Visa Business News

VISA

Best Practices 11 February 2021

Best Practices to Mitigate Risk of Account Takeover Fraud

Global | *Acquirers, Issuers, Processors, Agents*

Visa, Interlink, Plus Networks; V PAY; Europe Processing

Overview: Visa is providing information about common account takeover fraud techniques, along with best practices to mitigate the risk of such fraud.

Account takeover (ATO) fraud is a type of identity theft where fraudsters gain access to their victims' accounts, then make non-monetary changes that may include modifying personally identifiable information (PII), requesting a new card or adding an authorized user. This can allow criminals with stolen credentials open access to victims' accounts. ATO fraud has rapidly accelerated, with fraud losses growing from USD 4 billion in 2018 to USD 6.8 billion in 2019.[1]

ATO fraud affects consumers, merchants, issuers and acquirers globally. Its growth is largely due to the rise in e-commerce and the digitization and storage of PII online. Consumer demand for fast and frictionless services has led to a proliferation of new consumer-friendly person-to-person (P2P), business-to-consumer (B2C) and business-to-business (B2B) platforms as alternative payment mechanisms. With secure technologies like tokenization, EMV® migration and other security protocols for individual transactions, fraudsters have pushed to identify vulnerabilities upstream. Data breaches and theft of consumer information have resulted in the commodification of stolen credentials, making them increasingly available for purchase on the dark web.

Advancements in technology have been beneficial to both the payments industry and fraudsters alike. Newer tools, more readily available than ever, have increased the speed and lowered the cost of fraud attacks. As consumers adopt multiple devices in a mobile lifestyle, detection of account takeovers has become more challenging. Since ATO fraud is harder to detect, fraudsters have longer windows in which to monetize, making ATO fraud an increasingly attractive fraud vector.

[1] Javelin Strategy and Research, *2020 Identity Fraud Study: Genesis of the Identity Fraud Crisis*, April 2020

Digital Attacks

Digital attacks continue to pose challenges to the payments ecosystem. The proliferation of payment platforms / channels and the growing list of Internet of Things (IoT) devices provide fraudsters with an easily available and rapidly increasing range of targets. Two-factor authentication protocols requiring either email or text authentication for login have increased the criminal's need for diversion or interception of messages.[2]

How Does a Digital Attack Work?

- A fraudster gains access to an individual's email account and trolls for banking information.

- The fraudster accesses the target’s online banking site and initiates a password change.
- The bank sends a one-time passcode (OTP) to the email account as part of the two-factor authentication protocol.
- The fraudster uses the OTP to complete a password change, enabling access to the individual’s bank account.

[2] Aite Group, *Market Trends in Digital Fraud Mitigation*, December 2019

Phishing, Vishing and Smishing

Well-established techniques for stealing consumer credentials, such as phishing, remain a threat even as new methods such as ”vishing” and ”smishing” have emerged. Phishing is the fraudulent attempt to obtain sensitive information or data such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication. Vishing uses phone calls and smishing campaigns use text or SMS messages to achieve the same end. Email, phone calls, social media and text messages are all solicitation methods by which criminals persuade individuals to divulge sensitive personal information.

Phishing campaigns take various forms, as fraudsters find phishing to be an easy, inexpensive and effective tactic. Used by criminal gangs as well as nation state actors, a successful phishing campaign allows entry into email accounts and gives fraudsters the ability to steal credentials by changing passwords, consumer contact information or email addresses.

Digital Campaigns Targeting Public Anxiety

The global health crisis has opened up new opportunities and avenues for fraudsters to take advantage of individuals by leveraging public anxiety. In April of 2020, Microsoft intercepted and stopped a phishing campaign appearing to offer information related to the United States government’s COVID-19 stimulus programs. The campaign generated approximately 2,300 unique HTML attachments over the course of a single day. In the same month, the UK’s National Fraud Intelligence Bureau (NFIB) unearthed another phishing campaign directing consumers to a fraudulent site to make donations in support of the UK’s National Health Service. A third campaign uncovered in Germany was more successful, diverting up to EUR 100 million in stimulus funds into accounts controlled by fraudsters. That phishing campaign pointed consumers toward registration at a fraudulent replica of the official government stimulus registration website. Applicants who registered had their personal information stolen. Fraudsters used the harvested information to register at the legitimate government site but modified the registration information to include alternative banking information, directing stimulus funds to be wired into bank accounts controlled by the fraudsters.[3]

