www.cyberloq.com | info@cyberloq.com

LOCKING DOWN MOBILE TRANSACTION SECURITY

2022 WHITEPAPER

Current paradigms for securing mobile transactions and reducing fraud chargebacks aren't working, putting the longer-term growth of mobile commerce at risk. **Chris Jackson, President of CyberloQ** argues fully secure mobile transactions require failsafe authentication, including laser-focused geolocation technologies that can be easily integrated to prevent fraud before it happens.

TABLE OF CONTENTS

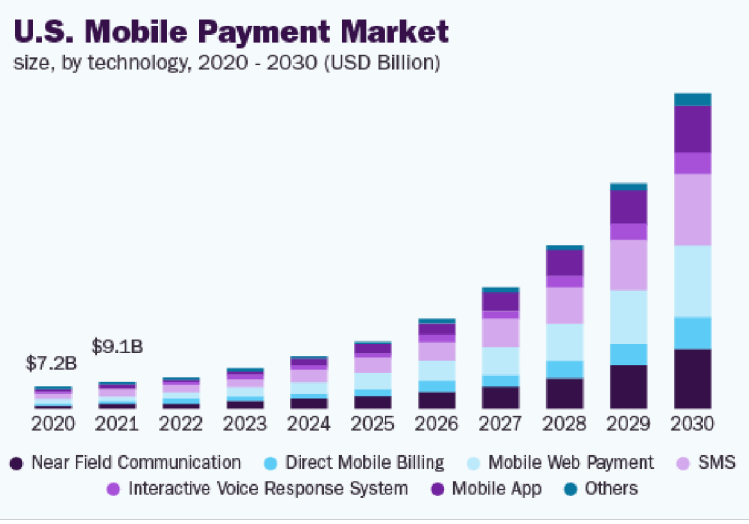
1. M-COMMERCE: GREAT GROWTH, GREATER FRAUD

"Such high levels of fraud are unsustainable, and put the future viability of m-commerce at risk."

The growth of mobile banking and payments has been a major economic and social phenomenon in the last decade. Data from Grandview Research shows growth of almost 27% between 2020 and 2021[1], to reach $9.1 billion in the US, more than 10% of all e-commerce sales.

According to Oberlo Technologies, online shoppers used mobile devices for the majority (72%) of purchases, reserving desktop purchases for higher-value transactions. There's no question that mobile is now the world's preferred way to pay.

Such rapid growth is good news for everyone – consumers, retailers and financial institutions. However, research from SEON[2] shows that fraud on mobile devices was responsible for 50% of all successful e-commerce fraud attacks last year. Meanwhile, the cost of dealing with chargebacks to all parties in the transaction chain keeps rising. Vesta[3] Technologies estimates that chargebacks cost merchants and intermediaries $130 billion globally in 2021 – more than three percent of total mobile sales volume. Clearly, such levels of fraud – and the costs associated with that fraud – are simply unsustainable, and put the future viability of m-commerce at risk.



M-Commerce's Marvelous Growth Trajectory
Credit: Grandview Research

It's also worthy of note that these massive increases in fraud attacks and associated losses come despite the introduction of a wide range of anti-fraud protocols (such as EMV 3DS2), and sophisticated fraud detection algorithms that use Artificial Intelligence (AI) and Machine Learning techniques.

2. MOBILE FRAUD: A PRESENT AND FUTURE DANGER

The core challenge in combating mobile fraud is the need to establish a strong connection between a device, its user and the credentials being used to complete mobile transactions. Criminals have not been slow to exploit this loophole – by some distance, the fastest-growing forms of mobile fraud in the last three years have been Account takeover (ATO) and synthetic ID fraud scams.

Account takeover occur when criminals purchase stolen account information over the dark net, or through faked extensions to customers' web browsers which harvest log-in credentials and store them for criminal use. By far the largest growth area for account takeover is in the mobile internet environment: Sift Technologies estimate this form of fraud rose by more than 300% between 2019 and 2021[4]. "Synthetic ID" scams happen when criminals blend stolen information from bank accounts, social security IDs and other sources to create a fake persona which is then used to purchase goods via the mobile channel.

