Protect the customer experience

The impact of fraud on your customer relationship

An Experian Perspective

Fraud. It continues to grow and evolve, affecting consumers, businesses and agencies alike.

In 2015, identity theft affected more than 13 million U.S. consumers which amounts to $15 billion in losses.[1] As technologies evolve and information security tightens, the savvy nature of fraudsters becomes more sophisticated. They are continually striving to be one step ahead of the next fraud-prevention strategy. As consumers move from face-to-face interaction to online and mobile transactions, there is a pressing need for more elaborate and accurate fraud prevention.

Many trends are impacting how businesses and agencies assess fraud:

- **EMV (or "chip- enabled" cards) —** The combination of a "chip and pin" system in credit and debit cards launched in October of 2015 to help prevent counterfeit cards and losses associated with fraud at the point of sale (POS). Businesses and agencies have seen a shift and increase in card-not-present (CNP), identity takeover and true-name or synthetic-identity fraud as a result.
- **Online expansion/Omnichannel interaction —** Mobile commerce has grown more than 60 percent from 2014.[2] As consumers take advantage of organizations offering more products and services online, the potential for fraudulent risk will rise. Customers are now interacting with the same organization in a growing number of ways. Thirty-six percent of organizations interact with their customer in five or more channels.[3] As more transactions take place in an omnichannel environment, the need for more strategic and covert fraud management is needed.
- **Data breach —** With the increase in reported data breaches comes an increased hesitancy from consumers to share their personal information. Also, as more and more personally identifiable information (PII) is compromised, it becomes less valuable for businesses and agencies to use as a singular or isolated means of authenticating consumers. While important in compliance-oriented identity checking, elements such as name, address, phone, date of birth, and Social Security Number (SSN) alone are no longer sufficient for risk-based authentication and assessment.
- **Expanded services —** Numerous additional services are now offered where personal or financial information is exchanged online or via mobile applications, such as remote deposits and person-to-person (P2P) payments. This allows tasks and transactions to be conducted online but exposes businesses and agencies to new fraud risks. As mobile transactions continue to grow, so too will the number of available online services making this channel a fertile breeding ground for fraudsters.

In 2015, **identity theft** affected more than 13 million U.S. consumers which amounts to **$15 billion in losses**.[1]

- **Regulatory compliance —** Many fraud compliance requirements are changing the way organizations do business. Consumers are wary of providing PII because of the risk of compromising these credentials. And lenders are tasked with diligently verifying and authenticating the consumer with limited data. Whether it is the Federal Trade Commission's Red Flags Rule requirements, USA PATRIOT Act checks, Consumer Financial Protection Bureau (CFPB) mandates, National Institute of Standards and Technology (NIST) levels of assurance in authentication or a myriad of other guidelines and rules, there exists a tension between meeting such requirements and minimizing reliance on PII.

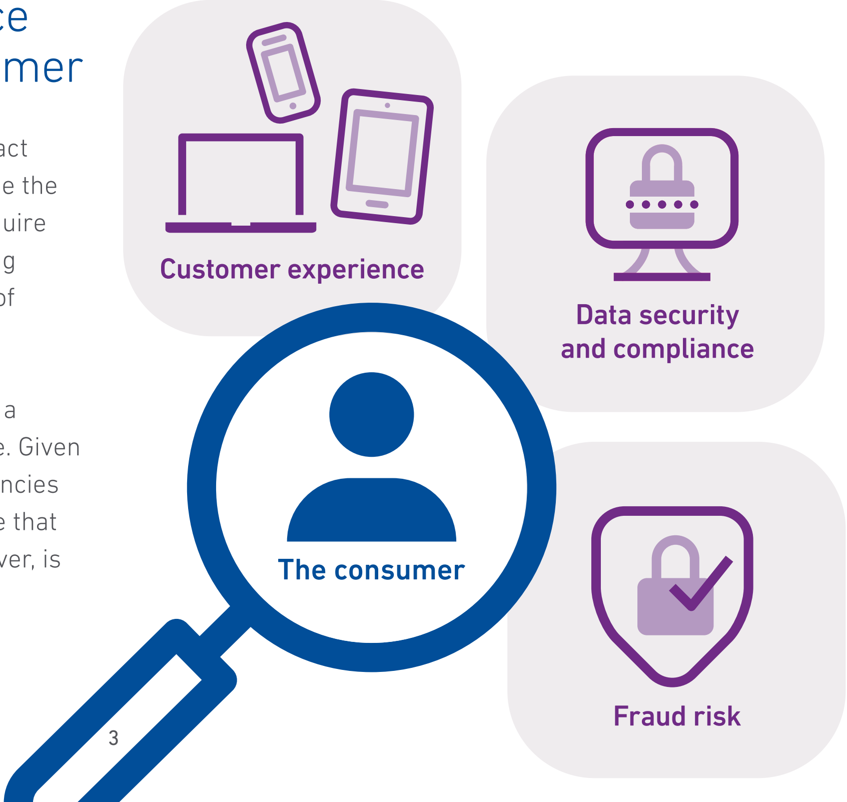
Fraud risk has been and will continue to be a primary issue for businesses and agencies as they strive to be stewards of customer identity and behavioural data associated with customer accounts and interactions. The more significant issue is the impact fraud can have on the customer relationship. Although the monetary cost of fraud losses can be high, the impact a loss or breach can have on customer relationships and brand integrity can be even higher. Customers like fraud protection. But they love convenience. The key to an effective fraud-authentication strategy is striking the perfect yet dynamic balance between accurately identifying and segmenting likely fraudulent customers and activities and seamlessly enabling the vast majority of legitimate customer transactions.

