Be bold. Be secure.

ACCOUNT TAKEOVER FRAUD

HOW TO PROTECT YOUR CUSTOMERS AND BUSINESS

eBOOK

Introduction

Account takeover fraud (ATO) is one of the top threats to financial institutions (FIs) and their customers. An identity theft crime, account takeover comes in many different forms. In this eBook, we explain the top techniques criminals use to take control of a bank account.

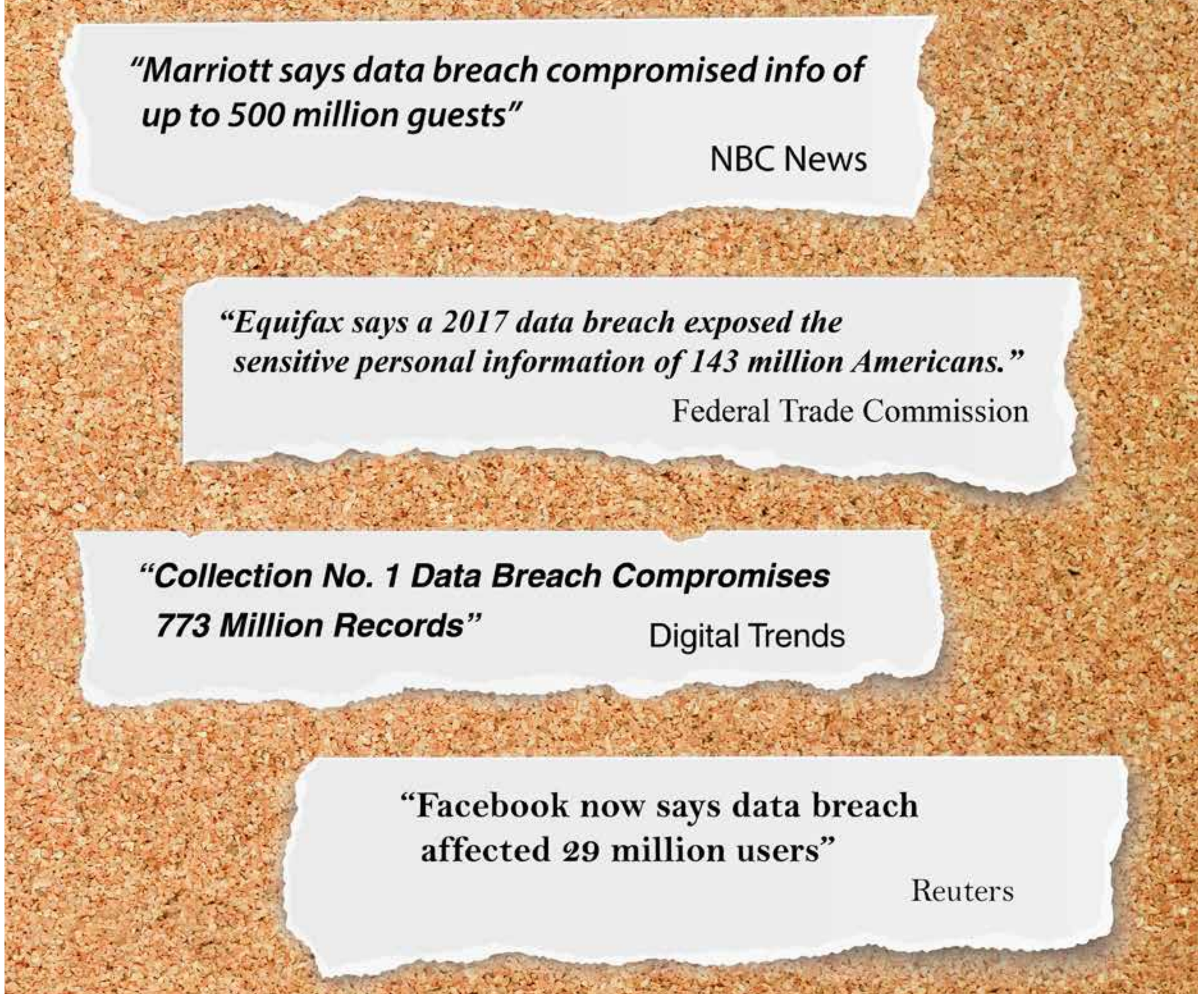
Fraudsters have a variety of weapons and methods of harvesting personal data and causing serious damage, which makes effective protection a challenge. The right multi-layered security approach, however, can help block account takeover fraud and protect customers at every stage of their digital journeys. This guide outlines a best practices approach to detecting and preventing account takeover fraud with proven technologies that shield users, devices, and transactions.

> “89% of FI executives believe ATO fraud is the most common cause of losses in the digital channel.”
>
> AITE Group[1]

ATO TECHNIQUES: DATA BREACHES

Some account takeover attacks begin with fraudsters harvesting personal data. This can happen long before a fraudulent transaction takes place. Bad actors simply purchase personal data leaked as part of a previous data breach. The many recent breaches of large corporations have exposed billions of usernames, email addresses, passwords, credit card numbers, and social security numbers.

With this leaked data, cybercriminals can prepare targeted phishing campaigns. They can also gain unauthorized access to accounts by using an automated attack (or in the case of less experienced fraudsters, by manually typing in combinations of credentials). If an FI's authentication mechanisms rely on weak security measures such as static passwords, criminals will use a technique known as credential stuffing. Credential stuffing is when an army of bots checks a list of stolen credentials against a range of websites hoping for a match. If the authentication process includes multi-factor authentication (e.g., fingerprint and one-time password), gaining unauthorized access to an account will require more effort.



"Marriott says data breach compromised info of up to 500 million guests"

NBC News

"Equifax says a 2017 data breach exposed the sensitive personal information of 143 million Americans."

Federal Trade Commission

"Collection No. 1 Data Breach Compromises 773 Million Records"

Digital Trends

"Facebook now says data breach affected 29 million users"

Reuters

> Only requiring a username/password for access to online or mobile banking systems is grossly insufficient for account security."
>
> KuppingerCole[2]

ATO TECHNIQUES: PHISHING

Phishing scams are a form of social engineering that take advantage of the natural human tendency to trust.

Phishing scams impersonate well-known brands and trusted individuals, and often appear deceptively legitimate. While phishing is executed in multiple ways, including SMS text messages (smishing), messaging services (e.g., Skype), and social media messages, the most common form of phishing is email.

A phishing message aims to create a sense of urgency, often by alerting the user that their account is at risk. Recipients are then persuaded to click links that redirect them to a fake banking portal or to open an attachment that will install a piece of credential-harvesting malware. In the case of mobile users, they don't even have to download an attachment: a link within an SMS can direct a user to a web page that automatically downloads malware to their device.

Common Phishing Techniques

Classic email phishing	Spear phishing	Whaling
Email sent to a large database	Scam targeting a specific individual or group (e.g., Bank X's customers)	Scam targeting a high-net-worth individual to maximize profit
Vishing	**Smishing**	**Overlay attacks**
Phone fraud where a fraudster impersonates a bank employee under the pretext of calling to warn about account access issues	SMS text messages containing a link to a fake banking portal; can also take the form of a messenger-based scam	Overlay attacks on Android devices leverage phishing techniques, creating fake screens to collect banking credentials

