Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **July 2022**
Commissioned by **Approov**

The State of Mobile App Security in 2022

Executive Summary

Mobile apps have become key tools for businesses to serve customers, earn revenue, and enable remote work by employees. Over the last two years, mobile apps have become critical to success for the majority of businesses. Three out of four respondents indicate mobile apps are now "essential" or "absolutely core" to their success—which is three times higher than two years ago.

Embracing secure development practices for building mobile apps and APIs is essential to safeguard data, customers, and corporate reputation. However, run-time security threats against mobile apps and APIs continue to inflict damage on organizations—and cannot be prevented merely by adopting more secure development practices. Run-time security threats are different than development threats and urgently require a separate set of security strategies.

KEY TAKEAWAYS

The key takeaways from this research are:

- **Secure development practices are essential but offer only partial protection**
  Better integrating secure development practices into the software development life cycle does not eliminate the threat of run-time attacks against mobile apps and APIs. Run-time attacks against APIs that render mobile apps non-functional impose a costly effect on 75% of organizations.
- **Organizations lack visibility into run-time threats against mobile apps and APIs**
  Three fifths of organizations do not have the optics to see a range of run-time threats against mobile apps and APIs, including data theft via API abuse, fake account creation, and credit fraud, among others.
- **Desire to reduce threats enabled by hardcoded API keys**
  With about half of mobile apps storing API keys as hardcoded secrets, the use of more than 30 third-party APIs per mobile app creates a significant run-time threat space. 55% of respondents place high priority on removing the need to store API keys and other hardcoded secrets in mobile apps.
- **The competitive market favors speed to market for new features over security—which is dangerous**
  Organizations are prioritizing speed to market for new features over security considerations, with one half of organizations willing to ship apps with known insecurities. For two fifths of organizations, security processes for third-party and inhouse developers are weak and insufficient. Security efforts are often under-resourced and less important than developing quickly.

Run-time security threats against mobile apps and APIs continue to inflict damage on organizations—and cannot be prevented by adopting better secure development processes.

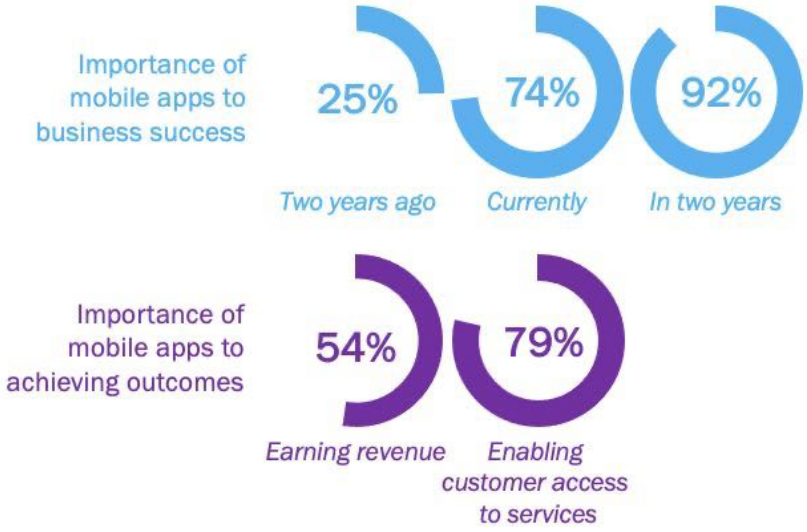
ABOUT THIS WHITE PAPER

In this white paper, we present the findings of a survey into the state of mobile app security in 2022, encompassing survey respondents from across the United States and the United Kingdom. The survey and white paper were commissioned by Approov. Information about Approov and details on the survey methodology are provided at the end of the paper.

Importance of Mobile Apps

The importance of mobile apps to business success has tripled over the past two years. Three out of four respondents indicate mobile apps are now "essential" or "absolutely core" to their success, up from one out of four two years ago. This is expected to increase even further in two years. Specifically, mobile apps are highly important for enabling customers to access services for four out of five organizations and are tied to earning revenue at more than half of organizations. Remote work, online shopping, and online entertainment fuel these measures. See Figure 1.

Figure 1
Mobile Apps and Business Success



Source: Osterman Research (2022)

The importance of mobile apps to business success has tripled over the past two years.

