4GUYSCOFFEE

# Annual Cybersecurity Report

2024

## 1. Background & Scope

Amidst our global success in the coffee industry, 4GuysCoffee recognises the lurking potential for cyberattacks. As we have expanded into e-commerce, the online platform selling our products presents new vulnerabilities, particularly to digital skimming and its ilk. To fortify our defences, we're committed to a holistic cybersecurity approach.

This approach, encompassing employee training, continuous security assessments, robust encryption, and expert collaboration, aims to build resilience against evolving digital threats. This proactive report stems from our unwavering dedication to protecting 4GuysCoffee's digital assets. Herein, we'll dissect the tactics of common cybercrimes along with a couple of case studies, expose potential weaknesses in our system, and lay out concrete steps to avoid pitfalls like digital skimming. By embracing these preventative measures, we safeguard not only our digital storefront but also the trust and security of our cherished customers. This report serves as a blueprint for achieving this critical objective.

## 2. Attack Vector Landscape

### 2.1. Digital Skimming

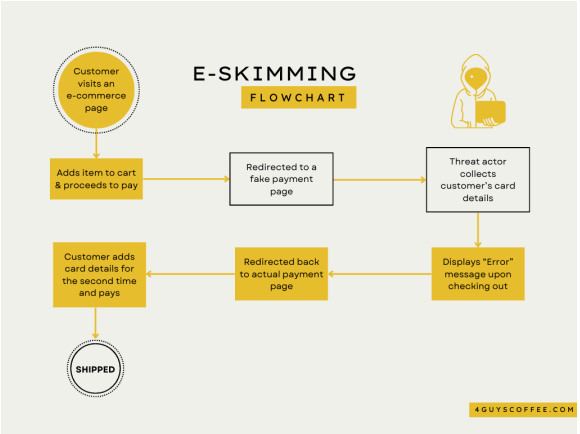
Visa's Biannual Threats Report of 2022 identified Digital Skimming as one of the upcoming Cybersecurity threats. Digital Skimming attacks involve cybercriminals injecting malicious code onto a merchant's website, primarily focusing on checkout pages to harvest payment account details and customers' personally identifiable information. These attacks often exploit misconfigurations or insufficient security controls in a merchant's environment, allowing threat actors to deploy the malicious skimming code successfully.

Digital skimming, also known as Magecart attacks, involves the covert insertion of malicious code into the payment processing pages of websites. This malicious code is designed to capture sensitive customer information, such as credit card details, during the online checkout process.

#### 2.1.1 Impacts & Consequences

As reported by Visa in 2022, its Payment Fraud Disruption (PFD) team identified an evolution to the pre-existing modus operandi. Threat actors can now place "a reverse shell dropper on the targeted eCommerce merchant's file system. Once a shell session has been initiated, the reverse shell (or 'connect-back shell') redirects the input and output connections of the victim's system, allowing the attacker remote control over the system. Once the attacker gains control over the victim's system, they append malicious digital skimming JavaScript code into the legitimate code of the victim's eCommerce

platform's checkout webpage. This malicious digital skimming code harvested payment account data as victims entered the data into the site's checkout fields. The malware harvested the victims' full PAN, expiration date, and cardholder information".[1]



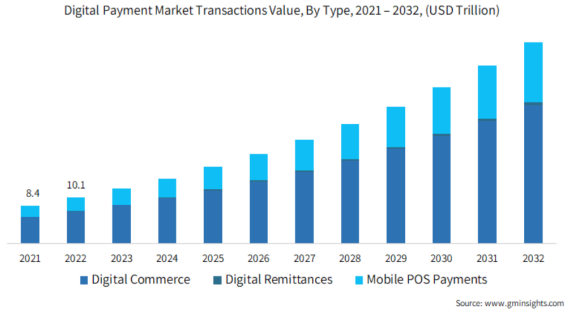

The consequences of a successful digital skimming attack can be far-reaching and devastating. They extend beyond financial losses, as they can erode customer trust and damage the reputation of our beloved brand.

For individuals, the primary concern is the theft of sensitive financial information, including credit card numbers, expiration dates, and CVVs. This could result in unauthorised charges, fraudulent transactions, and financial hardship for victims. Moreover, stolen payment card data can be used for identity theft, where criminals take on the victim's financial identity to open new accounts, obtain loans, or commit other fraudulent activities. This can significantly damage the victim's credit score and cause long-term financial problems.

On the other hand, it could slap the affected businesses with hefty fines and legal repercussions from regular payment card processors. Most notably, investigating and mitigating a skimming attack can be time-consuming and resource-intensive, disrupting business operations and potentially leading to revenue loss.