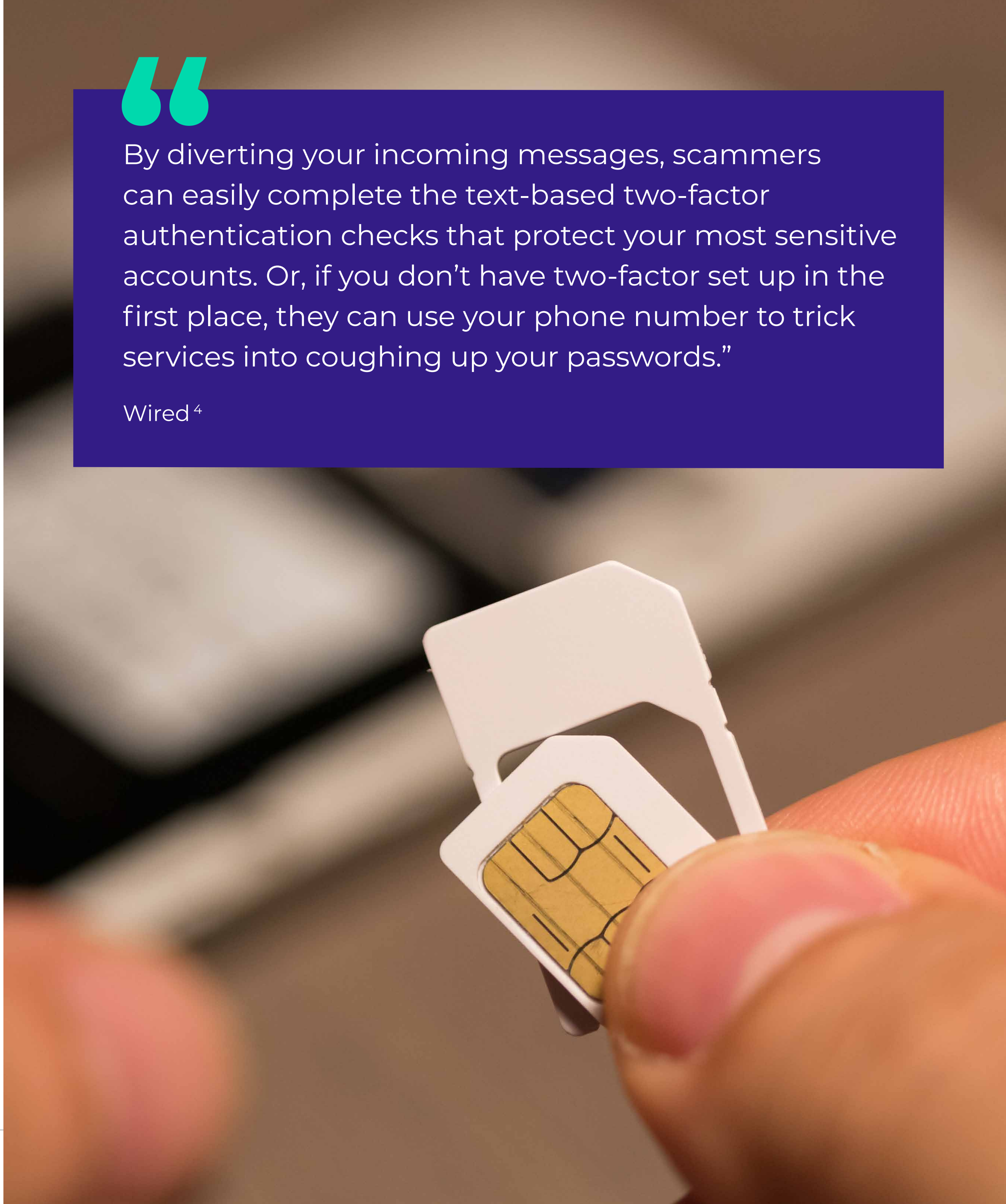
> According to MCSA, there are approximately 15.2 million texts sent every minute of every day. More than 90% of them are opened within 3 seconds, making it a very attractive channel for fraudsters.
>
> Midwest Cyber Security Alliance [3]

ATO TECHNIQUES:
SIM SWAPPING

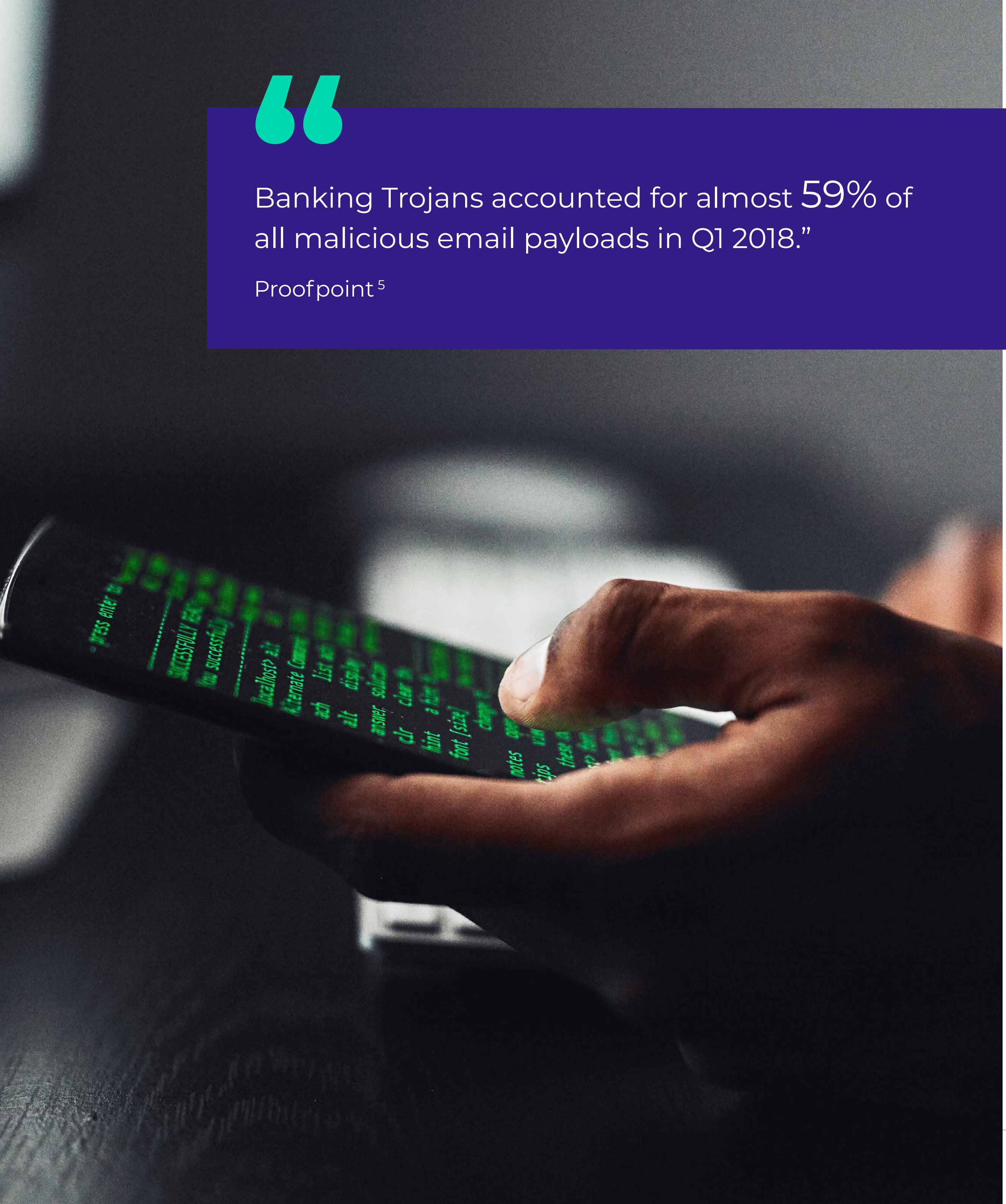
Swapping a SIM card is a legitimate service offered by mobile phone operators when a customer switches to a new device, and the old SIM card is no longer compatible.

Fraudsters can abuse this service. While the fraud requires research and preparation, the hack itself is relatively simple. In what is known as a SIM swap scam, fraudsters use social engineering techniques to transfer the victim's mobile number to a new SIM card. All of the victim's SMS messages are then redirected to the fraudster.

This enables the fraudster to target banking solutions that use the mobile phone as part of the authentication flow. For example, if enrollment of a mobile banking app happens through SMS, fraudsters can use SIM swapping to impersonate the victim and activate the banking app on the fraudster's phone. Also, if the bank's authentication mechanism includes text messages as a means of delivering one-time passwords (OTP), then taking over the victim's number becomes an attractive way for a criminal to authenticate fraudulent transactions, add beneficiaries, or perform other operations within the banking session.



