the customer's, then you may allow certain lower-risk activities without further authentication steps. For higher-risk activities or when first-defense measures give negative results, further authentication may be necessary. Examples include when a device used to log in has a history of fraudulent behavior or is located in an area different from the individual's home or work.

Facial matching.

Facial matching is one of the most secure authentication methods available today. It's truly unique and easily accessible to the individual. With the prevalence of smartphones, this technology is becoming more widespread, as it's easy to have a consumer take a "selfie" and then match the picture against a digitally stored image that draws upon the unique characteristics of the human face. When this is combined with a comparison against officially issued documentation, such as a driver's license or passport, counterfeiting becomes more difficult for the fraudster.



One-time passcodes.

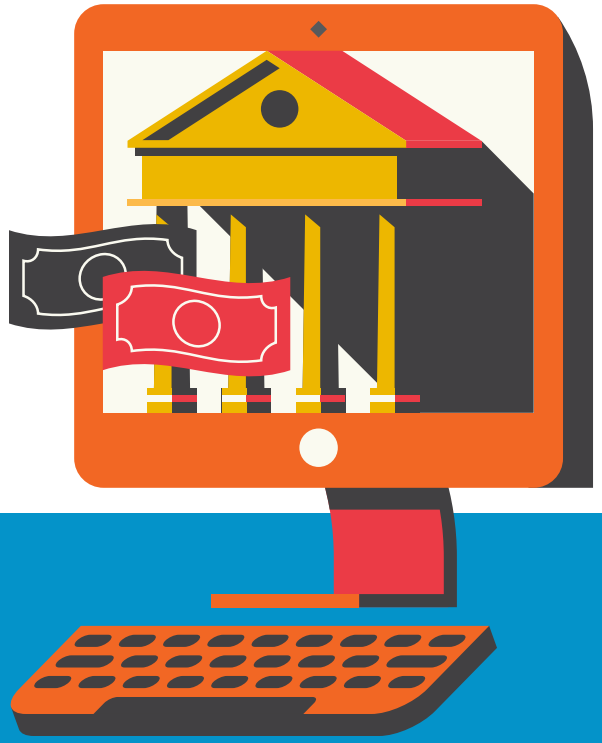
This is a way for your business to further secure at the transactional level. It entails sending a single-use passcode that expires within a few minutes over a separate communication channel — usually a mobile phone (via SMS, email or voice) — to the end user before the transaction can be completed. This is generally a more secure authentication method since it involves a separate communication outside of your organization's application channel (usually the web channel). Multiple channels for authentication make committing fraud more difficult due to the multiple safeguards that are in play. It's a good idea to verify the phone an account holder adds before sending a security code to help prevent fraudulent changes in contact information aimed at gaining account access.

Knowledge-based authentication (KBA) questions.

This process authenticates an applicant's identity by presenting multiple-choice questions to the applicant that should only be known by that actual person. Equifax has patented the KBA process, which binds the applicant to the identity information entered and then leverages a statistical model that provides a fraud index score as part of the overall assessment.

Contact center verification.

Contact center interactions provide unique challenges, because it can be difficult to verify identity and thus prevent fraud by voice only. Using basic data gathering — such as verifying name, address, and account or other identifying numbers — is a start. Integrating other methods of technology can help, too. For example, the contact-center employee may send a link to the individual via email or text directing him or her to log in to his or her account to verify the transaction. In such cases, device authentication may be possible when the customer or applicant logs in to access the account.



SOLUTIONS LEAD TO BETTER RESULTS

As fraud evolves, so must prevention strategies. Examining organizational threats and developing appropriate solutions that allow customers a great measure of convenience is a critical philosophy that will help your organization remain competitive. This includes using modeling to predict areas where fraud is likely to occur and to take action to help reduce opportunities for fraudsters.

The approaches need to be multifaceted. Investing in identification technology, training employees to verify identity and recognize clues that they may be dealing with fraudsters, and ensuring that legacy systems are kept up to date are all important measures. Companies such as Equifax offer comprehensive identity verification and fraud-detection solutions, plus advanced keying and linking technology. This enables the connection of disparate data systems and helps reveal gaps in information within your call center, online channel and billing programs to help prevent losses related to application or account-opening fraud.

Contact Equifax today to learn how our analytical solutions integrated with deep, rich business insights can benefit your company. Call 877-262-5261 or visit equifax.com/business/prevent-fraud