By implication, attacks that render mobile apps non-functional cause significant negative impacts:

- **Successful attacks against mobile APIs would impose a damaging effect at three out of four organizations**
  Threat actors are intensifying their focus on the mobile channel as an attack vector. The intent is to breach customer data, stop apps from working, and compromise customer accounts. For three out of four organizations, a successful attack against their mobile APIs that rendered mobile apps non-functional would have a moderate or major effect on their business. Negative effects include customers not being able to access services, customers abandoning services and switching to alternate providers with a stronger security story, and lost revenue when customers shop elsewhere.
- **Corporate reputation, customer trust, company value, regulatory breaches, and revenue are intricately linked to mobile apps and APIs**
  On average, two out of three organizations indicate that security for mobile apps and APIs is important to safeguard corporate reputation, customer trust, and company value. Avoiding regulatory fines is a significant factor for three out of five organizations.

Threats Against Mobile Apps and APIs: Unaddressed Run-Time Threats

Mobile apps and APIs face a set of attacks at run-time that cannot be stopped or prevented by integrating secure development practices earlier in the software development life cycle (the "shift left" movement). In this section, we look at the nature of run-time threats and the weaknesses in organizational processes for protecting against these threats.

RUN-TIME THREATS AGAINST MOBILE APPS AND APIs

Mobile apps and APIs need to be developed with security as a core practice, but even apps with no security vulnerabilities cannot eliminate a range of run-time threats against mobile apps and APIs. Threat actors are pursuing new types of attacks to compromise accounts, breach data, and wreak havoc on organizations. Getting secure development practices right is essential to deal with coding vulnerabilities, misconfigured storage settings, and lack of segmentation in databases, but these mitigations do not address run-time security threats, such as:

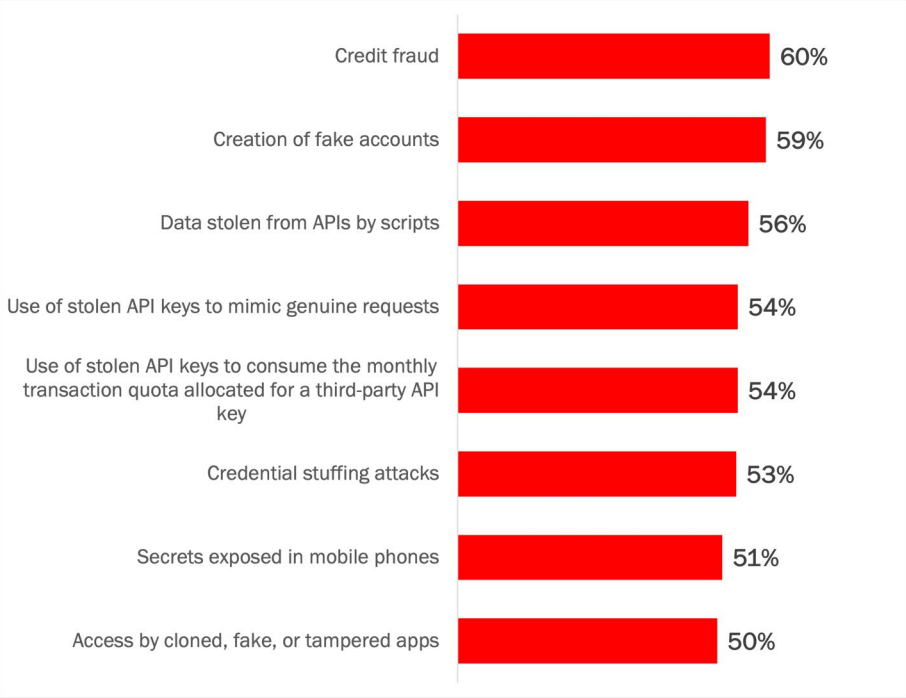
- **Abuse of APIs to steal data, mimic genuine requests, and consume quotas**
  API keys are extracted from valid mobile apps and used by threat actors to gain access to data they should not be able to view or edit. Many organizations store the API key in their mobile apps for ease of deployment—for both APIs developed internally and by third parties—but when these API keys are extracted from the genuine app, they can be used by threat actors to gain access to data in unauthorized ways. Stolen API keys can also be used to mimic genuine requests and consume transaction quotas—which becomes costly when additional quota must be purchased to restore functionality that has been consumed by rogue transactions.
- **Access by cloned, fake, or tampered apps**
  Threat actors clone a genuine app and adjust how it operates. This can include the addition of new functions (e.g., to steal customer credentials by sending a copy to a server controlled by the threat actors), modification of internal checks (e.g., the right to access premium features always evaluates to true), and the use of API keys extracted from other apps to gain access to controlled resources. In 2021, Apple rejected over 500,000 apps for containing undocumented features, being copycat apps (e.g., cloned), or violating privacy[1]—25% of the total number of apps in its App Store.
- **Creation of fake accounts**
  Threat actors use bots to bypass the account registration form and leverage APIs to create fake accounts, which offers a foothold in the app to influence product reviews, spread misinformation, and stockpile signup bonuses. Having a high share of fake accounts decreases the reputation of the app and its provider, undermining user confidence in the app and reducing network effects and revenue. In recent years, Facebook has routinely removed billions of fake accounts each year.[2]
- **Credit fraud**
  Credit fraud occurs whenever threat actors use stolen payment credentials to submit unauthorized transactions for products or services, e.g., when stolen credit card details are used to purchase gift cards that can be distributed rapidly for laundering. In 2021, Apple stopped nearly $1.5 billion in fraudulent transactions on its App Store and blocked 3.3 million stolen credit cards.[3]