[1] Javelin 2016 report.
[2] Study conducted by Experian Decision Analytics. [2] Study conducted by Experian Decision Analytics.
[3] Experian Marketing Services.

More than 85% of consumers are using online and/or mobile channels to conduct business.

The authentication balance with a focus on the consumer

Online and mobile growth has created a fast-paced world. Consumers are looking to interact with companies and agencies that can provide the products/offerings/services they want or require with the ease of a few clicks while maintaining security and integrity. More than 85 percent of consumers are using online and/or mobile channels to conduct business. And, it is not uncommon for today's consumer to abandon a transaction if the process is too cumbersome. Given this need for immediacy, businesses and agencies are tasked with creating an online experience that is secure yet easy to navigate. The key, however, is assuring a positive customer experience!



The “old world” of authenticating a consumer’s identity primarily relied on checking personal information — such as name, address and SSN — and returning binary flags to indicate discrepancies. Simply using a binary approach resulted in false positives that had to be reviewed manually, which often included a request to the customer to provide more information to verify identity. In today’s world, any delay in the process will likely result in the loss of a customer thus a loss in revenue and/or the inability to deliver necessary services quickly and effectively. Having a covert, behind-the-scenes, automated and tiered approach that provides a panoramic view of the customer is essential.

Benefiting from a panoramic view of your customer

Keeping data security/compliance, fraud risk and customer experience at the center of the authentication balance calls for a need to integrate multiple authentication tools in a layered and risk-based approach to deliver a panoramic view of the customer throughout his or her life cycle. A panoramic view includes the data provided by the consumer, data from established third-party organizations, and uses advanced analytics and decisioning to validate, verify and authenticate a consumer comprehensively. A panoramic view evaluates the customer from all points of contact and is an ongoing process that evolves as more data is captured. Ideally, it is a process that is seamless, includes consortium data collected from like businesses and agencies, includes big timely and applicable to the consumer based on his or her risk level.

Data

- Data breadth, quality and recency.
- Consortium.
- Big Data.

Analytics

- Advanced analytics.
- Identity associations.

Decision

- Flexible and dynamic decisioning.
- Single platform and point of integration.
- Proportional service options.

A **panoramic view** includes the data provided by the consumer, data from established third-party organizations, and uses advanced analytics and decisioning to validate, verify and authenticate a consumer comprehensively.

Data

Data breadth quality and recency

Any fraud and risk-prevention strategy is only as good as the underlying data. In the case of accurately authenticating a consumer, the breadth, quality and recency of the data used for authentication and to predict fraud risk is critical. If underlying data does not have enough history, is inaccurate or has not been recently updated, it will create doubt in the consumer's mind about the reputation of the company or agency he or she is attempting to do business with. Data breadth, quality and recency is a critical component to authenticating a consumer; therefore, selecting companies and agencies with accurate data is key.

Consortium data

There are a variety of ways to leverage consortium data to provide a panoramic view of the consumer and help detect and capture fraud.

> Customers doing business with companies and agencies that have access to Big Data **significantly benefit** by knowing decisions are being made using a complete customer view.