### 2.1.2 Trend Analysis

According to Allied Market Research, the projected Compound Annual Growth Rate (CAGR) for the digital payment market is set to be 17.2% by the year 2032.[2]




The market is experiencing significant growth driven by the widespread adoption of digital payments in online shopping. This surge is primarily attributed to time efficiency and convenience. Additionally, the market is propelled forward by the advent and ubiquity of smartphones, fast internet connectivity, a growing consumer preference for digital payments, and widespread acceptance of this payment method among merchants.
This increases the number of users exposed to e-skimming threats and contributes to the evolution of these threats. Unlike conventional methods, e-skimming attacks persistently intercept customer payment details during the point of purchase, making them challenging to

[1] VISA, rep., *Biannual Threats Report* (VISA, 2022), 9.

[2] Allied Market Research, rep., *Digital Payment Market Size, Share, Competitive Landscape and Trend Analysis Report*, Global Opportunity Analysis and Industry Forecast (Allied Market Research, 2023).

identify and often invisible to both customers and retailers. Most e-skimming incidents are only detected after weeks or even months of operation. The mean time to detect (MTTD) and mean time to respond (MTTR) for client-side security breaches are extremely long. Attackers have also integrated valid SSL certificates linked to domains delivering malicious code, creating the illusion of legitimate traffic and preventing customers from receiving mixed content warnings when the website blends trusted, encrypted content with unencrypted malicious content.

A recent report has detailed Magecart attacks in which misconfigured access controls on Amazon S3 buckets enabled attackers to append their skimmer code to existing JavaScript application code files.[3] This was made even easier with automated AWS S3 scanners that they have developed that enable them to detect misconfigured S3 buckets.

As explored earlier, magecart operators are well-known for their capacity to adjust and refine their strategies. In recent years, they have utilised 404 error pages –a standard feature on every website– to conceal and execute their malicious code designed for stealing credit card information. What distinguishes this method is its novel utilisation of the default '404 Not Found' page. As described by Akamai Security Intelligence in their report, "This concealment technique is highly innovative and something we haven't seen in previous Magecart campaigns."[4]

[3] DXC Technology, "As Online Shopping Grows, So Does The Risk of e-Skimming Attacks," n.d.

[4] Roman Lvovsky, rep., October 9, 2023, https://www.akamai.com/blog/security-research/magecart-new-technique-404-pages-skimmer.

### 2.1.3 Case Study: British Airways Magecart Attack

During the summer of 2020, British Airways (BA) experienced a sophisticated Magecart attack. Cybercriminals implanted malicious code into the airline's website, targeting the checkout page for online bookings and travel transactions. This code surreptitiously collected sensitive customer payment details, such as credit card numbers and CVVs.

The breach remained undetected for months, potentially affecting many travellers. Fortunately, upon discovery, BA promptly responded by shutting down the compromised website, investigating the breach, and informing affected customers. They worked diligently to contain the fallout by cooperating with payment processors to identify and nullify fraudulent transactions. Additionally, BA offered credit monitoring services to individuals affected by the incident. Here's a breakdown of the attack timeline:

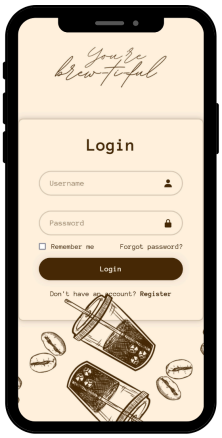
| | |
|---|---|
| **July 2020** | Hackers inject a Magecart skimmer into BA's website checkout page through a compromised JavaScript library used by a third-party customer service chat tool. |
| **July - September 2020** | Unbeknownst to BA or its customers, the skimmer silently captures payment information (credit card numbers, CVVs) entered during online bookings and travel purchases. |
| **September 2020** | Security researchers discovered the skimmer and alerted BA. |

| | |
|---|---|
| **September 2020** | BA promptly took down its website to contain the breach and investigated with a cybersecurity firm. |
| **September - October 2020** | The investigation confirms the Magecart attack and identifies the stolen data. BA publicly discloses the breach and advises customers to change their payment passwords. |
| **October - November 2020** | BA works with payment processors to identify and cancel fraudulent transactions made with stolen data. They also offer free credit monitoring services to affected customers. |
| **November 2020** | Law enforcement agencies launch an investigation into the attack. |
| **December 2020** | BA launches a new, secure website with enhanced security measures to prevent future attacks. |

Despite the swift response to the breach, it's undeniable that customer data was compromised, leading to significant repercussions for British Airways under GDPR regulations. Initially facing a fine of £183 million, the penalty was later reduced to £20 million. This incident underscores the peril digital skimming attacks pose to businesses.