Organizations lacking protections against run-time threats are disregarding a large share of the threats against their apps and APIs.

- **Credential stuffing attacks**
  Scripts run credential stuffing attacks using account details assembled from earlier breaches or password spray attacks to test if a valid customer account exists with the same details. If a match occurs, while the account details are valid, the person supplying the details is acting with malicious intent and without authorization to use those details. In 2020, Akamai detected 193 billion credential stuffing attacks, including 3.4 billion against financial services firms.[4]

Between half and three in five organizations lack visibility into a range of run-time threats against mobile apps and APIs—they are unable to see, detect, or have the optics on common run-time threats. In combination, these attack types allow threat actors to establish a presence in an organization's systems, manipulate APIs to steal data they have no right to access, gain access to protected data (e.g., customer data that should be protected in keeping with good practice and regulations such as GDPR), and create fake purchase transactions that rely on credit fraud. See Figure 2.

Figure 2
Lack of Visibility into Security Threats Against Mobile Apps
Percentage of respondents indicating poor visibility



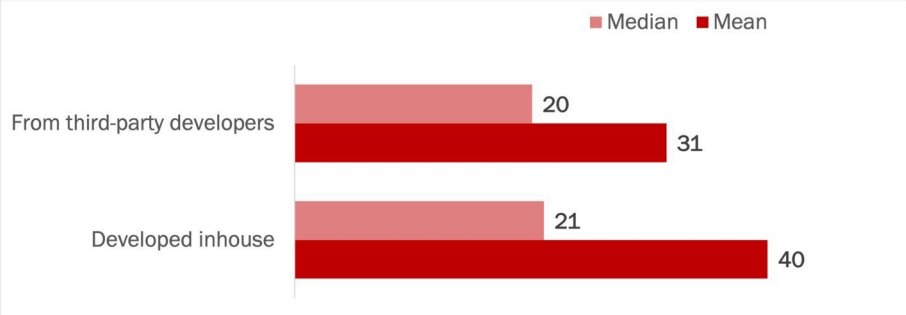
Source: Osterman Research (2022)

Mobile apps and APIs face a set of attacks at run-time that cannot be prevented by merely embracing secure development practices.