> “By diverting your incoming messages, scammers can easily complete the text-based two-factor authentication checks that protect your most sensitive accounts. Or, if you don't have two-factor set up in the first place, they can use your phone number to trick services into coughing up your passwords.”
>
> Wired[4]



> Banking Trojans accounted for almost 59% of all malicious email payloads in Q1 2018."
>
> Proofpoint[5]

ATO TECHNIQUES: MALWARE

Another way to take control of a bank account is through malware. This malicious software may be installed on the victim's computer or mobile device through a wide range of user actions. These include visiting risky websites, opening attachments from phishing emails, or downloading mobile apps from untrusted sources. It can also be bundled with other programs (e.g., masquerading as a Flash Player update).

Malware programs can perform different kinds of attacks. Some will install configuration files on the infected computer in order to redirect the victim to a malicious website. Some, called key loggers, will intercept everything the victim types, including their banking credentials.

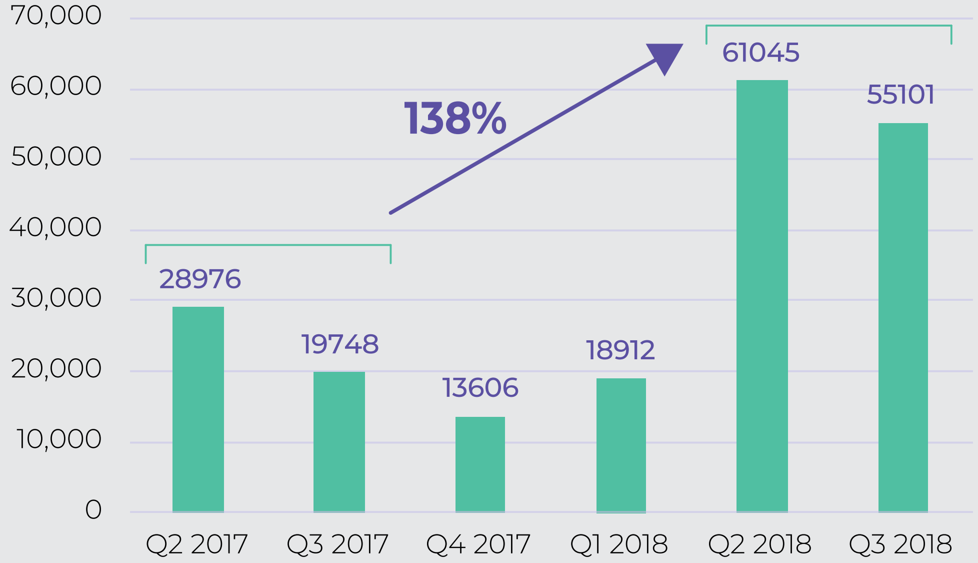
Others can infect a web browser by installing as an add-on. Known as a Man-in-the-Browser attack, they are capable of intercepting credentials or modifying transaction details or other data.

ATO TECHNIQUES: MOBILE BANKING TROJANS

Mobile banking Trojans have been growing in volume and complexity. With as much as 50% of the entire global banking population using their mobile devices for banking services[6], we will continue to see mobile banking malware in the headlines.

One of the functionalities of a mobile banking Trojan is an overlay attack. In an overlay attack, the Trojan presents its own screen on top of the legitimate bank application. The Trojan's fake login interface mimics that of the legitimate banking app, so that the user is none the wiser. This malware will monitor running applications and wait for the targeted mobile banking app to launch. At that point, it will activate and push the legitimate banking app to the background to display its own login interface. The malware then captures the victim's authentication credentials.

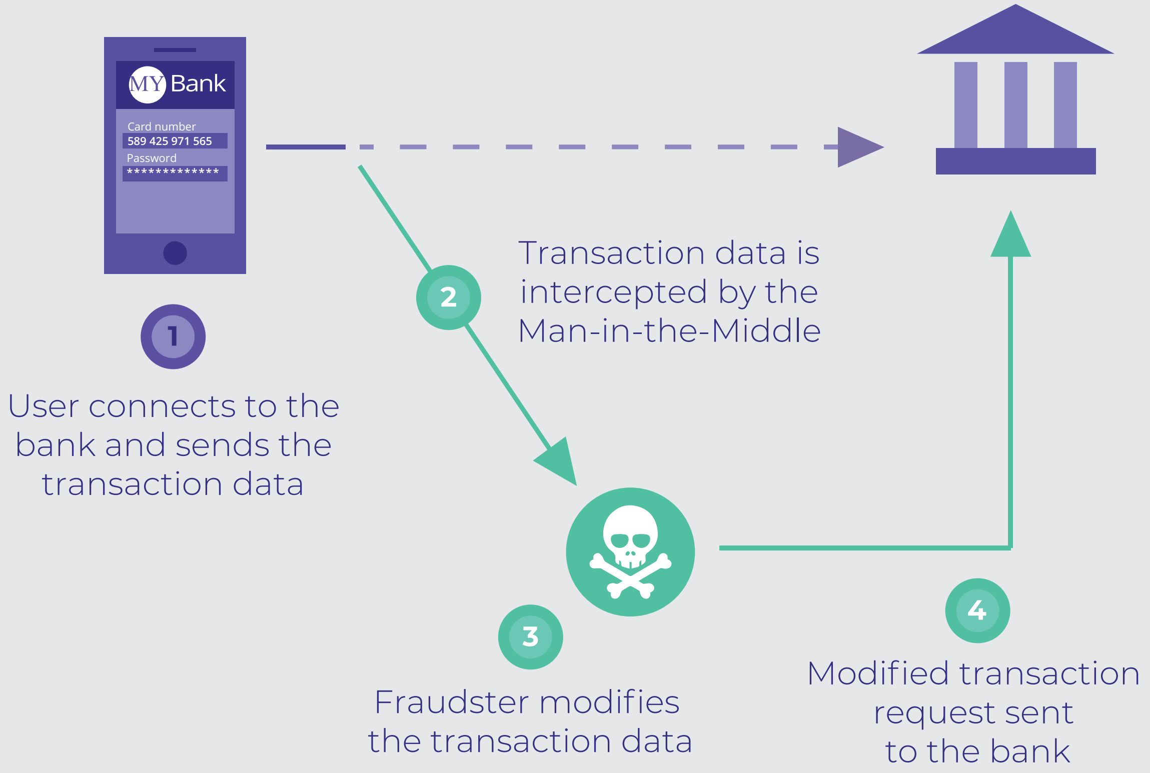
The damage doesn't end there. Mobile banking Trojans can remain active while the victim performs other actions during the banking session. For example, the malware can modify transaction data by intercepting a funds transfer and redirecting the money to a fraudulent account. Some versions of overlay malware, including the newer iterations of BankBot, are even able to intercept text messages.