### 2.1.4 A Cup of Trouble: How Magecart Attacks Could Brew for 4GuysCoffee

As the aroma of freshly roasted coffee beans fills our office, a chilling fact simmers beneath the surface – the potential for a Magecart attack to disrupt our cherished 4GuysCoffee experience. Just as British Airways faced a brutal data skimming attack, our login and checkout pages could become invisible honey traps, silently syphoning customer data, leaving a bitter aftertaste of fear and distrust.




The spectre of Magecart lurks in the shadows of compromised plugins or third-party scripts, injecting malicious code into our online haven. This digital gremlin, unseen by our customers, intercepts entered information – credit card numbers, CVVs, login credentials – brewing a potent storm of financial and reputational damage. The consequences stretch far beyond stolen data, with potential lawsuits, fines, and a tarnished brand image threatening to engulf our carefully crafted cup of comfort.

### 2.1.5 Suggested Controls & Mitigation

At 4GuysCoffee, security is not an afterthought. But the secret ingredient that keeps our virtual cup brimming with customer satisfaction. The rise of online skimming attacks serves as a cautionary signal for service providers and merchants. Magecart hackers are getting increasingly creative in developing JavaScript sniffers capable of compromising any e-commerce site lacking adequate security measures. Consequently, proactive steps must be taken to address this growing threat.

We recommend these industry-practised preventive measures:

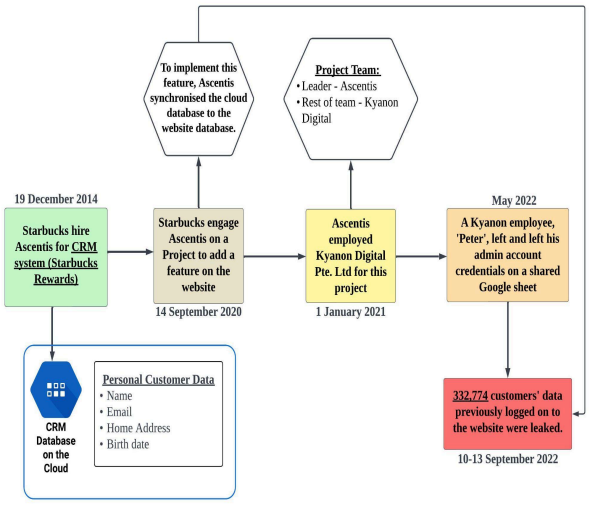
1. Regularly inspect the code for vulnerabilities.
2. Given that the recent attacks exploit misconfigured write permissions in widely-used CDNs such as our AWS resources, it is imperative to appropriately configure and limit secure access to these resources and the overall CDN implementations.
3. Employ a unified and secure configuration for all implementations to avoid inconsistencies.
4. Implement Web Application Firewalls (WAFs) to help block malicious code injections.
5. Implement proactive measures such as penetration testing to uncover vulnerabilities, timely patching to address gaps, and maintaining multi-layered security systems to thwart intrusions.

For enhanced security, merchants and service providers are strongly advised to utilise solutions management systems such as the Security Information and Event Management (SIEM). "Check-out Solutions" are also instrumental in these situations as they enable customers to input transaction information on a separate payment page, redirecting them away from the primary e-commerce site.

### 2.2 Starbucks Data Breach

In September 2022, around 330,000 Starbucks customers' data were leaked and put up for sale on an online forum. The coffee chain was only made aware of this leak three days later, and the affected customers were notified via email almost a week later. The affected customers had accounts and made online transactions on the website or the mobile application. The PDPA Act was violated. Information on the case was based on the report released by the Personal Data Protection Commission in 2023.

#### 2.2.1 Overview of Incident




- On 19 December 2014, Starbucks SG engaged the Organisation to develop, implement, support, and host a Customer Relationship Management system (the "CRM System") to support Starbucks SG's "My Starbucks Rewards" loyalty program (the "Rewards Program").
- When an individual signed up as a member of the Rewards Program, their personal data, including name, email address, telephone number, and birth date, was collected and stored on a cloud database (the "CRM Database").
- On 14 September 2020, Starbucks SG contacted Ascentis Pte. Ltd. on the website for the sale and purchase of products offered by Starbucks SG.
- On 1 January 2021, Ascentis Pte. Ltd. hired the services of Vietnamese tech organisation Kyanon Digital to provide additional manpower and software development support for the project.
- One of the features and project requirements was that the member's

personal data would be auto-completed when filling out the form - this led to having another copy of the customer database, which is hosted and operated independently from the cloud database, on the website platform.