API KEYS ARE COMMONLY STORED IN MOBILE APPS—CREATING A MASSIVE AND UNPROTECTED ATTACK SURFACE

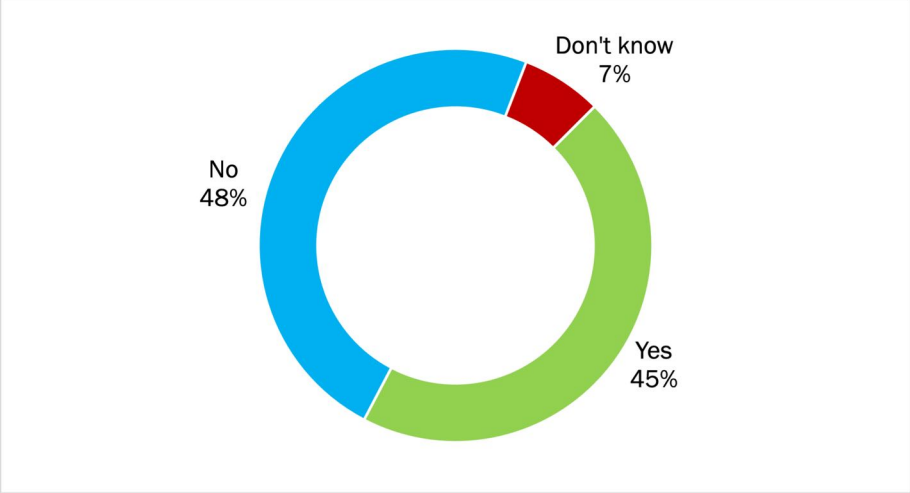
Almost half of organizations store API keys for third-party APIs in their mobile apps. With an average of 31 third-party APIs included in each mobile app (see Figure 3), any threat actor who can extract the API key from the mobile app can use it for malicious purposes. API attacks against mobile apps expose data to unauthorized individuals, put sensitive customer data at risk, fabricate fake user accounts, and create false transactions that undermine customer trust in the integrity of apps. Storing API keys in mobile apps creates a massive attack surface for bad actors to exploit, signaling the priority of protecting against run-time attacks. See Figure 4.

Figure 3
Number of APIs in Mobile Apps by Source
Average and median number of APIs



Source: Osterman Research (2022)

Figure 4
Third-Party API Keys Stored in Mobile Apps
Percentage of respondents



Source: Osterman Research (2022)

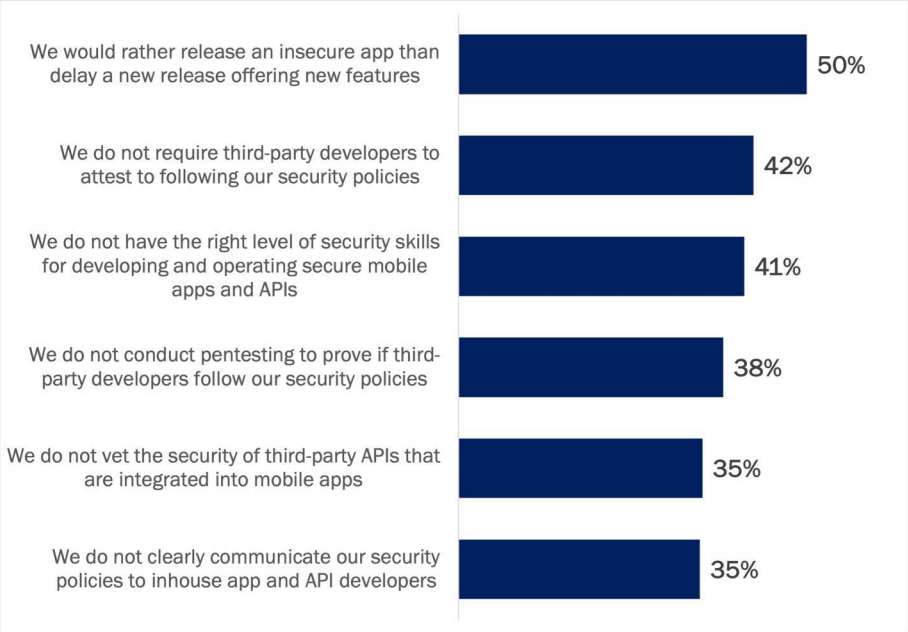
Organizations that store third-party APIs keys in mobile apps are likely to follow the same strategy for APIs developed internally. With an average of 40 APIs per mobile app with inhouse development, the combination of both types more than doubles the attack surface than with storing third-party API keys alone.

Storing API keys in mobile apps creates a massive attack surface for bad actors to exploit, signaling the need to protect against run-time threats.

A COMPETITIVE MARKET DEMANDS NEW FEATURES

Competitive market dynamics for retaining customers mean that organizations are emphasizing getting new features to market in their mobile apps—but lack the secure development practices to ensure security needs are met. See Figure 5.