The number of mobile banking Trojan installation packages increased **138%** over Q2 and Q3 2017
- Kaspersky Lab[7]

> "BankBot now targets over 420 leading institutions in countries such as Germany, France, Austria, the Netherlands, Turkey and the United States."
>
> PaymentsSource[8]

Man-in-the-Middle Scenario



1 User connects to the bank and sends the transaction data

2 Transaction data is intercepted by the Man-in-the-Middle

3 Fraudster modifies the transaction data

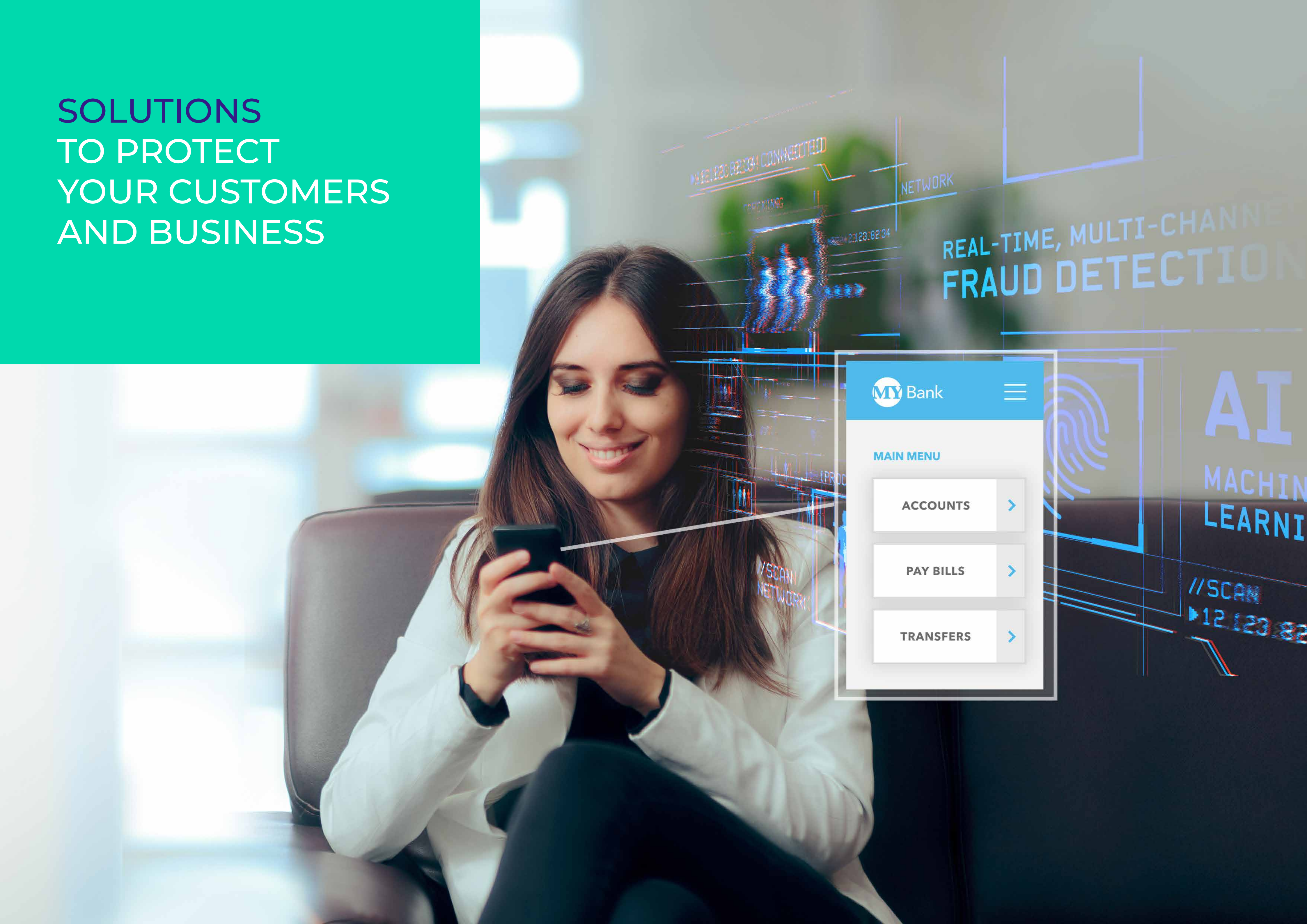
4 Modified transaction request sent to the bank

ATO TECHNIQUES: MAN-IN-THE-MIDDLE

In this type of attack, fraudsters position themselves between the bank and the user in order to intercept, edit, send, and receive communications without raising suspicion. Taking over the communication channel between the user's device and the server can be done by setting up a malicious Wi-Fi network as a public hotspot (known as a rogue access point). People take advantage of public hotspots, not realizing they may be transferring their payment data through a network controlled by a bad actor.

A Man-in-the-Middle attack can also take place through the use of a mobile banking application. Mobile banking apps should apply certain security measures when communicating with a server. However, improper design can make an app vulnerable. Incorrect configuration or lack of a secure channel for mobile data-in-transit also increases the risk of this type of attack.

SOLUTIONS TO PROTECT YOUR CUSTOMERS AND BUSINESS



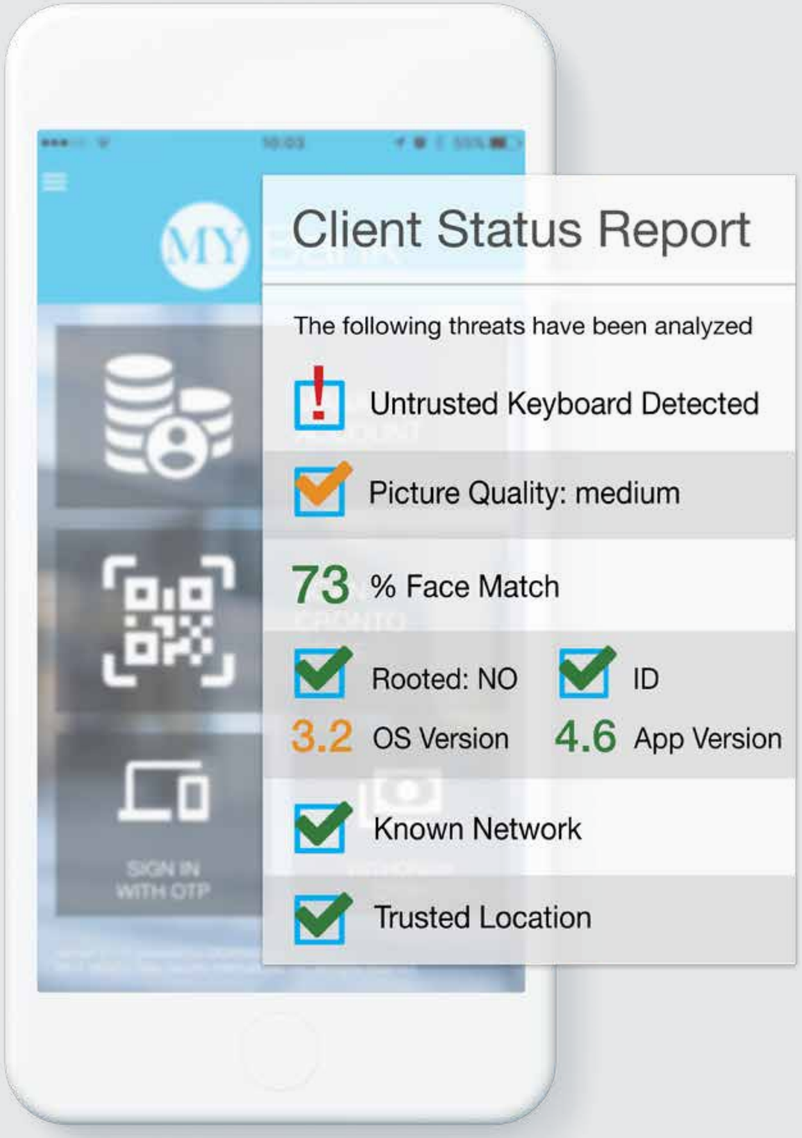
MULTI-LAYERED PROTECTION

Financial institutions apply various security measures to protect customers from becoming victims of account takeover fraud. For example, many educate customers on topics such as how to recognize phishing and how to protect their mobile devices against malware. Despite such preventive measures, the amount of account takeover fraud is growing, with the financial losses now in the billions of dollars.

That is why FIs need additional layers of protection. A multi-layered security approach can minimize the risk and impact of account takeover fraud – protecting a bank's customers and operations, without any negative impact on the user experience.

The next part of this guide explores solutions designed to:

- Protect the user
- Protect the device and the banking session
- Proactively detect fraud across all digital channels
- Provide flexible and secure authentication journeys



Client Status Report

The following threats have been analyzed

! Untrusted Keyboard Detected

✓ Picture Quality: medium

73 % Face Match

✓ Rooted: NO ✓ ID

3.2 OS Version 4.6 App Version

✓ Known Network

✓ Trusted Location

A MULTI-LAYERED APPROACH

Protecting the user

With attack scenarios increasing in variety and complexity, it is important for FIs to implement solutions that help minimize the risk of customers interacting with a fraudster and becoming victims of social engineering or Man-in-the-Middle attacks.