- The project was controlled and managed by Ascentis Pte. Ltd., but Kyanon Digital employees carried out the work. The employees had accounts with administrator privileges for the website platform, including exporting data from the platform.
- In May 2022, one of the employees, 'Peter', left the company and left his admin account credentials on a shared Google sheet for the rest of the team. His account was not disabled, and the other employees continued using the account after changing the password to 'Kyanon@123456'.
- Sometime between 10 and 13 September, the malicious actor used Peter's admin account to grant admin access to other accounts, gather data, and export data to an external email address.
- In total, the personal data of 332,774 individuals comprising names, email addresses, dates of birth, the physical addresses of 181,875 individuals, and the telephone numbers of 310,560 individuals was breached in the incident.
- The data was then auctioned on an online forum on the dark web. The Singapore Computer Emergency Response Team was notified on 13 September 2022, and Starbucks SG and Ascentis Pte. Ltd. submitted data breach notifications to SGPDPC on 15 and 16 September 2022, respectively.

**2.2.2 Attack Vectors**

- Account Takeover - it was reported that the admin accounts only had single-factor authentication. Moreover, the login credentials passed on were not encrypted and shared with the entire project team on a Google document. Also, when the password was changed, although it met the requirements, it was predictable and included the company's name, making it more susceptible to attack.
- Distributed Data Storage - the data was replicated and stored in a database on the website, which was hosted and operated independently. This increases the attack surface significantly.
- Lack of Access Management - admin privileges were granted to all team members; hence, every team member had full access to the data and could modify it, export it, etc. An issue of roles
- Lack of encryption - the data stored on the platform's web server was not encrypted.
- Lack of Detection Measures - Ascentis Pte. Ltd. did not pick up on the data breach and incident until the SGCERT team was notified of the data being sold and auctioned on the dark web. No checks or alerts were raised, especially when an email was sent to an external email address, and other accounts were granted admin privileges.
- Lack of Security Policies - no proper exit clearance and procedures were enforced for 'Peter' with his account (with admin privileges) not being disabled after he resigned from the company.

### 2.2.3 Solutions

The case study above of Starbucks SG's customer data breach is highly applicable and relevant to our coffee business, which has an online store and a member system. By analysing the case study and identifying the vulnerabilities that have been or could have been exploited by malicious threat actors, we have devised the following solutions to mitigate the risks involved.

- Security Policy - this relatively broad area enforces information security and generalises the attack surface to comply with laws and regulations. One of the policies would be to have Multi-Factor Authentication as a requirement for the administrator accounts. This would validate that the person accessing the admin accounts is true.
- Secondly, password hygiene that does not include anything relevant to the company should be enforced for added security.
- The principle of least privilege should be exercised. This can be facilitated further by the project lead defining the roles and responsibilities of each team member. Hence, a suitable level of access rights can then be given to each member.
- To enhance Organisational Security, a proper exit clearance and procedure must be implemented. This ensures that exiting employees will have their accounts disabled to prevent unauthorised usage and access.
- A proper detection system should also be in place to monitor any unusual activity to minimise the risk of a zero-day attack, which occurred in the case study.
- A single database system should be used as it reduces the web application's attack surface, and it is easier to manage the transactions in the database, i.e., any database changes or queries made.
- If a distributed database has to be used, then authentication and authorisation should also be enforced. Certain actions for certain people only should be allowed based on the principle of least privilege. Data encryption in the databases and the backup should be done to ensure confidentiality.
- Regular data edits should also be conducted to review the IT infrastructure and minimise vulnerabilities continuously.

## References


1. Allied Market Research. Rep. *Digital Payment Market Size, Share, Competitive Landscape and Trend Analysis Report*. Global Opportunity Analysis and Industry Forecast. Allied Market Research, 2023.

2. DXC Technology. "As Online Shopping Grows, So Does The Risk of e-Skimming Attacks," n.d.

3. Lvovsky, Roman. 2023. Review of The Art of Concealment: A New Magecart Campaign That's Abusing 404 Pages. Akamai Security Intelligence. https://www.akamai.com/blog/security-research/magecart-new-technique-404-pages-skimmer.

4. VISA. Rep. *Biannual Threats Report*. VISA, 2022.

5. PERSONAL DATA PROTECTION COMMISSION, 2023. SGPDPC 10, Case No. DP-2209-C0193 / DP-2209-C0217. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/GD_Ascentis_12092023.pdf