Negative records

Reliable organizations contribute known and verified fraud records for use in exception checking for account opening and account management. Known and suspected fraud records also can include device-based attributes, such as device fingerprints, which can be used to identify any further activity using that device.

Identity attribute network

Our aggregation of identity transactions are updated in real time and via link analysis. The Identity Attribute Network derives attributes and scores related to up-to-the-moment identity activity to create a predictive measure of the current risk profile, enabling businesses and agencies to capture fraud in real time.

Consumer alert feedback

Consumers have the ability to respond to an alert with affirmation or denial that their account was used in some type of authentication process, enabling the consumer to be empowered when their PII is used.

Big Data

All industries are relying on the use of Big Data to better authenticate consumers. Big Data enhances the customer experience by providing the most robust and in-depth view of the customer through the volume of data (petabyte, terabyte, gigabyte), the velocity of the data (real time, near time, batch) and the variety of the data (structured, semistructured, unstructured).

Using Big Data allows decision makers to leverage new and emerging data assets to improve positive authentication rates, further segment true fraud risk and eliminate false positives and negatives. Integrating Big Data into the authentication process helps to maintain fast response times and system availability standards and relies more on levels of confidence versus binary pass or fail responses. Customers doing business with companies and agencies that have access to Big Data significantly benefit by knowing decisions are being made using a complete customer view.

Big Data can help you enhance the customer experience through the use of advanced analytics by providing the most robust and in-depth view of your customer through the **volume** of data, the **velocity** of the data and the **variety** of the data.

Analytics

Advanced analytics

Data is the key underlying element of any authentication process. How that data is analyzed and interpreted is what transforms the data into knowledge. When authenticating a consumer using a simple binary yes/no flag based on "matched" data, the decision maker is limited at best. These limitations often place additional burden on the consumer who is looking to make a purchase or open a new account. Oftentimes consumers are pushed into a manual review queue, required to provide additional information and asked to follow up to prove the legitimacy of the information. By synthesizing scores and attributes, consumers who would have fallen into the review process can be segmented better to determine true fraud-risk potential. Based on that consumer's actual fraud-risk propensity, specific treatments can be overlaid on the data to determine if additional information is needed. For example, an identity or device risk score can be used to determine if the consumer should be asked qualifying knowledge-based authentication questions to further assess identity risk. Because scores and additional analytics can be integrated seamlessly into the overall decision process, the consumer is able to move quickly through the process, whether on his or her mobile device or in person. This ease of doing business will not only provide a positive customer experience, but significantly cut down on the time and cost associated with manual reviews.

An analytics-driven fraud-detection and authentication system allows institutions to make customer relationship and transactional decisions based on a holistic view of a consumer's identity and predicted likelihood of associated identity risk, rather than a handful of rules or conditions in isolation. Many specific fraud rules are not "silver bullets" that ensure the detection of fraudulent activity. A risk-based system allows for an operationally efficient method of detection and reconciliation of high-risk conditions in tandem with identity-theft mitigation. The inherent value of risk-based authentication can be summarized as delivering a holistic assessment of a consumer and/or transaction with the end goal of applying the right authentication and decisioning treatment at the right time across the customer journey or life cycle.

17%
of consumers reported having an online transaction declined when device information was not available.

Identity attribute associations

Ongoing authentication can be derived from historical and real-time identity attribute associations, device intelligence and positive linkages with the consumer, as well as through knowledge-based authentication and alert responses. The linking of online transactions with offline data provides a holistic fraud-management process that allows organizations to authenticate and verify the identity of a person better. Historical data can be leveraged by aggregating online activity to provide greater confidence that a person is who they say they are when conducting online and mobile transactions. For example, if a U.S. consumer travels abroad and tries to use a credit card to buy a train ticket in Europe, they may be declined solely because it is not where they typically make purchases. In fact, 17 percent of consumers reported having an online transaction declined when device information was not available.[4] Overlaying credit card information with device information makes it possible to verify the computer or device for which a credit card is normally used. Consumer trust is higher because the business can authenticate the device with the credit card.

> **Flexibility is key**, as every customer and transaction is unique in risk profile.