Protecting the device and the banking session

Mobile devices inject risk into the banking journey – but with the proper security, they can actually become an asset and contribute to a safe user experience. Therefore, it is important to include mobile security capabilities, such as app shielding in the app design.

Proactive fraud detection across all digital hannels

It is possible to detect the signs of an account takeover before the customer is affected. To do this, FIs need a solution that can review and act on data collected from users' actions. Within this user data, there are often clues that a customer may be under attack. A modern, comprehensive fraud detection and prevention solution will score every action and every user in all digital channels by gathering knowledge on all actions before, during, and after the session to create a complete overview of the transaction.

Dynamic and flexible authentication flows

A modern approach should support a wide range of authentication methods across different channels. For each transaction, the fraud prevention system should evaluate risk in real time and apply the precise level of security necessary for that specific transaction. Every user action should be treated uniquely and should dynamically trigger the most appropriate authentication challenge. This creates an additional barrier for a fraudster while providing the best possible experience for legitimate customers.

PROTECTING THE USER

OneSpan's unique, patented Cronto® visual transaction signing solution helps protect customers from social engineering and Man-in-the-Middle attacks that lead to account takeover.

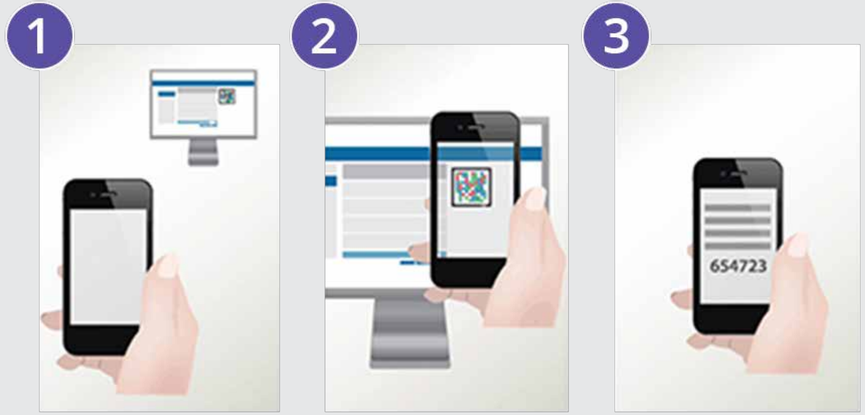
As explained on page 8, in a MitM attack a bad actor intercepts the communication between the customer and the bank and alters the details of a transaction. Such an attack could change a genuine payment into a rogue transfer to an imposter.

To thwart these attacks, Cronto technology displays a unique visual challenge that contains the transaction details. When the user wants to make a payment or funds transfer, they:

1. Enter the payment information into the online banking application. The banking server uses that data to generate a colored cryptogram displayed on the customer's screen.
2. Scan the cryptogram using their phone's camera or a dedicated hardware device. This decodes the cryptogram, decrypts the payment data, and shows it to the user as clear text.
3. Authenticate to their device, and Cronto calculates the authentication response code using a cryptographic key stored on their device. This confirms to the bank that the amount and payee are correct and have not been tampered with. The transaction can proceed.

A bad actor cannot modify the contents of the transaction since the cryptogram is uniquely connected to the transaction details. Any change will invalidate the code. This creates a secure virtual channel between the FI and the legitimate account holder, preventing a MitM scenario.

Cronto Technology in Action



Start the Cronto app on your phone...

... scan a Cronto image on the screen...

... check payment info and use a unique secure number to authorize it.

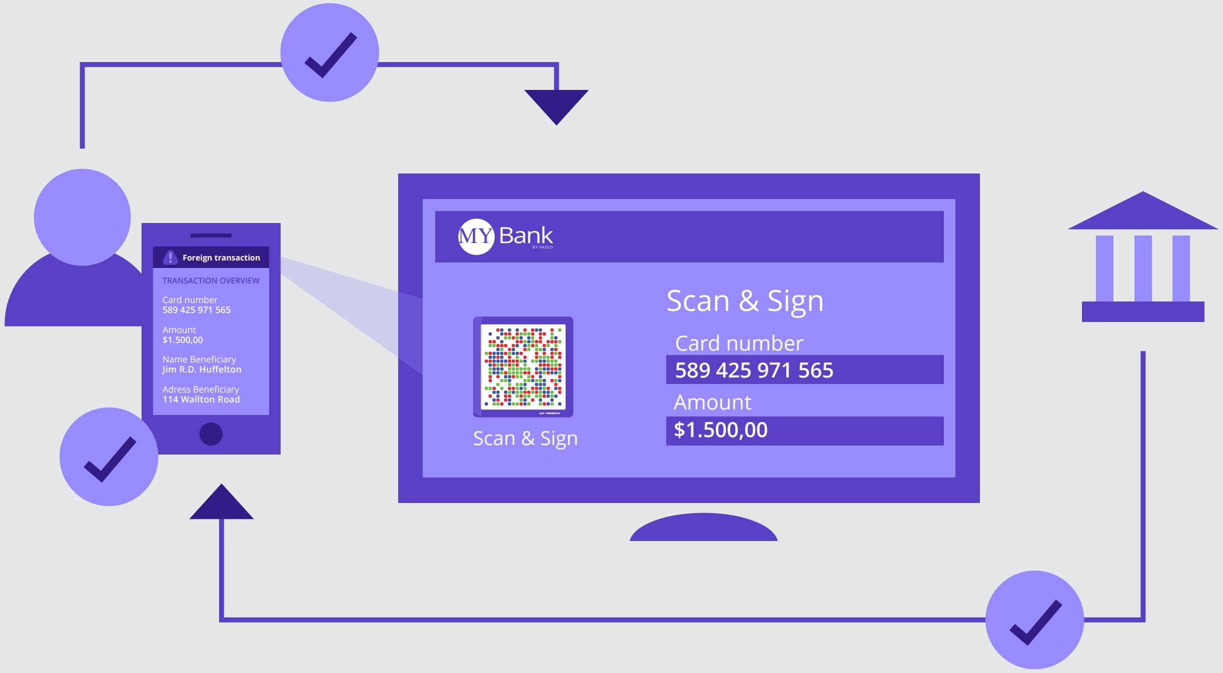
Learn about Cronto in this eBook: Social Engineering: Mitigating Human Risk in Banking Transactions[9]

PROTECTING THE USER

Cronto has been designed to thwart social engineering attacks. The user can trust the security of the transaction knowing only their bank can generate the code, and only their device can decrypt the contents of the code.

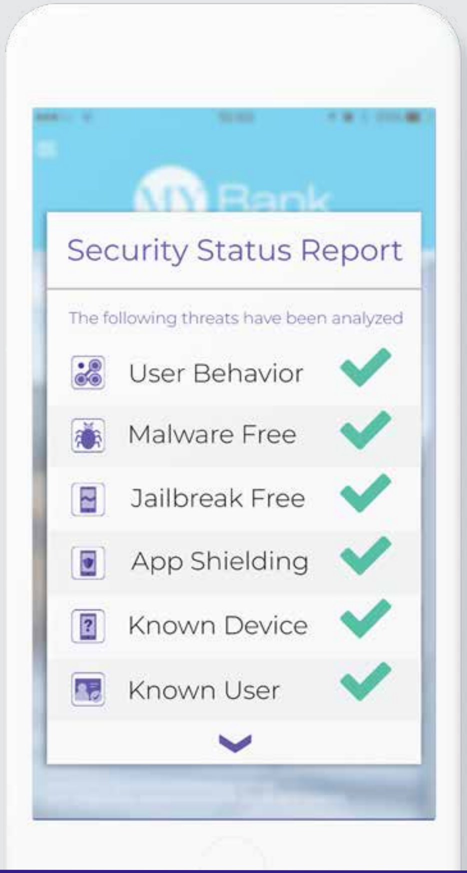
The colored Cronto code contains all transaction data, including the device used, the transaction amount, and recipient account details.