"Mobile fraud is rocketing because current measures cannot identify users and their physical location or presence. These measures also slow down transactions and add unnecessary friction at checkout."

Mobile fraud is rocketing because current anti-fraud measures cannot precisely identify both the identity of a user or their physical location and presence in a transaction. What's more, today's anti-fraud measures are slowing transactions down and adding unnecessary friction at checkout, especially when it comes to cross-border purchases.

As new payment channels such as account-to-account transactions that promise instant clearing and settlement become increasingly popular, we can expect fraud-based chargebacks to become even more of a problem, given the as-yet undeveloped regulatory environment around such transaction types. Crypto-currency payments, currently growing at around 30% per month, add yet another dimension to the problem, as crypto users have no recourse in the event of fraud as things stand today.

3. TRIPLE-LOCKED MOBILE SECURITY

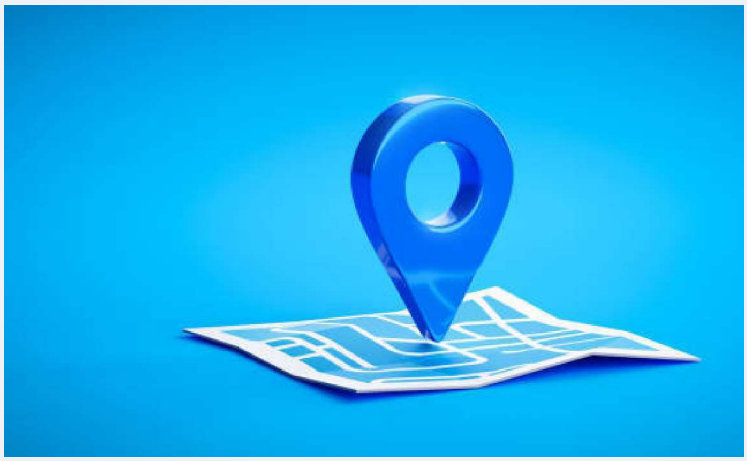
"As well as enabling genuine users with less friction via strong on-device authentication, we need a solution that stops fraud from happening – rather than merely discovering it."

The mobile commerce market urgently needs a security solution that accurately and rapidly identifies the fraudulent use of a mobile device, while at the same time confirming the identity of bona fide users to make their transactions faster and smoother. As well as enabling genuine users to transact with less friction via strong on-device authentication, we need a solution that identifies and prevents fraudulent transactions before they complete, rather than belatedly identifying "successful" fraud events. In other words, a solution that stops – rather than merely discovers – fraud.

CyberloQ has created a Multi-Factor Authentication (MFA) solution which features a unique CyberloQ User ID. By cross-referencing this ID with a mobile device's unique hardware identification number – such as an iPhone's Unique Device Identifier or UDID – users can be authorized rapidly and effectively. Most importantly, usage can be restricted to clearly defined geographic boundaries and the CyberloQ application will only function within these boundaries.

4. THE POWER OF PRESENCE AND PLACE

In addition to confirming User ID on-device, CyberloQ's authentication technology is currently the only solution available that can permit or deny transactions within a tightly-defined geographic area by confirming the precise location in which a transaction is taking place. Unlike other systems, which only include latitude and longitude, CyberloQ also includes an elevation dimension – acting as an additional security factor confirming that a device is in fact in the location it reports.



These features are simply invaluable when it comes to combating ATO and synthetic ID attacks: a report from Syniverse[5] found that although Brazil, the UK and Mexico were most affected by mobile fraud, most attacks using devices in these countries actually originated in the US, Spain and Peru. CyberloQ's technology effectively interdicts the possibility of such attacks taking place by matching geolocation data with device information and authenticated user ID.

Furthermore, by placing CyberloQ's proprietary multi-factor authentication ahead of any merchant credential requirements, location and identity are confirmed before any transactions take place. This means that CyberloQ acts as a rapid and effective authentication solution, with authentication times significantly faster than the lengthy and complex escalated or manual authentications experienced when using EMV 3DS2 or other digital security arrangements.