Decision

Flexible and dynamic decisioning

In order to process, evaluate and assess properly the data and analytics provided by a consumer, an organization needs a system that allows for flexible and dynamic decisioning that meets the needs of all of its customers. It is also critical that the system allows for the creation of customized decision strategies based on the organization's risk tolerance and compliance rules. Once defined, the strategy can be tailored to the customer based on customer history and additional information, such as scores and advanced analytics, to authenticate the customer better. Flexibility is key, as every customer and transaction is unique in risk profile. Businesses and agencies want the ability to treat a customer individually. For example, if a consumer appears to be low risk, a business or agency would rather not put him or her through unnecessary verification steps and create a negative customer experience. Another consumer may look marginally risky, so there may be the need to put him or her through basic authentication checks. What is most important is not to set up additional, unnecessary steps that could increase customer friction and deter a good customer, resulting in revenue or service loss and additional costs to the business or agency. It's essential to have a flexible and dynamic system that monitors performance and provides the ability to adapt and optimize strategies over time.

[4] *Experian Decision Analytics.*

Single platform and point of integration

Another capability to consider when selecting a decisioning system is the ability to integrate a host of authentication services so that customers are able to interact with the business at a single point of contact. Again, having a seamless, timely and accurate authentication process is the key to providing a good customer experience. To achieve this, businesses and agencies need a decision platform that can integrate authentication inputs, including:

- ☑ **Scores**
- ☑ **Out-of-wallet questions**
- ☑ **Device intelligence**
- ☑ **Performance monitoring**
- ☑ **Any other element of the decision process**

A single platform that evolves and updates over time — continually adding new data elements, continually incorporating third-party data, and incorporating new data and services as they become available and proven — is essential.

A single point of integration allows agencies to minimize integration efforts and customer service processes to service better those customers who truly fall into a review category while allowing the customer to have a personalized experience.

Proportional service options

Not all transactions and customer interactions should be treated equally. Certain transactions are higher risk than others, and for that reason, each customer interaction should be treated relative to its risk potential. A lender, for example, may want to vary its authentication strategy based on life cycle (new customer versus existing customer), channel (in-store versus mobile) or the transaction type itself (funds transfer versus account view). For example, a consumer setting up a brand-new account may be required to undergo a few more layers of authentication than an existing customer who is making a deposit using an established password and visiting your Website from the device he or she usually uses with behaviors consistent with his or her normal visits. To tailor the customer experience and provide appropriate authentication strategies, a system is needed that can vary the treatment based on the service options that are selected.

Fraud is not a single event. The panoramic view of the customer requires end-to-end authentication from the initial customer interaction through all points across the Customer Life Cycle. A successful authentication strategy does not rely on a single point-in-time interaction with customers. Rather, it involves an ongoing authentication relationship that protects customer identities over time while mitigating fraud risk. Such a relationship requires that organizations use a layered approach and a multitude of authentication tools to provide a panoramic view to validate, verify and authenticate the customer seamlessly over time. By knowing the customer each time he or she visits (whether in person or via a mobile device), the customer is further recognized as an individual, and his or her trust in the company or agency increases. At the end of the day, customers want to be known by the companies or agencies they do business with but want to do so as easily as possible.

Fraud is **not a single event**.
The panoramic view of the customer requires end-to-end authentication from the initial customer interaction through all points across the Customer Life Cycle.

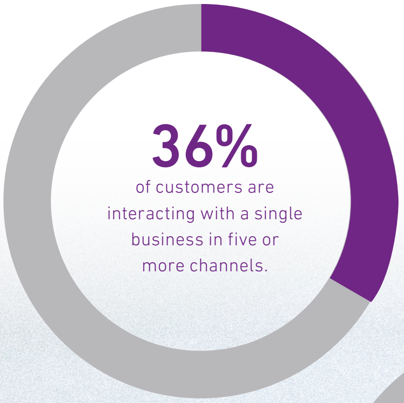
Evolution of fraud and the next frontier

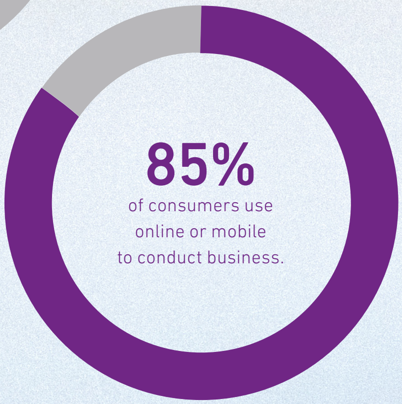
We have evaluated some of the “old” ways of authenticating a customer and provided new strategies to evaluate a consumer from a panoramic perspective by overlaying data, analytics and implementation strategies. However, as new technologies are developed and new ways of doing business are introduced, fraudsters are finding new approaches to perpetrate fraud. Fraud is constantly evolving, regulations continue to impose more constraints and consumers’ expectations are increasing along with the diversity of their interactions with various entities. Customer risk assessment and decisioning strategies will have to evolve at the same pace as customer-engagement changes, fraud schemes, and the emergence of viable authentication and fraud detection data and technologies.