Cronto establishes a secure communication channel between the bank and the legitimate user. Cronto assures the user that the transaction authorization request is coming from the bank.



Cronto provides a clear-text summary of the transaction to the user for review and authorization. To avoid “authorization blindness”, banks can visually alert users to high-risk transactions.

The bank controls the transaction authorization process. Cronto ensures that transaction signature requests reviewed and authorized by the user originate from the bank and can only be viewed by the legitimate user.



Security Status Report

The following threats have been analyzed

User Behavior	✓
Malware Free	✓
Jailbreak Free	✓
App Shielding	✓
Known Device	✓
Known User	✓

Some FIs claim they don't experience much fraud in the mobile channel. While possible, it is more likely that the organization is just unable to track it appropriately. For example, a mobile overlay attack is designed to capture a user's login credentials. The attacker could then use those credentials to infiltrate the online channel – a classic example of online fraud that originated in the mobile channel.

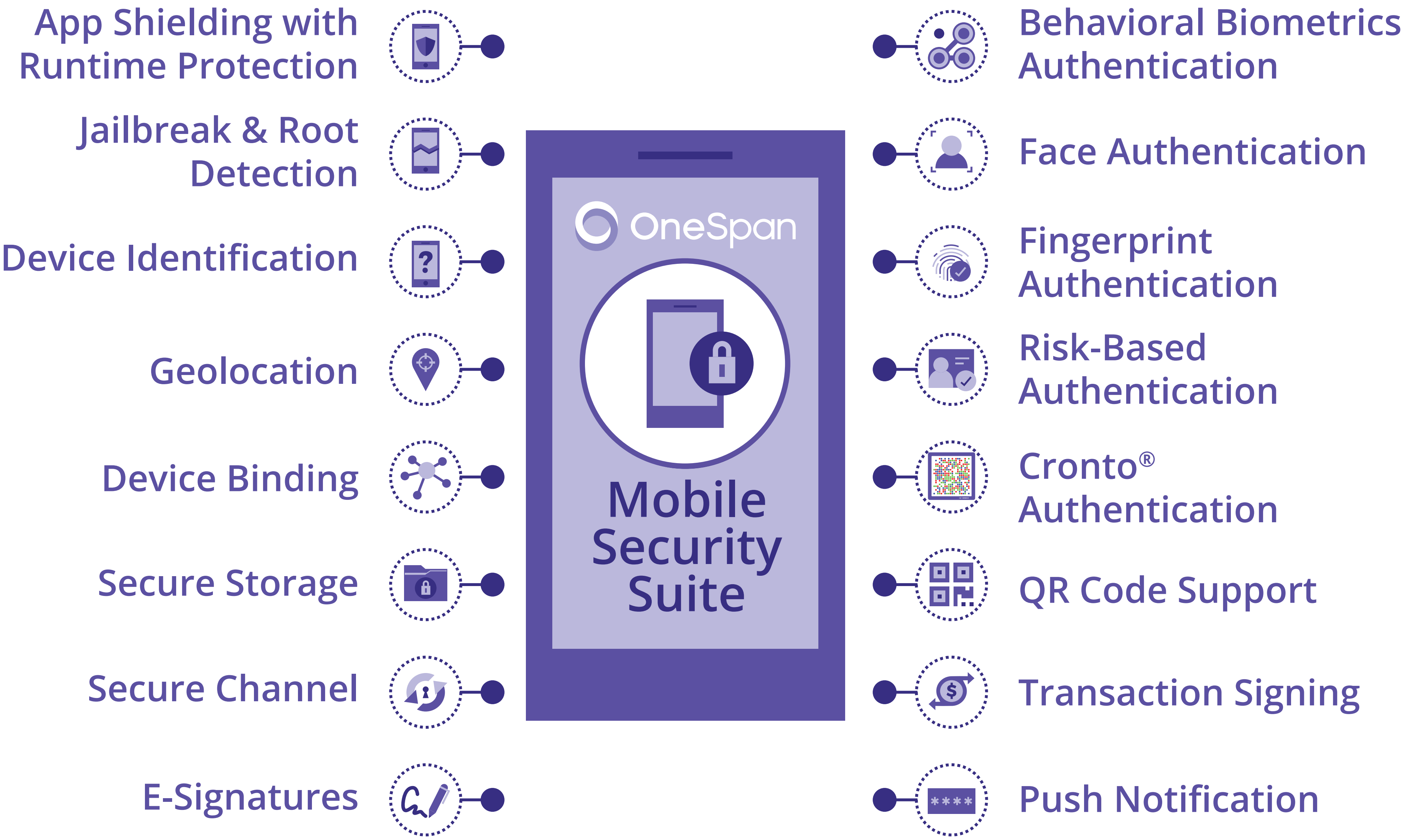
PROTECTING THE DEVICE AND THE BANKING SESSION

With OneSpan's Mobile Security Suite, financial institutions gain visibility into risks in the mobile channel. The solution applies a 360° approach to mobile security, taking into account factors such as the app, device, interface, communications, storage, and users. It can detect risk factors related to the user's device and apply countermeasures. With app shielding and runtime protection, it is able to provide advanced protection against overlay attacks, key loggers, and other malicious technologies. For example, OneSpan App Shielding has a built-in mechanism to detect if an app is put into the background state, which together with other criteria can help determine whether an overlay attack is in progress.

The Mobile Security Suite can also identify risk factors such as a jailbroken or rooted device – and still maintain a secure environment for the app to operate in. This enables customers with a higher device risk profile to continue to benefit from mobile banking.

The Mobile Security Suite includes encrypted, secure communication channels as well as secure storage to prevent eavesdropping. In addition, FIs can implement flexible authentication scenarios with fingerprint, face, behavioral biometrics, and more.

PROTECTING THE DEVICE AND THE BANKING SESSION



OneSpan

Mobile Security Suite

- App Shielding with Runtime Protection
- Jailbreak & Root Detection
- Device Identification
- Geolocation
- Device Binding
- Secure Storage
- Secure Channel
- E-Signatures

- Behavioral Biometrics Authentication
- Face Authentication
- Fingerprint Authentication
- Risk-Based Authentication
- Cronto® Authentication
- QR Code Support
- Transaction Signing
- Push Notification

PROACTIVE FRAUD DETECTION

OneSpan Risk Analytics provides financial institutions with the ability to proactively detect signs of an account takeover before it affects users. The solution continuously analyzes and scores numerous data points in real time across digital channels to create a full picture of user actions (before, during, and after the session). Leveraging machine learning, the risk analytics engine can spot anomalies in user behavior and take appropriate action based on the transaction's risk level.

Risk Analytics detects certain combinations of signals in the user, device, and transactional data, which can provide indicators that customers are under attack. It can also provide an overview of customer actions to help identify suspicious combinations of events.

Thanks to these capabilities, Risk Analytics is also an important security layer in the detection of SIM swap attacks. It collects behavioral biometrics data and other risk-based parameters, such as geolocation, time of the day, or the number of total requests for reactivation. A spike in such requests could be a sign of a SIM swapping attack.