Figure 5
Weak Security Practices for Mobile Apps and APIs
Percentage of respondents



Source: Osterman Research (2022)

For at least two out of five organizations:

- **Insecure apps are released to rush new features to market**
  Rushing a new feature to market is preferred over fixing known insecurities before doing so (at 50% of organizations).
- **Weak security processes for third-party developers**
  Third-party developers are not required to attest to following required standards (at 42% of organizations), penetration testing is not conducted to evaluate the security of third-party code (at 38% of organizations), and the security of third-party APIs is not vetted (at 35% of organizations).
- **Security processes for inhouse app and API development isn't any better**
  The weaknesses exhibited for third-party development of mobile apps and APIs are not much better for in-house approaches. In addition to the cultural preference of releasing insecure apps to rush new features to market, 41% of organizations lack the right level of security skills to develop and operate secure mobile apps and APIs, and 35% do not clearly communicate security policies to inhouse app and API developers.

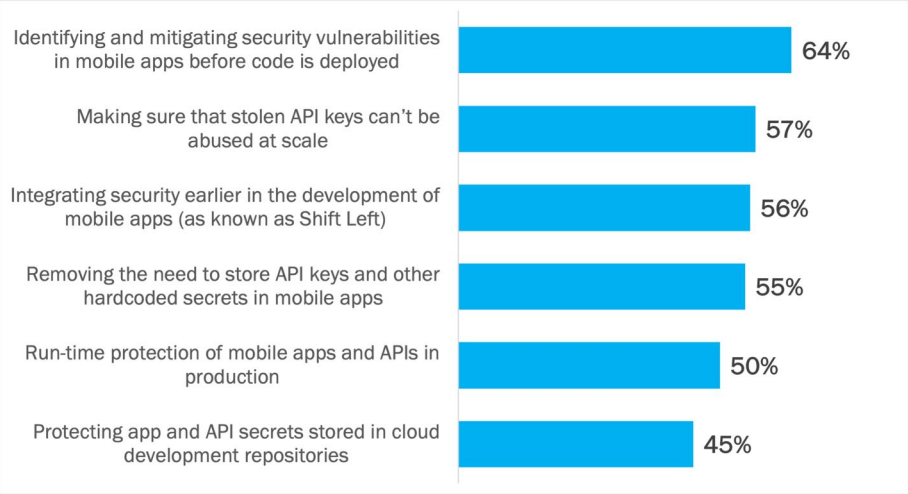
Given the current state of play with development processes in organizations, protecting against run-time threats is essential when known vulnerabilities persist in mobile apps and APIs and when the security posture of third-party code and APIs has not been tested, evaluated, or checked.

Two out of five organizations have weak mobile app and API security processes for both third-party and inhouse development approaches.

ORGANIZATIONS INDICATE HIGH PRIORITY FOR ADDRESSING RUN-TIME THREATS

Protecting mobile apps and APIs at run-time is an enduring requirement irrespective of how well security has been integrated into development processes. Mobile apps and APIs in production will be under attack regardless of how well the application was developed. While respondents indicate their organizations place the highest priority on secure development practices, protections against run-time threats are of high priority as well. See Figure 6.

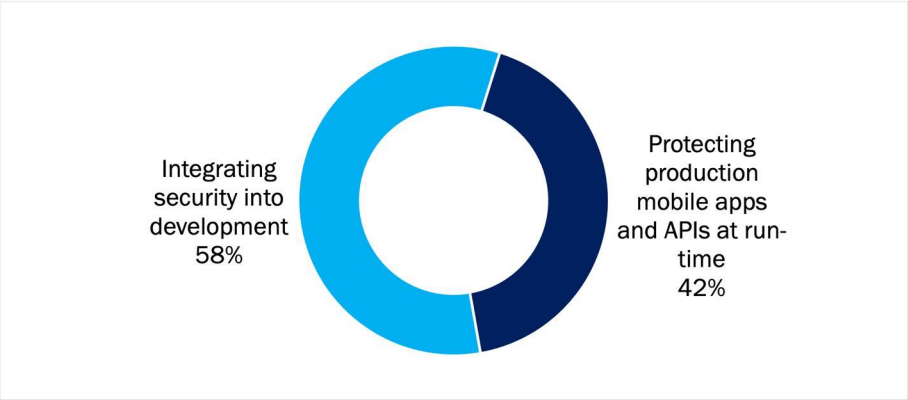
Figure 6
Priority of Various Security Strategies
Percentage of respondents indicating "priority" or "an extreme priority"



Source: Osterman Research (2022)

Respondents would allocate 42% of their security budget to protecting production mobile apps and APIs from run-time threats. See Figure 7.

