E-BOOK

The Rising Cost of Fraud

twilio

ABOUT THIS E-BOOK

Introduction

The pandemic has accelerated the shift from physical to digital, sharply increasing the scale and frequency of digital interactions. Whether it's distributed teams working remotely or customers engaging online, companies need to address the increased threat to account security and identity protection. It's critical that organizations adopt technology and policies that make it as simple as possible for customers to verify their identities with secure remote access.

Prior to the coronavirus outbreak, online fraud had already exploded from a minor nuisance to the single biggest headache facing businesses. From the creation of fraudulent bot-generated user accounts to costly takeovers of high-value customers to identity hijacking during the account recovery process, cybercriminals continue to exploit every gap in the security of online accounts. In this ebook, we'll look at how fraud is typically committed, what businesses are doing about it, and how identity verification can help stem losses caused by widespread fraud.

What's inside

CHAPTER 1

Online fraud—A colossal challenge

The surface area for fraud is so vast that no attack vector takes priority over others.

- **Data breaches,** once a rare news item, are increasing in scope and occurring more frequently. Meanwhile, data farmed from those breaches are used to open fraudulent accounts which, in turn, are used to commit identity fraud and exploit any value your business provides, like free credits or loyalty programs.

- **The takeover of existing accounts** is also fair game for fraudsters, especially when there is a monetary value that can be extracted. Even if there is no financial gain to be had, hacked accounts can be used to troll or spam other customer accounts, devaluing your business.

- **Attacks to both new and existing accounts** often happen via web-based or mobile apps, but these aren't the only customer channels exposed. A lack of investment in securing contact centers from fraud has made these a prime target as well. A contact center staffed with live agents is particularly vulnerable. While the contact center is supposed to increase customer satisfaction, introducing complex security steps often has the reverse effect.

Balancing fraud controls with customer experience is an ongoing challenge and can often lead to a loss in revenue. The more restrictive a signup, login, or contact center engagement is, the more frustrated customers become.

Fraud by the numbers

Fraud generated by automated bots remains a significant threat for nearly two-thirds of midsized to large e-commerce companies. And fraud costs, as a percentage of annual revenue, also are on the rise. Account takeovers can cost businesses as much as $15,000 per incident.

And customer support teams can spend **upwards of $50 per instance** helping customers regain access. Unchecked, these expenses grow linearly with your business.

Account takeovers can cost businesses as much as $15,000 per incident.

CHAPTER 2

Combating fraud with identity proofing

One of the most significant challenges to ensuring a viable customer-facing online business is 'identity proofing,' the process used to verify a subject's association with their real-world identity.

The challenges inherent in online account creation are more complex than in the physical world, where a utility bill paired with a passport or driver's license usually suffices. Verifying a government ID during an online signup is bound to slow down the typical user onboarding. To balance the business need for security and the user preference for convenience, you'll want to allow for quick user registrations with enough verification to reduce fraudulent account creation and filter out bad actors.

So how is identity proofing typically done?

Email: Simple but not always secure.
A vast majority of online accounts are identified by user email addresses. This practice gained a foothold in business early on since an email address is unique to an individual, customers rarely forget their own email address, and email was thought to be the best way to contact the account holder. However, it's almost impossible to determine if an email is fraudulent or not.

Biometrics: Newer, not necessarily better.

Biometrics promises trustworthy identity confirmation to correctly determine who is using a device by recognizing, storing, and comparing physical attributes—like fingerprints or iris scans. In practice, capturing and storing biometric data doesn't make it impervious to mass data breaches. Once a person loses control over their biometric data, it's not possible to change it like you would a password. In combination with other privacy issues, such as biometric data collection practices, storage, and cybercrime vulnerabilities, this has led to valid concerns and lawsuits regarding the use of biometric data in the secure verification and authentication of real people.

Multiple data points: Too much too soon?