Examples of combinations of events indicating the possibility of an account takeover attack

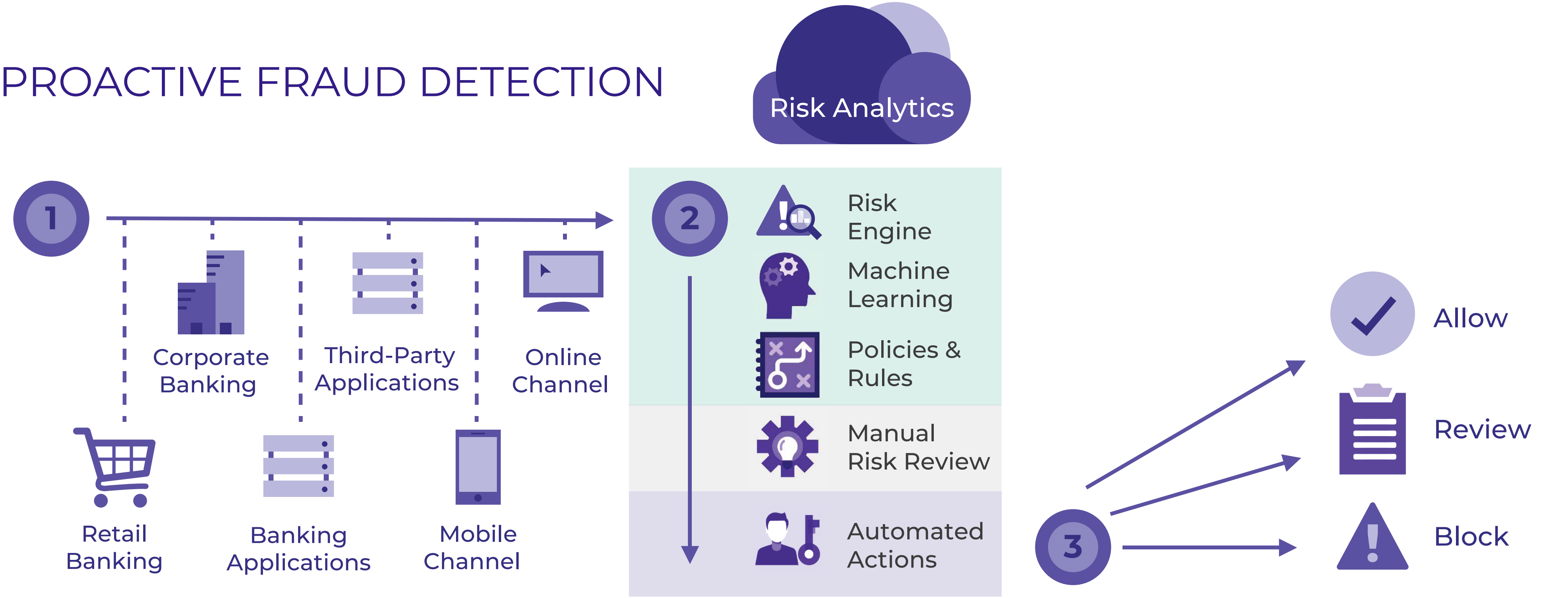
A **login** from a **new location** followed by a password reset and changes in contact details

A **login** from a **new IP** followed by checking the account balance followed by requesting a large transfer

Sudden **password change requests** from multiple users

Accumulation of **unsuccessful login** attempts

PROACTIVE FRAUD DETECTION



1 Risk Analytics collects and analyzes data from a variety of different sources, including:

- **Devices** – Endpoint-centric data monitoring at the device level
- **Behavior** – Analyzes interactions with the device as well as session navigation behavior, such as the speed and time of browsing, to identify suspicious activity
- **Historical** – Analysis of user and account activity in a digital channel, on a historical basis
- **Multi-channel** – Analysis of user behavior across multiple channels, devices, and applications
- **Business applications** – Analysis of financial and third-party application data

2 To determine the risk associated with each financial transaction, Risk Analytics analyzes and scores user, device, and transaction data points across multiple digital channels in real time.

3 Based on the risk score, Risk Analytics automatically takes appropriate action:

- **Allow:** Low risk score – Allows the financial transaction to continue
- **Review:** Medium risk score – Creates an activity case for review; more customer validation is required
- **Block:** High risk score – Blocks the transaction and creates an activity case for review

PROACTIVE FRAUD DETECTION

Identification of Account Takeover Indicators

OneSpan Risk Analytics helps identify indicators of an account takeover attack. It provides an overview of all users and actions; this data can help detect a new attack vector targeting customers. Risk Analytics helps to detect known and emerging fraud scenarios, which is crucial considering the ever-increasing variety and volume of account takeover attacks. For example, by analyzing the http referrer, the solution can indicate the probability of a phishing attack that can lead to an account takeover.

Real-time, Multi-channel Fraud Detection

OneSpan Risk Analytics works in the background, collecting and scoring activities in real time based on a detailed analysis of user behavior, transaction details, and other key contextual data across multiple digital channels. It proactively protects against fraudulent activities by identifying risk at critical steps, predicting risk levels, and taking action when suspicious activities are identified.

Machine Learning, Risk-based Analysis

OneSpan Risk Analytics leverages machine learning and sophisticated data mining and modeling to gain the most accurate predictions of risk and fraud. It collects vast amounts of data from multiple sources and digital channels to ensure the most accurate risk score. These scores drive intelligent workflows that trigger immediate action based on pre-defined and/or bank-defined security policies and rules. The combination of intelligent automation and risk scores streamlines processes, reduces operational costs tied to manual review, and ultimately improves the user experience through fewer false positives.

PROACTIVE FRAUD DETECTION

RISK ANALYTICS HELPS PREVENT:

ATTACKS ON THE LOGIN PROCESS

UNAUTHORIZED CREATION OF NEW BENEFICIARIES

UNAUTHORIZED USER PROFILE ACCOUNT CHANGES

SUSPICIOUS FUNDS TRANSFERS

Risk Analytics is able to help prevent these four scenarios because it:

- Profiles new and existing devices, identifies device changes, and analyzes location and contextual data
- Profiles user behavior, analyzes the user's journey in a banking session, and detects account changes (e.g., changes in spending patterns, profile information, and login speed)
- Profiles new and existing payees (e.g., verifies payee change details, how payees are related to other users, and whether a user has exceeded the number of saved payees)
- Detects suspicious combinations of sensitive operations (e.g., change of user profile, creation of a new payee, change of contact information followed by a money transfer to a new bank account)
- Correlates suspicious activities (e.g., automatically updates hotlists with rogue elements on blacklists or watchlists)

FLEXIBLE, DYNAMIC AUTHENTICATION

The fourth layer of protection is customer authentication. By taking a flexible and dynamic approach to authentication, financial institutions can block account takeover attacks. To provide this level of flexibility, a modern fraud detection solution should:

- Support a wide range of risk-based authentication methods (which in turn enables FIs to eliminate static passwords)
- Evaluate risk in real time for each event and respond by applying the precise level of security
- Assess every action taken by a user and apply the precise level of security to each individual transaction (e.g., a higher risk score may require both a fingerprint scan and a one-time password)

At the same time, a multi-layered security solution must simplify the user experience. Too much friction in the transaction process will alienate customers, while potentially increasing the risk of fraud.

FLEXIBLE, DYNAMIC AUTHENTICATION

OneSpan's Intelligent Adaptive Authentication (IAA) solution provides the precise level of security at the right time for each transaction, based on real-time risk analysis of user, device, and transaction data. Every authentication journey is different – that's why the solution evaluates all user actions case by case to determine the most suitable authentication method(s) based on the level of risk. Tailoring the authentication flow to each unique transaction makes it more difficult for fraudsters to predict and plan their attacks. This unpredictability thwarts a fraudster's attempt to turn a fast profit with minimum effort.

This level of risk-based intelligence also ensures the best possible customer experience. From the user's perspective, the usual actions will be seamless; they will not be bothered with cumbersome authentication methods for low risk transactions. The solution will introduce the right level of friction into the authentication process in order to protect customers' money.

This deep analysis never interrupts the user experience unless it's necessary. Instead, users are only impacted when IAA determines that the level of risk and propensity for fraud justify it. Unlike most fraud tools, IAA ensures the best possible experience for every unique transaction.

Intelligent Adaptive Authentication Process

1. Data collection

IAA collects comprehensive data on the integrity of the device and mobile apps, the behavior of the user, transaction details, and other key contextual data across all digital channels.

2. Risk assessment

IAA leverages a machine learning-equipped risk analytics engine to analyze and score risk for each transaction. In addition, IAA also uses pre-configured rule sets. This powerful combination provides the best method to detect both known and new fraud techniques.