> One of the most significant factors shaping the next frontier in fraud management is the **rapid growth in online and mobile commerce** as the preferred methods of doing business for many consumers.

Mobile and online access expansion

One of the most significant factors shaping the next frontier in fraud management is the rapid growth in online and mobile commerce as the preferred methods of doing business for many consumers. With more than a third of customers interacting with a single business in five or more channels[5] and more than 85 percent of consumers using online or mobile to conduct business,[6] the need for omnichannel fraud prevention becomes a requirement. These trends make mobile-device intelligence as important to the authentication process as traditional personally identifiable information. As a result, the need to integrate device intelligence into the authentication process to associate a consumer to a known device is critical. Companies already are beginning to incorporate device intelligence into their authentication strategies. The ability to verify a customer through his or her device is a huge benefit to the overall customer experience and not only makes it easier for the customer to do business with you, but also adds an additional layer of validation.





[5] *Experian Marketing Services study.*

[6] *Experian Decision Analytics.*

As data breaches become more prevalent, consumers are becoming wary of providing personal information.

Less personally identifiable information available

As data breaches become more prevalent, consumers are becoming wary of providing personal information, even to very reputable and secure businesses and agencies. At the same time, many consumers are moving to mobile devices to conduct business "on the go," which demands a quick and streamlined process that minimizes data entry, saving consumers time and effort. Because there likely will be significantly less PII present in transactions going forward, it is even more important for organizations to implement other nontraditional data sources and incorporate device intelligence into the authentication process. Consumers are more likely to do business with companies and agencies that ask little of them while still maintaining adequate levels of assurance and security.

Knowledge-based authentication expansion

Historically, knowledge-based authentication (or out-of-wallet questions) was based solely on information the consumer provided at account setup (often referred to as "secret questions"). Eventually these questions evolved to include more predictive and dynamic questions derived from third-party data sources and vendors. These questions would often be used in isolation or overused to the point where the questions would become less effective in accurately authenticating the consumer.

The primary goal in using knowledge-based authentication (KBA) is to have another means to assess risk beyond identity validation scores without compromising the customer experience. KBA provides organizations a tool to deliver layered authentication in a consistent and auditable process. This method uses structured questions that are tracked and linked to fraud risk as opposed to randomly selected or customer-created questions that may not be indicative of risk, particularly when cross-referenced with other risk attributes. These goals remain in place today. Significant evolution has occurred in how questions are used within an overall risk-based strategy. In isolation, the questions may not be as effective as they are when layered within a risk-based strategy that looks at a compilation of scores, attributes, consortium data, device and other authentication elements. It is the use of the various authentication tools together in a layered approach that enables out-of-wallet questions to be effective.

Significant evolution has occurred in how questions are used within an overall **risk-based strategy**.

Viability of alternative authentication methods

There are a variety of tools available for organizations to integrate into their authentication process. These tools not only enhance the customer experience and make it easier to do business, but help increase accuracy and reduce costs.

Context-based/Device authentication — As more consumers move to mobile/online transactions, organizations will begin to merge offline data, such as credit profile and in-house data, with online activity to provide a more complete picture of the consumer. Context-based authentication is ideal in that it is the most frictionless way to authenticate since it does not require additional effort on the consumer's part. It enables the business or agency to evaluate device elements, such as whether the device is operating under the appropriate time zone and browser settings on the phone or assessing transaction frequency to ensure an appropriate amount for the user. Context-based authentication is used as part of the risk-based authentication strategy so that an organization can vary the level of scrutiny based on the level of current transaction and access methodology risk cross-referenced with historic and/or contextual experience with that customer and similar interactions with other customers.