[3] Visa, *Situational Intelligence Report*, June 2020

Digital Campaigns Targeting Corporations

“Spear phishing” campaigns target employees of companies with access to sensitive or valuable information and can lead to business email compromise. This type of opportunistic fraud often involves criminals impersonating high-level executives distributing instructions to subordinates. These types of scams can include instructions for payments to known suppliers or transfers of funds to bank accounts controlled by fraudsters. Business email compromises involving individuals in the human resources function of an enterprise can serve as the first step for more damaging attacks when the hacked account is used to send batch requests to employees for PII. Hacked email accounts of company CEOs and presidents have resulted in the theft of employee W-2 and tax information including names, addresses, and Social Security numbers.[4]

[4] Trend Micro, *Security 101: Business Email Compromise (BEC) Schemes,* January 2016

Risk Mitigation Recommendations for Digital Attacks

Issuers, acquirers and merchants should take the following steps to mitigate the risk of digital attacks, including phishing, vishing and smishing campaigns:

- Educate clients and employees on maintaining device and software security, with emphasis on phishing, smishing and vishing campaigns.
- Do not click on hyperlinks found in emails or text messages from unknown or suspicious sources.
- Always keep a lookout for email addresses that do not match or reflect the name of the organization or institution, and check for spelling or grammar errors as well as altered logos or images.
- When in doubt about a phone call, SMS text or email received, contact the financial institution directly by calling back using the number on the back of the card or their website, and encourage customers (where applicable) to do the same.

Device Cloning

Devices are now a significant vulnerability in the battle against ATO fraud. Device cloning, or porting, refers to the unauthorized transfer of a phone number or merchant ID number to a device controlled by a fraudster (also known as SIM swap fraud). With merchants now commonly using mobile devices to facilitate transaction processing, the number of device takeovers reported has doubled every year since 2014.[5]

[5] Javelin Strategy and Research, *2019 Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt*, March 2019

Cloning Consumer Devices

Devices such as mobile phones are inexpensive and easily available, and identity verification requirements for new account setup can be satisfied with compromised information available to fraudsters. This allows criminals to use stolen identities to open new accounts or port over existing legitimate phone numbers. This grants threat actors access to OTPs sent out as part of two-factor authentication. Digital wallets stored on devices now store large amounts of valuable information, including account numbers, passwords, phone numbers and email addresses. Furthermore, phone hacking software is now easily available online, eliminating or reducing technical expertise as an impediment to fraud.

How Does Device Cloning Work?

- A fraudster obtains an individual’s PII data from the dark web.
- The fraudster calls into a telecommunications provider, claiming the mobile phone is lost.
- The fraudster provides the stolen PII data to verify their identity, and requests a new SIM card for the phone.
- The telecommunications provider sends out a new SIM card and disables the one in the victim’s phone.
- The fraudster uses the newly issued SIM card to gain access to login information protected by two-factor authentication.

Cloning Merchant Devices

Merchant device cloning and payment gateway takeover is increasingly common. This fraud vector unfolds in a two-step process, occurring through the cloning of POS devices along with the use of illegitimately acquired credentials. Fraudsters obtain POS devices or terminals through theft, online resellers or directly from acquirers by impersonating legitimate merchants. Once in possession of POS devices, threat actors connect these terminals to third-party processor hosts, fraudulently authenticating the connection between the host and the cloned POS devices. This fraud type also requires access to compromised merchant credentials including merchant descriptors, merchant identification numbers (MIDs) or terminal identification numbers (TIDs). Merchant credentials can be stolen through phishing campaigns or brute force campaigns, where fraudsters send high volumes of authentication credential variations to the host. The takeover of the payment gateway allows criminals to push through large volumes of fictitious purchase return transactions. The fraud is monetized when the proceeds are posted to gift cards or credit cards and rapidly cashed out at ATMs.[6]

[6] Visa Security Alert: Ongoing Purchase Return Fraud, March 2019

Risk Mitigation Recommendations for Device Cloning

Cloned merchant devices can be difficult to protect against, as legitimate transaction activity occurs at the same time. This makes it difficult for the processor / acquirer to impose a block on transactions.

Issuers

- Educate clients and employees on maintaining device and software security, with emphasis on phishing, smishing and vishing campaigns.
- Do not click on hyperlinks found in emails or text messages from unknown or suspicious sources.
- Watch for unexpected and/or extended periods of phone silence.
- Conduct real-time velocity monitoring and monitor Bank Identification Numbers (BINs) for spikes in transactions.