Figure 7
Allocating Budget to Secure Mobile Apps and APIs
Average percentage of budget allocated by respondents



Source: Osterman Research (2022)

Mobile apps in production will be under attack regardless of how well an organization has incorporated security into development processes.

Conclusion

The importance of mobile apps and APIs to business success has grown rapidly in the past two years, yet many organizations lack visibility into and effective protections against a range of run-time security threats. Elevating secure development practices is important for every organization, but threats against mobile apps and APIs in production cannot be prevented by an over-reliance on Shift Left strategies. We recommend every organization reliant on mobile apps and APIs to immediately assess the efficacy of their solutions for run-time mobile security and take urgent action to address identified shortcomings.

About Approov

Approov solutions help stop API abuse at the edge and prevent security breaches in mobile channels. With more businesses moving to digitalization and future-ready services that utilize mobile API connections, securing those connections properly can get overlooked or not fully implemented for all possible threats, exposing organizations and their users to breaches, fraud, denial of service, and other forms of API abuse.

www.approov.io

@approov_io

Approov API Threat Protection provides a multi-factor, end-to-end mobile API security solution that complements identity management, endpoint, and device protection to lock-down proper API usage. It ensures that only safe and approved apps running in safe environments can successfully and securely access an organization's APIs, and turns away unauthorized accesses by attacker scripting, bots and fake or tampered apps.

Approov prevents the run-time attacks which are described in this report by identifying and blocking:

- API requests coming from mobile applications which have been copied, cloned, or modified in any way.
- API requests based on the result of security checks of the client environment: Potential risks include when emulators or frameworks are present, or where the OS has been jailbroken or rooted. What is acceptable is fully and dynamically configurable to allow for different use-cases (e.g., gaming apps vs. banking apps).

Approov also makes best-in-class security practices easy to apply and manage. Approov dynamically manages:

- Certificate pinning, thereby eliminating the threat of man-in-the-middle attacks of the channel between app and backend.
- API keys for owned or third-party APIs, in a way that eliminates any need to store them in app code, preventing them from being stolen or exploited.

Learn more at www.approov.io

Methodology

This report was commissioned by Approov. Osterman Research surveyed 302 security directors and mobile application development professionals in the United States and the United Kingdom during April 2022 on how their organization was addressing mobile application and API security threats.

DEMOGRAPHICS OF SURVEY RESPONDENTS

Geography	
United States	55%
United Kingdom	45%
Role	
IT and security	61%
Application development	39%
Industry	
Technology	23%
Healthcare	10%
Financial services, banking	9%
Consumer products	7%
Construction, architecture, engineering	7%
Food and beverage	5%
Manufacturing	4%
Education	4%
Energy, utilities, oil, gas, minerals, mining	4%
Logistics, transportation	4%
All other industries (nine types)	23%
Respondent Role	
CTO	32%
Application developer	24%
Security director or VP	17%
IT operations (e.g., admin, architect)	8%
Backend developer	8%
Software architect	7%
Security operations (e.g., analyst, architect, engineer)	2%
CISO	2%
Company Size	
Up to 100 employees	13.6%
101 to 250 employees	8.6%
251 to 500 employees	26.2%
501 to 1,000 employees	16.9%
1,001 to 2,500 employees	17.5%
2,501 to 4,999 employees	7.9%
More than 5,000 employees	9.3%

[1] Apple, App Store stopped nearly $1.5 billion in fraudulent transactions in 2021, June 2022, at https://www.apple.com/newsroom/2022/06/app-store-stopped-nearly-one-point-five-billion-in-fraudulent-transactions-in-2021/

[2] Engadget, Facebook reveals the AI tool it used to ban 6.6 billion fake accounts, March 2020, at https://www.engadget.com/2020-03-04-facebook-reveals-the-ai-tool-it-used-to-ban-6-6-billion-fake-acc.html

[3] Apple, App Store stopped nearly $1.5 billion in fraudulent transactions in 2021, June 2022, at https://www.apple.com/newsroom/2022/06/app-store-stopped-nearly-one-point-five-billion-in-fraudulent-transactions-in-2021/

[4] Akamai, Financial Services, Credential Stuff & Web Application Attacks, May 2021, at https://www.akamai.com/newsroom/press-release/-akamai-security-research--financial-services-continues-getting-