Biometric authentication — As the mobile/online space continues to grow, biometric authentication, using unique physical characteristics, will become more integrated into the authentication process. There already are biometric elements being used today, such as fingerprint authentication, but for the most part, biometrics has not widely been adopted across all markets. Voice verification is one option that likely will continue to see growth. This will allow call centers and consumers using mobile devices to use voice recognition to help authenticate a person calling in to conduct business. Fingerprint and handprint (and eventually iris) verifications are forms of biometrics that will potentially expand alongside the growing mobile space. The key to assessing potential in biometric adoption is ease of use and channel applicability. Those technologies that can support call center, online and mobile access channels are more likely to succeed.

Email and mobile phone verification — Email is frequently used to aid in verification, and its use is expected to grow in the future as direct customer interaction decreases with the movement toward online business. Today, an email address or mobile number is used as frequently as, if not more than, a Social Security number and is often considered to be an identity element. The email address also is used as a multifactor or out-of-band verification element. Consumers can use an email address to set up an account or make an account change prompting the company or agency to send an email confirmation or a text message asking the consumer to click on a link to verify a transaction or his or her identity. Additionally, the email address can be linked to the device on which the transaction took place to verify it is the device where the email address typically is used. We expect to see a further increase in multifactor verification using email, text and device in the future.

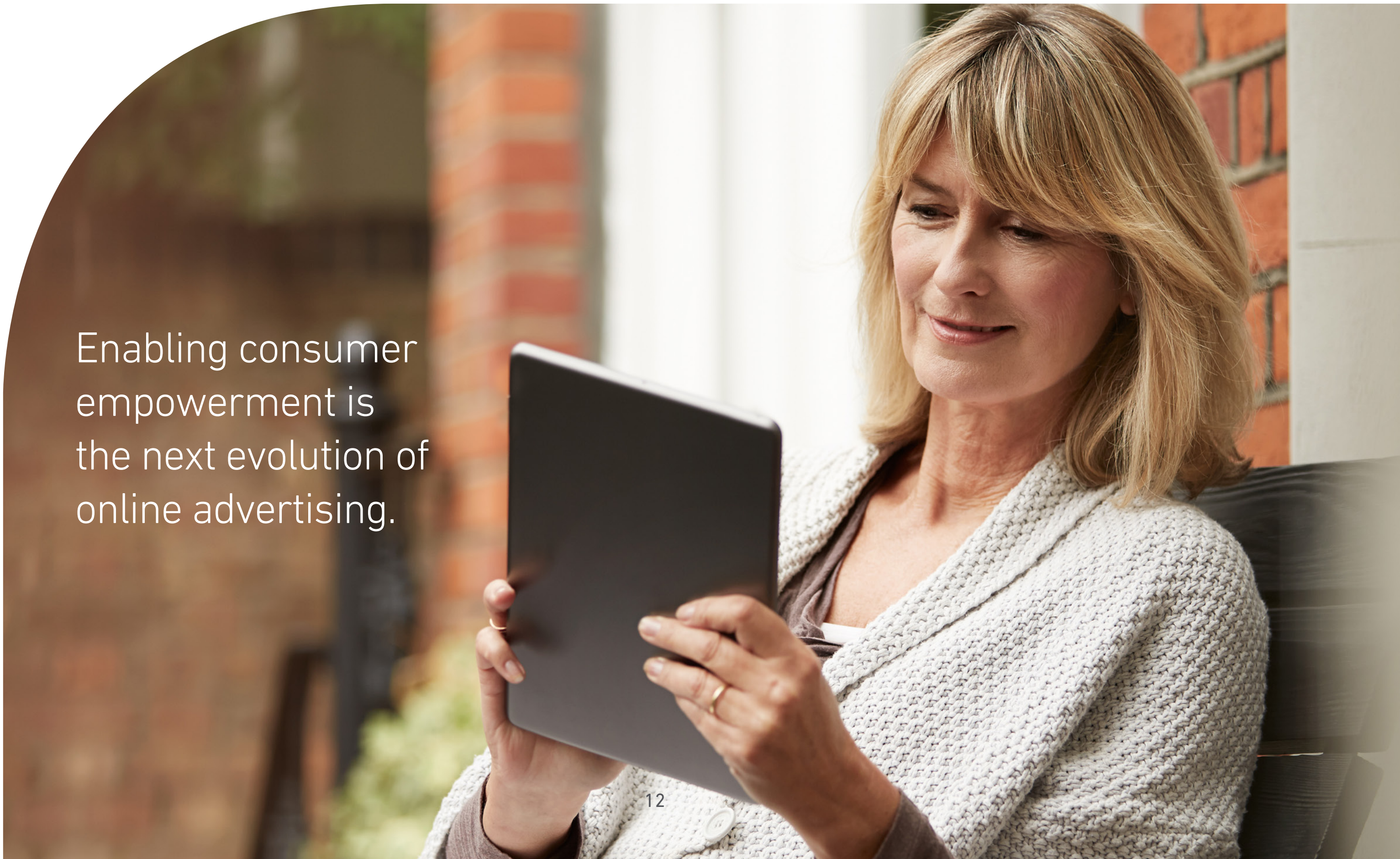
Consumer alerts — Traditionally, identity monitoring was used to monitor credit activity and alert a consumer if there had been a change to his or her credit profile. This has evolved now to alerting a consumer if his or her identity is deemed to be at risk of fraud or theft. Alerts may be centered on identity attribute changes or transactions (both monetary and nonmonetary). This transfer of power, where the consumer now is in control of knowing when his or her information is used in authentication, increases overall consumer confidence and also helps businesses and agencies to engage with the consumer by proactively reaching out in cases where potential fraudulent activity is taking place.