Acquirers

- Educate clients and employees on maintaining device and software security, with emphasis on phishing, smishing and vishing campaigns.
- Do not click on hyperlinks found in emails or text messages from unknown or suspicious sources.
- Watch for unexpected and/or extended periods of phone silence.
- Monitor merchant attributes and utilize additional criteria along with the MID and TID to identify cloning. Maintain strict control over POS terminal inventory, randomize TIDs and utilize point-to-point encryption.
- Encrypt the authenticator code or assign a long alphanumeric value.
- Utilize stronger authentication or physical tokens.
- Use transaction keys and real-time velocity monitoring by account.
- Make basic security measures compulsory, such as ensuring the transaction data matches the existing merchant name, TID and acquirer BIN.

Merchants

- Educate clients and employees on maintaining device and software security, with emphasis on phishing, smishing and vishing campaigns.
- Do not click on hyperlinks found in emails or text messages from unknown or suspicious sources.
- Watch for unexpected and/or extended periods of phone silence.
- Use a layered validation approach, employing both Card Verification Value 2 (CVV2) and Address Verification Service (AVS).
- Print only required information and ensure no sensitive information is included on customer receipts.
- Insert random pauses in transaction processing to throttle accounts and slow down brute force attacks.
- Monitor accounts for excessive bandwidth consumption.
- Monitor for failed login events and login attempts with device and session data elements that differ from known user device information (IP address / geolocation, device ID, language, time zone, etc.). Multiple transactions using different cards with the same email address and device ID or multiple logins coming from many different IP addresses should trigger an alert and automatic review.

Credential Stuffing

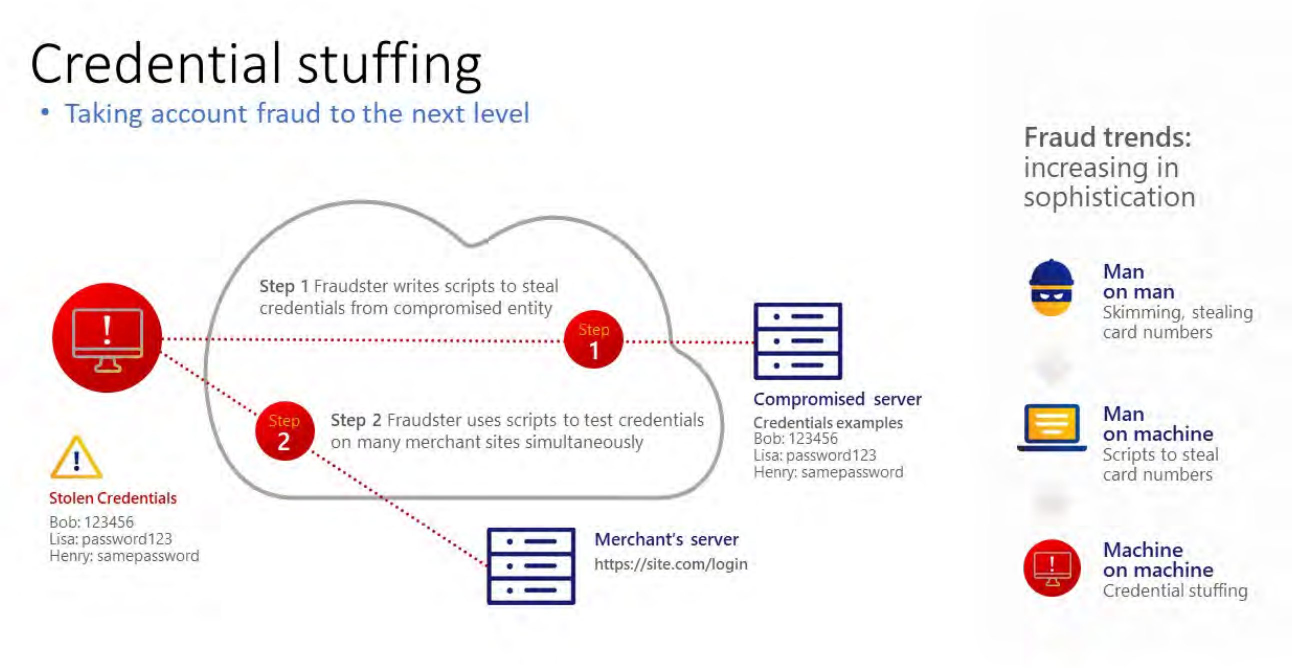
Technological advancements in the payments industry have led to the automation of fraud attacks.[7] New, inexpensive tools are now easily available, allowing for coordinated and multi-prong attacks.