Another method of verifying that a real person is behind your signup or password reset request is to ask for numerous pieces of personal information. Due to the inherent risks of doing business online, it is standard practice for many modern businesses—like financial services or insurance companies—to require social security numbers, government IDs, home addresses, and proof of previous work history. This step dramatically improves the chances that new account signups are from real people, but it also introduces user friction into the process. And while, according to Gartner, the friction of online documentation verification is less than it would be to do the same in person, it's not friction-free. It's also not suitable for every scenario. Providing this data to open a bank account makes sense, but might be overkill when signing up for a ride-sharing app.

CHAPTER 3

Answering the call against fraud—phone numbers

The unique attributes inherent to phone numbers make them a compelling option for the quick and efficient verification of a person's identity. You've probably already come across this practice in real-life.

Companies like Facebook, Google, Yahoo, Twitter, Microsoft, and Amazon are already incorporating phone numbers in their identity proofing processes.

Here's why:

- **Like email, phone numbers are easy to remember and hard to forget.** Unlike email, it's more difficult to fake a phone number, since they are harder to obtain and are typically unique to an individual. And while its reasonably simple to automatically generate thousands of email addresses to create bogus accounts, doing the same with phone numbers is more difficult, time-consuming, and expensive —all things cybercriminals look to avoid.

- **Phone numbers also reveal plenty of useful information that can be used to verify the authenticity of an account.** First, phone numbers are identified as either a landline, mobile, or Voice over Internet Protocol (VoIP). Second, phone numbers are associated with countries of origin. And third, phone numbers can be tied back to a telecommunications carrier. These three attributes help businesses filter out potentially-fraudulent traffic from specific geographies, while also identifying phone numbers associated with real devices owned by real people.

Signup and login screens for many websites often give the user the option to supply either an email address or phone number as the key identifier. In mobile apps, it's increasingly common to leverage the phone number as the only required information when installing and signing up. For example, the popular, US-based ride-sharing app Lyft requires only a phone number for all new accounts.

As companies grow globally, they'll come to find that some geographic regions lean more towards the use of phone numbers as primary identifiers. For example, South Korean consumers tend to be more willing to share a phone number than an email address. So, whether or not you're a business with a global footprint, employing phone numbers in identity proofing is a significant first step in fighting fraud.

Obtaining and using a phone number

The rise of robocalls and telemarketing has made consumers more wary of sharing their phone numbers than ever before. With that in mind, consider the following best practices around requesting, using, and evaluating phone numbers.

- **Ensure accuracy.** Get the full phone number, including the country code, and make sure the national formatting protocol is correct. This is important, as phone numbers are formatted differently worldwide. Acquiring this data typically happens at the time of account sign up. Users select their country and number entry is formatted accordingly.

- **Simplify for mobile.** On mobile platforms, where the device itself might have a phone number directly associated with it, data collection may be more straightforward. Android, for example, lets apps present all the phone numbers associated with the device. The user simply clicks on the number they want to use.

- **Verify validity.** Just as emails can be fraudulent so too can phone numbers. The most common method for confirming a working number belongs to the account holder is by sending a one-time code—usually a 4 to 6 digit token—via SMS and asking the recipient to enter that code back into the application. For the simple reason that this process is near impossible to automate, it's incredibly effective.

- **Consider alternatives.** Sending this SMS-based code—sometimes called an OTP, or one-time passcode—won't cover all of your users, as some have voice-only phone numbers like landlines or other restrictions that prevent SMS usage. So, be sure to offer the option of receiving a voice call or having the code read aloud over the phone. Additional methods, such as Push verifications or Time-based One-time Passcodes (TOTP) offer increased security for both a business and end-user. Again, verification happens when the recipient enters that unique code back into the application.

CHAPTER 4

Post-Signup—Ensure every door to fraud is shut

The challenges of fraud are not limited to the signup phase. Attacks to legitimate, existing accounts can cause significant havoc for large and small businesses alike. As an example, advances in combating credit card fraud have resulted in cybercriminals now focusing their efforts on taking over any online account that has a monetary value. Cryptocurrency sites are a popular target, but there has also been an increase in attacks against traditional banks, many of whom still use outdated online security protocols. Regardless of the industry, here are some top areas in which using a phone number to validate a legitimate user makes good security sense.