5. SIMPLE INTEGRATION, EXCELLENT RESULTS

CyberloQ has recently teamed up with banking orchestration platform Pannovate to facilitate the integration of our system for financial institutions and fintechs of all sizes in any geography. Already trusted by some of the world's largest payment and banking brands, Pannovate's Banking as a Service (BaaS) platform and orchestration layer enables banks, fintech and businesses to power growth and deliver seamless digital and embedded finance experiences, ensuring the best user experience over any device. By working with Pannovate, your firm can integrate CyberloQ quickly and easily, so your end users can benefit from best-in-market mobile transaction security.

Locking down mobile transaction security

CyberloQ has created the most robust, flexible and dynamic security platform available to the payments industry anywhere. Key capabilities include:

Multi-Factor Authentication – users are allotted a unique combination of an app User ID and PIN. CyberloQ retains a record of the unique device identifier (UDID) for each authorised device. The ability to transact can be denied instantly and automatically if credentials are not confirmed, preventing fraud before it happens.

Geofencing – access can be restricted to clearly defined geographic boundaries which can move from continents to countries, cities, neighbourhoods and, if necessary, specific custom-drawn boundaries (e.g., one or two specific city blocks). Specific users can have different geographic authorisation boundaries applied to their device, making CyberloQ an ideal solution for payments using company devices – among other applications.

Access Credentials – because CyberloQ sits ahead of any authentication solution from merchants or banks, it effectively prevents the use of fake IDs before such events occur.

Comprehensive Activity Logging – all user activity can be comprehensively logged, including map-based location information and user access activities. Such information is essential in tracking, proving and preventing fraudulent transactions.

6. RESPONDING TO MOBILE'S GREATEST CHALLENGE

Securing mobile commerce may be the biggest challenge facing the payments industry today. Current solutions have failed to make the connection between the physical location of a device user and the credentials being used to authorise transactions.

CyberloQ's innovative solution solves this weakness through its combination of device identification, geo-location validation and multi-factor authentication to deliver on mobile commerce's promise of faster, safer and more secure transactions in any environment.

To find out more about how CyberloQ reduces fraud and chargebacks in mobile payments networks while enhancing business growth from permissioned users, contact us at info@cyberloq.com or +(1) 612-961-4536

Appendix

[1] See Grandview Research, 2022, “Mobile Payments Industry Analysis”: https://www.grandviewresearch.com/industry-analysis/mobile-payments-industry

[2] See Card Not Present.com, 21 July, 2022, “Mobile Devices Driving Fraud Growth”: https://news.cardnotpresent.com/news/mobile-devices-driving-fraud-growth

[3] See Vesta.io – “How to reduce chargeback expenses”, 4 March 2021 on https://www.vesta.io/blog/

[4] See Helpnetsecurity.com, October 6, 2021: “ATO attacks increased 307% between 2019 and 2021”: https://www.helpnetsecurity.com/2021/10/06/ato-attacks-increased/

[5] See BusinessWire: “Syniverse Report Highlights Countries with Most Mobile Fraud” https://www.businesswire.com/news/home/20170110005121/en/Syniverse-Report-Spotlights-Countries-Highest-Mobile-Fraud

ABOUT CYBERLOQ

CyberloQ is a cybersecurity solution that enables clients to implement highly robust Multi-Factor Authentication (MFA) that includes client-defined location-based geofencing constraints. Our state-of-the-art solution protects access to our client's sensitive Personal Identifiable Information (PII) and to any digital assets, including, but not limited to: Bank Cards, Digital Wallets, Web Portals, IOT, Structured Data, Equipment or Process Activations.

Connect with us today to learn more!
www.cyberloq.com | info@cyberloq.com

About Our Partner Pannovate

Panovate is a Banking-as-a-Service platform and orchestration layer that empowers banks, fintechs and businesses to deliver seamless digital and embedded finance experiences for the connected economy. With 150 APIs and a network of 47 fully integrated and proven partnerships from processors to KYC providers and BIN sponsors, clients can seamlessly gain access to Pannovate's modular solutions and orchestration layer for wallet management, payment processing, and card issuing.

Our platform has been designed from the ground up to include the most relevant features needed to launch a banking or payments proposition with speed to market, while offering the flexibility to accelerate the development of digital capabilities.