3. Taking action

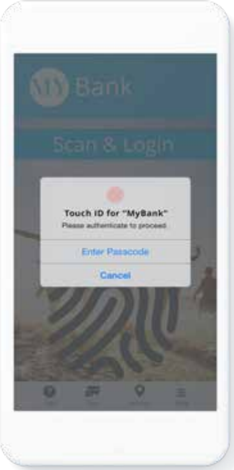
IAA takes action based on a precise risk score. Higher-risk transactions will dynamically initiate a step-up authentication process and lower-risk transactions are completed seamlessly.

> Two- or multi-factor authentication solutions can significantly reduce the possibility of fraud, especially if used in conjunction with risk-adaptive solutions incorporating user behavioral analytics."
>
> KuppingerCole [2]

FLEXIBLE, DYNAMIC AUTHENTICATION

User journey examples with Intelligent Adaptive Authentication

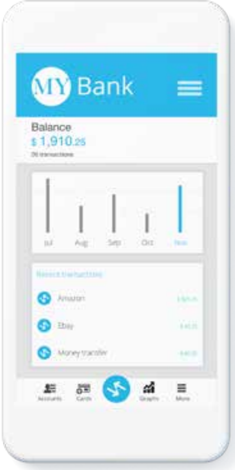
LOW RISK



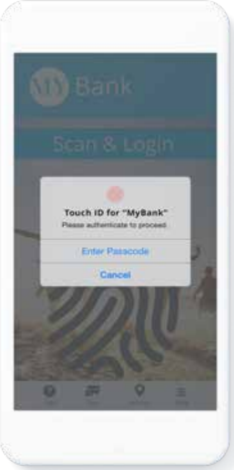
Touch ID for "MyBank"
Please authenticate to proceed

Analysis: **Low risk.**

Action: Fingerprint authentication



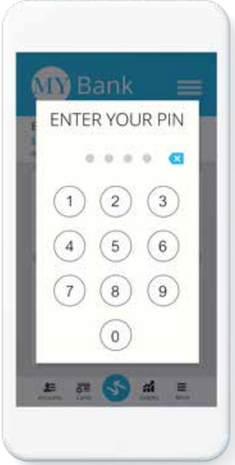
HIGH RISK

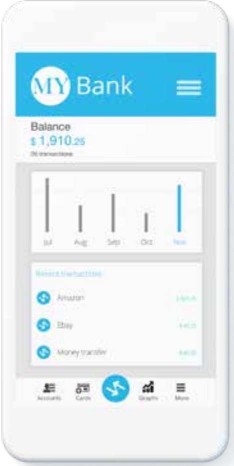


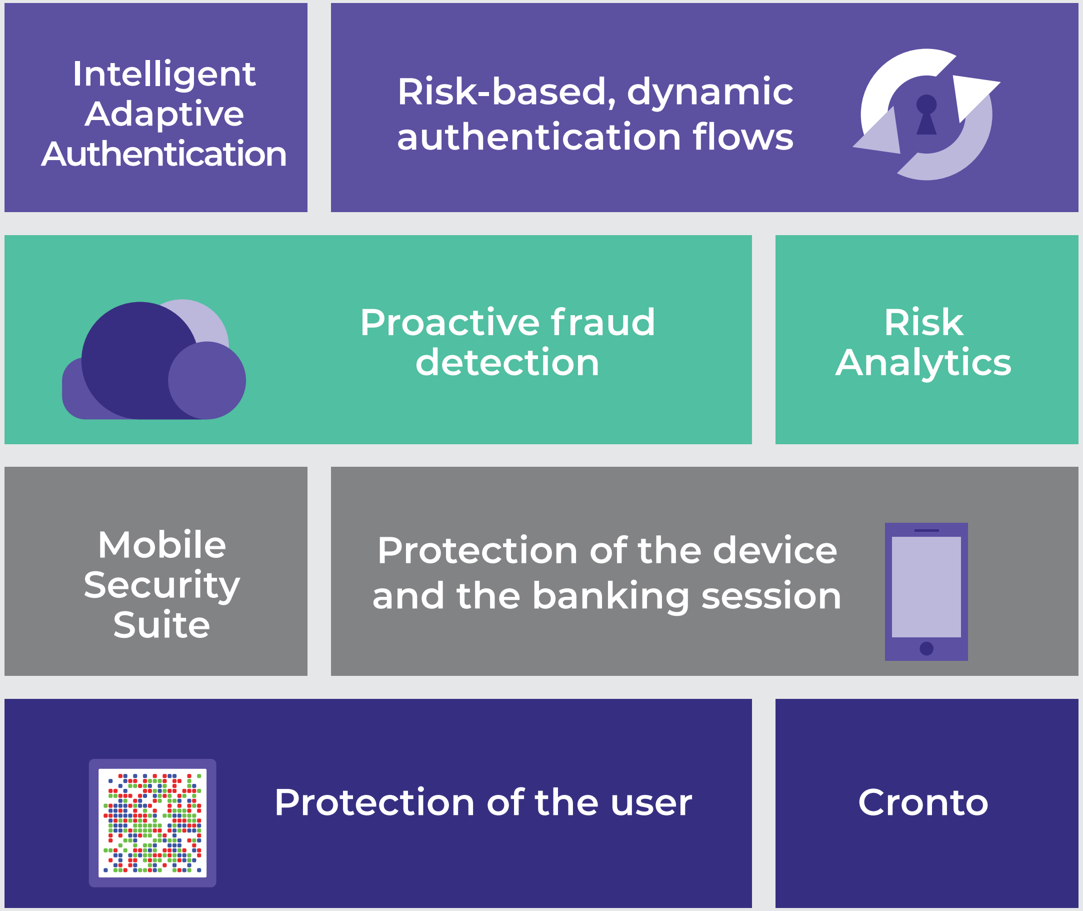
Touch ID for "MyBank"
Please authenticate to proceed

Analysis: **High risk.**

Action: Step-up authentication with PIN







Intelligent Adaptive Authentication

Risk-based, dynamic authentication flows

Proactive fraud detection

Risk Analytics

Mobile Security Suite

Protection of the device and the banking session

Protection of the user

Cronto

SUMMARY

Account takeover fraud is one of the biggest threats facing financial institutions. Unfortunately, it is too attractive a source of profit for criminals. While not everyone can create a new Trojan, account takeover is offered as a service, and tools to perform an account takeover are readily available on the dark web.

Multiple factors contribute to the scale of the threat; for example, the increase and complexity of mobile Trojans, the sophistication of social engineering attacks, and data breaches exposing customers' personally identifiable information.

At OneSpan, we understand the complexity of account takeover fraud and provide the risk-based, intelligent analytics to fight it – in a way that is invisible to users.

Our approach to fraud prevention encompasses: intelligent authentication methods, risk-based analytics, Cronto, and a mobile security suite to protect your customers' digital journey.

To learn more, visit OneSpan.com or contact us.

CONTACT US

For more information:

info@OneSpan.com

OneSpan.com

OneSpan

OneSpan enables financial institutions and other organizations to succeed by making bold advances in their digital transformation. We do this by establishing trust in people's identities, the devices they use, and the transactions that shape their lives. We believe that this is the foundation of enhanced business enablement and growth. More than 10,000 customers, including over half of the top 100 global banks, rely on OneSpan solutions to protect their most important relationships and business processes. From digital onboarding to fraud mitigation to workflow management, OneSpan's unified, open platform reduces costs, accelerates customer acquisition, and increases customer satisfaction.

Last Update February 2019.

[1] https://www.vasco.com/resource-library/download-digital-channel-fraud-mitigation.html

[2] https://www.onespan.com/kuppingercole-intelligent-adaptive-authentication

[3] https://www.midwestcyber.org/smishing-attacks

[4] https://www.wired.com/story/sim-swap-attack-defend-phone

[5] https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q118-quarterly-threat-report.pdf

[6] https://www.juniperresearch.com/document-library/white-papers/futureproofing-digital-banking-2018

[7] https://securelist.com

[8] https://www.paymentssource.com/opinion/self-protection-can-shield-banks-from-new-android-bankbot-card-malware

[9] https://www.onespan.com/solutions/social-engineering-mitigating-human-risk-in-banking-transactions