Fighting account takeovers

To a fraudster, exploiting an existing, validated account is a great deal more valuable than trying to create a dozen fake new ones. That's why we've witnessed a 182% jump in account takeovers (ATOs) over recent years. ATOs have damaged reputations, disrupted revenue, and driven up IT and account security costs to the tune of $25.6 billion in losses.

Any account with value is vulnerable, not just financial accounts. For example, businesses that make up the gig economy, like Uber and Airbnb, provide their drivers and hosts with the ability to withdraw earnings into personal bank accounts. Fraudsters can target these accounts, take them over, extract the value, and transfer it to accounts overseas.

Value isn't always about money; many businesses today rely on the quality of interactions on their platform. The enjoyment and trust found in using social media forums, dating websites, and reviews on e-commerce sites all depend on limiting fake accounts, spam, and trolling.

Protecting your existing user base is critical. Using a phone number, in conjunction with two-factor authentication at login, ranks high among the best options to increase the protection of user accounts and reduce the cost of fraud to the business.

Protecting transactions

Financial gain is the most significant driver behind a majority of fraud. Being able to spoof, intercept, or falsify a financial transaction is the most profitable tactic. It's also the most costly to a business.

Luckily, protection isn't complicated. Financial accounts opened with an email address/password pair could be simply blocked from making withdrawals until a user's identity is verified by phone number. The account owner is presented with a clear trade-off: provide a phone number, and you can access your money. Scenarios of similar customer engagements that could benefit from stronger identity verification can be imagined for all types of business. However, keep in mind that customers will want to know why you require this data.

The EU has mandated strong authentication for all online payments.

Transactional fraud has grown so much that the European Banking Authority (EBA) has begun enforcing new laws impacting millions of European consumers who will experience a change in the way they shop online. The new European banking law, PSD2, will mandate a stronger form of authentication for all in-app and over-the-phone payments that exceed €30.

This extra layer of security, which could impact conversion and sales for online businesses, can be made easier for customers using phone number verifications via one-time passwords over SMS. Although these regulations aren't rolling out globally, enforcing this type of verification at important touchpoints in customer transactions reduces fraud attempts and can give customers peace of mind knowing you're taking extra steps to protect them from fraud.

Bolstering contact center security

Today's contact centers need to be able to engage with their customers in seamless, ongoing conversations across different channels without losing context along the way. Giving agents the ability to easily switch back-and-forth between multiple communications channels is powerful, but it also opens new opportunities for fraud attempts.

Call center fraud occurs when a fraudster contacts an organization's call center pretending to be someone they're not. Customer use-cases and approaches to addressing contact center fraud can vary, but certain best practices are almost universal. At the most basic level, having agents ask the caller to respond to a phone number verification process before continuing with a conversation will help stop many instances of fraud in their tracks.

International toll fraud

International revenue-sharing fraud (IRSF), aka toll fraud, is a scheme where fraudsters artificially trigger a high volume of calls to premium-rate numbers on expensive routes and then take a cut of the revenue generated. Though there are many other schemes in telecom fraud, IRSF is the most prevalent and has grown six-fold since 2013. Telephony-based fraud continues to climb with the adoption of VoIP and communications APIs, making it easier to place international calls. According to statistics from the Communications Fraud Control Association, losses to telcos and their consumers range around the $38.1 billion mark.

90%

of toll fraud occurs on weekends.

Approximately 90% of toll fraud occurs on weekends. By making concurrent calls, they fly under the radar of detection systems that rely on call detail records, which are only created upon call completion. As a result, attacks will not be detected until calls wrap up, and by then, the damage will have already been done.

As you can imagine, there is no silver bullet for toll fraud. The best prevention strategy is a combination of measures to limit a fraudster's access to your calling capability.