Identity as a service

We expect the trend to continue toward an ecosystem of shared and credentialed identities online across multiple organizations and applications, both private and public. A consumer will no longer have to manage multiple passwords and user names when logging in to various online and mobile applications. Identity as a service (IDaaS) represents the umbrella of activities and solutions supporting the identity relationship life cycle, such as password resets, attribute verification, identity proofing, multifactored authentication and credential management, biometrics, device intelligence and authentication, linkage analysis between identities and devices, and, ultimately, any activity or service providing a trusted identity relationship between a person, entity or thing. Moving in this direction will create a new level of authentication measures that ensures organizations are in sync with one another. IDaaS would make it significantly easier for consumers to manage access to identity information, resulting in a real "transfer of power" in favor of the consumer.

Identity as a service (IDaaS) represents:

- Password resets.
- Attribute verification.
- Identity proofing.
- Multifactored authentication and credential management.
- Biometrics.
- Device intelligence and authentication.
- Linkage analysis between identities and devices.
- Trusted identity relationships.



Enabling consumer empowerment is the next evolution of online advertising.

Conclusion

Fraud is evolving. And there are a number of factors contributing to this changing landscape. **First**, fraud schemes will continue to rise in sophistication and criminals will remain focused on how to "beat the system." This will place continuous pressure on businesses and agencies to adopt new approaches to manage fraud and protect information. **Secondly**, consumers will continue to expand their use of Web-enabled devices and mobile devices to conduct various forms of business, changing the types and amounts of information provided during the application process and transactions. **Lastly**, regulatory pressures around protecting and disclosing consumer information will continue to rise in breadth and depth.

All of these factors point to the need for organizations to evolve their authentication and fraud-management practices to include both offline and online fraud strategies that can deliver a panoramic view of the consumer and the customer relationship across the life cycle. To manage this holistic view of the consumer, the authentication process must shift from a single binary-fraud review to a layered, risk-based and contextual authentication approach that will include comprehensive, real-time updates of consumer information.

Big Data and advanced analytics, consumer alerting and multifactor authentication, device intelligence, biometrics, and the sharing of authenticated and credentialed identities across industries will become more commonplace. The ever-changing fraud environment, alongside data and technology evolution, will further drive organizations toward fewer but more robust and dynamic platforms through which to manage customer risk today and for years to come.

A panoramic view of the consumer will ensure data security and compliance as well as mitigate fraud risk. Ultimately, this shift in how businesses and agencies manage fraud and protect consumer identities will provide greater consumer confidence and create a more positive customer experience, which is the first, and most important, prong in the authentication balance. Consumers, businesses and agencies will feel confident in the authentication process by establishing an authentication program that is seamless and straightforward to the customer, while providing a holistic customer view to the business.

About Experian Fraud and Identity

Experian is a leader in identity and fraud solutions. We help our largest clients to detect and prevent fraud worth US $500 million each year, maximizing profitability while at the same time providing secure, hassle-free customer interactions. Every year, we check that 182 million people around the world are who they say they are, providing an effective, discreet identity solution that delivers streamlined customer experiences, every time. Our unique combination of unsurpassed data access, real-time analytics, cross-industry expertise and global perspective has us earned the trust of organizations and consumers from around the world.

Learn more

Experian
475 Anton Blvd.
Costa Mesa, CA 92626
T: 1 888 727 8330
www.experian.com