Fraudsters use bots to attack multiple servers simultaneously, running scripts using login credentials stolen during prior security breaches. The exponential growth of low-cost credentials available for purchase has led to decreasing costs and increasing pay-off potential in this fraud vector. This in turn has attracted more sophisticated, well-funded and better-organized fraud rings, increasing the difficulties associated with controlling this type of fraud.

How Does Credential Stuffing Work?

Given the common practice of consumers using a single “favorite password” across most of their accounts, credential stuffing is an attractive and successful method for fraudsters.

- A fraudster uses scripts to steal credentials from a targeted entity.
- The fraudster uses scripts to test the stolen credentials on many merchant sites simultaneously.



Credential stuffing

- Taking account fraud to the next level

Step 1 Fraudster writes scripts to steal credentials from compromised entity

Step 2 Fraudster uses scripts to test credentials on many merchant sites simultaneously

Stolen Credentials
Bob: 123456
Lisa: password123
Henry: samepassword

Compromised server
Credentials examples
Bob: 123456
Lisa: password123
Henry: samepassword

Merchant's server
https://site.com/login

Fraud trends: increasing in sophistication

Man on man
Skimming, stealing card numbers

Man on machine
Scripts to steal card numbers

Machine on machine
Credential stuffing

[7] Aite Group, *Market Trends in Digital Fraud Mitigation*, December 2019

Credential Stuffing Risk Mitigation Recommendations for Issuers, Acquirers and Merchants

- Educate clients and employees on maintaining device and software security, with emphasis on phishing, smishing and vishing campaigns.
- Do not click on hyperlinks found in emails or text messages from unknown or suspicious sources.
- Do not use the same password for multiple sites.
- Develop strong up-front identification and verification procedures.
- Use third-party tools to assess the risk of consumer session data elements such as email, IP address, phone number and device fingerprint.
- Monitor consumer session data elements for use across multiple accounts to identify atypical access patterns.
- Use behavioral biometrics to differentiate between legitimate consumer behavior at login and fraudulent or bot-driven behavior.
- Monitor high-risk account changes and logins, coupled with high-risk transaction or authentication activity.

Social Engineering: Call Centers and Consumers

Social engineering exploits human psychology rather than technology to gain access to sensitive information. It relies on persuasion, manipulation or deception to induce individuals to break normal security procedures and best practices.

Call or contact centers remain an essential component of the customer service experience, with 35% of customer contact channeled through inbound calls to contact centers.[8] Fraudsters use persuasion or phone spoofing to impersonate clients in order to manipulate call center employees into divulging sensitive information. Tasked primarily with the handling of problems and disputes, and focused on customer satisfaction, call center service representatives are not always well-trained or equipped for the detection of fraud.[8] Caller identification and authentication should happen before any customer call reaches a telephone agent.

Criminals are increasingly going beyond call / contact centers to target consumers directly. Direct-to-consumer social engineering involves fraudsters getting sensitive information directly from consumers through phone calls in which they pose as representatives of banks or government institutions. For example, a fraudster in possession of enough information on a consumer's account could call the consumer directly and convince them to provide the OTP received on their phone, effectively bypassing identity authentication protocols.

[8] Javelin Advisory Services: Retail Banking, *Securing the Contact Center*, December 2019

Social Engineering Risk Mitigation Recommendations for Issuers, Acquirers and Merchants

- Educate clients and employees on maintaining device and software security, with emphasis on phishing, smishing and vishing campaigns.
- Do not click on hyperlinks found in emails or text messages from unknown or suspicious sources.
- When in doubt about a phone call, SMS text or email received, contact the financial institution directly by calling back using the number on the back of the card or their website, and encourage customers (where applicable) to do the same.
- Organize call / contact centers into separate sections based on expertise, with regular operations separated from calls considered high risk for fraud detection.
- Monitor call centers for spikes in calls from account holders regarding unauthorized changes to their accounts.
- Be diligent with account holder verification processes. Ask less commonly-used questions or questions regarding other accounts the customer may have or transactions they may have made.
- Invest in multi-factor authentication and layered background risk assessment tools for channeling calls. Phone printing technologies to detect spoofing, synthetic voices and behavior anomalies are available for use and encouraged in high-risk call centers. Additional available tools include natural language understanding (NLU), geolocation, voice biometrics, behavioral analysis and validation, and continuous authentication.
- Establish authentication hubs to fortify caller identity authentication processes and controls.

EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo, LLC.

For More Information

Merchants and third party agents should contact their acquirer.