2FA: The second factor of security

User login credentials can be compromised in a number of ways. For example, who hasn't walked past a coworker's desk and seen a password written on a piece of paper and taped to a computer monitor? As a business, you have limited control over that, and once compromised, a fraudster can break into your user's account and your application to commit fraud. Consider implementing a cloud-based two-factor authentication protocol into your app. Once a user verifies their identity via a registered phone number, each subsequent login will require an authentication token that a fraudster wouldn't have access to: your user's mobile device. Without that second factor, the impersonator can't log in and commit fraud.

Account recovery and password reset

As cybercriminals always look for new avenues to exploit, you'll also need to consider protecting the process of account recovery. If you use passwords to protect your users' accounts, you've undoubtedly designed and implemented password reset procedures.

The vast majority of applications today send an email with a link to reset forgotten or expired passwords. Unfortunately, if the email address used to open an account has also been compromised, sending an account reset to that email does no good. Once again, using a phone number as the primary way to prove account ownership is faster than email and more accurate. Plus, if an account recovery request is fraudulent, the real owner will immediately be alerted when they receive the reset text message. Conversely, if they actually are the person making the reset request, they'll find that phone number verification is more secure and more convenient.

CHAPTER 5

What about SMS?

While there are legitimate concerns about the security of SMS, it does have advantages as an identity verification channel. First of all, there's reach. According to a GSMA intelligence study from 2020, more than 5 billion people send and receive SMS messages on their phones. That's about 65% of the world's population. The end-user doesn't need to install any app and can still provide an attestation of their identity. Secondly, it's simple for developers to implement. The Twilio Verify API, for example, can be enabled with just two lines of code.

About 65% of the world's population send and receive SMS messages on their phones.

CHAPTER 6

Considerations for secure solutions

Before investing in more robust account security, be confident that those accounts are worth protecting in the first place. The value of your business will decrease if it's full of fake accounts spreading spam and trolling actual customers. Accounts created with the sole purpose of impersonating others are even more troublesome.

Our advice is to verify all users but to implement additional security for exceptional cases, based on risk assessment.

If you are providing authentication by sending your one-time passcode to the user via SMS, note that while a vast majority of your users will have access to a text-enabled phone, some do not. In these instances, OTP codes are deliverable via a voice call. And while SMS is a common way to get users verified, the best user experience–and a more secure solution for high profile accounts–can be found within app-based 2FA and push authentication strategies. You can deliver both of these types of security protections using a pre-built mobile app like Authy or build it into your mobile app using SDKs. There are also biometric solutions that are being implemented worldwide.

If you allow high-value transactions, such as significant money transfers or the deletion of mass amounts of data, you can add extra protection via the same methods used for login. Consider sending a new authentication instance before approving a transaction, but note that it may not always make sense to authorize every transaction. Only require re-authentication when the transaction value is of high risk or over a certain threshold.

Your speed of response is key to providing excellent user experiences. So, you might want to consider looking to push authentication to offer the quickest and most straightforward user experience. Keep in mind that opportunities for fraud should be addressed at all points of user interaction with your business, from account creation to login to transaction.

Your speed of response is key to providing excellent user experiences.

CHAPTER 7

When to verify

Several stages in the typical customer lifecycle are logical places where identity verification might be beneficial. In fact, some should be mandatory. For example, it is best practice to run identity checks during the onboarding of a new customer or the opening of a new account.

Another critical time to run verification is when there are significant modifications to the account, such as password resets or change of addresses. These account management actions are a vulnerable point for the integrity of the account, as unwarranted changes can lead to account takeover.

To help prevent losses, and to reassure the customer, ensure that the true account holder is the source of the request before allowing substantial account changes.

Verifications also come into play when a transaction triggers a flag. It might be a large transaction amount or some other risk factor that changes the risk assessment and requires further due diligence and additional information.

CONCLUSION

A final word on fraud

Nearly every company faces challenges with fraud and account security nowadays. Fraudsters are continually innovating on ways they can rip off, scam, or spam both companies and users. By using the phone number verification as part of your application flow, in conjunction with APIs that leverage the number to verify, authenticate, and authorize users, you can significantly reduce the risk of fraud, and improve security for your users' accounts.

Thanks for reading.

Would you like to learn more
about what Twilio can do
for your business?

Talk to us