



Centrale Bank van Aruba

Scams & Fraud in Digital Payments in Aruba

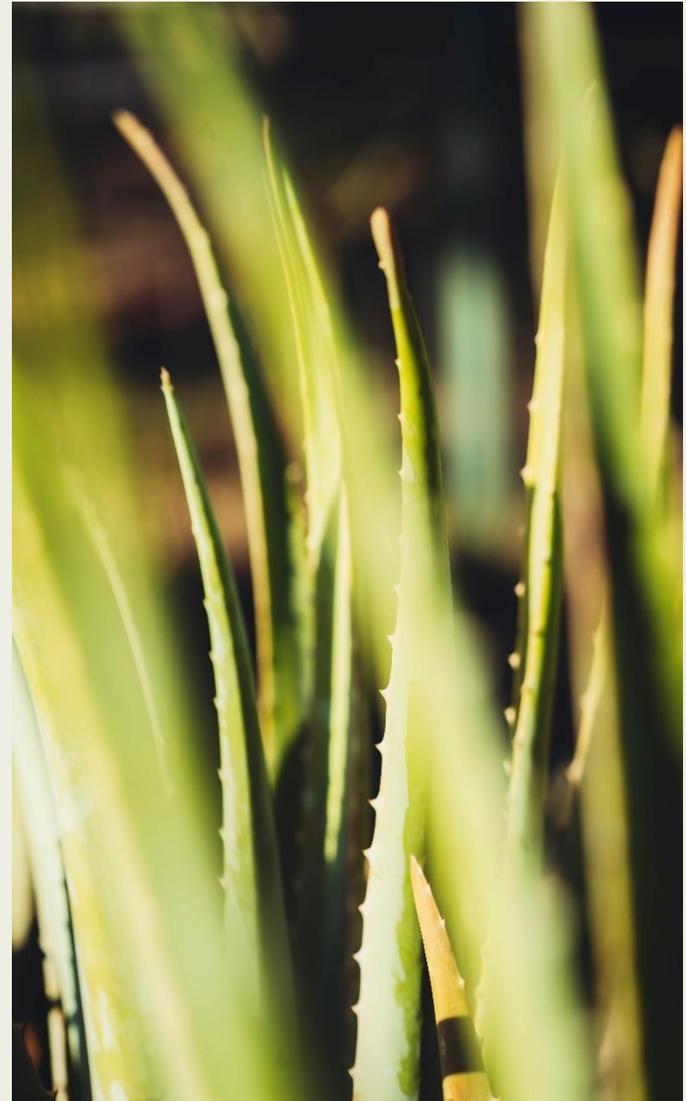
Report published in March 2026



Abstract

Scams and digital fraud in payments are not yet common in Aruba, but a small group, particularly senior citizens, faces repeated threats, making them the most vulnerable among all age groups.

In 2024, the Centrale Bank van Aruba (CBA) conducted a survey covering consumers' experiences and encounters with scams or digital fraud related to payments in Aruba, and common patterns and the frequency of fraudulent activities. This survey revealed that while such incidents are not yet widespread in Aruba, a vulnerable minority, particularly senior citizens, faces repeated threats. All age groups encountered scams and digital fraud, but senior citizens show the highest risk of recurring victimization. Scammers predominantly target credit and debit card users, with small financial losses being more frequent, though significant losses still occur. Victims often respond proactively by contacting their commercial banks or payment service providers to seek reimbursement, yet delays and gaps in reimbursement persist. Encouragingly, user awareness is growing, with many adopting preventive behaviors such as avoiding suspicious emails, unknown calls, and monitoring bank statements. However, basic digital security practices like updating passwords and enabling two-factor authentication remain underutilized, highlighting areas for improvement in personal cybersecurity habits.



Contents

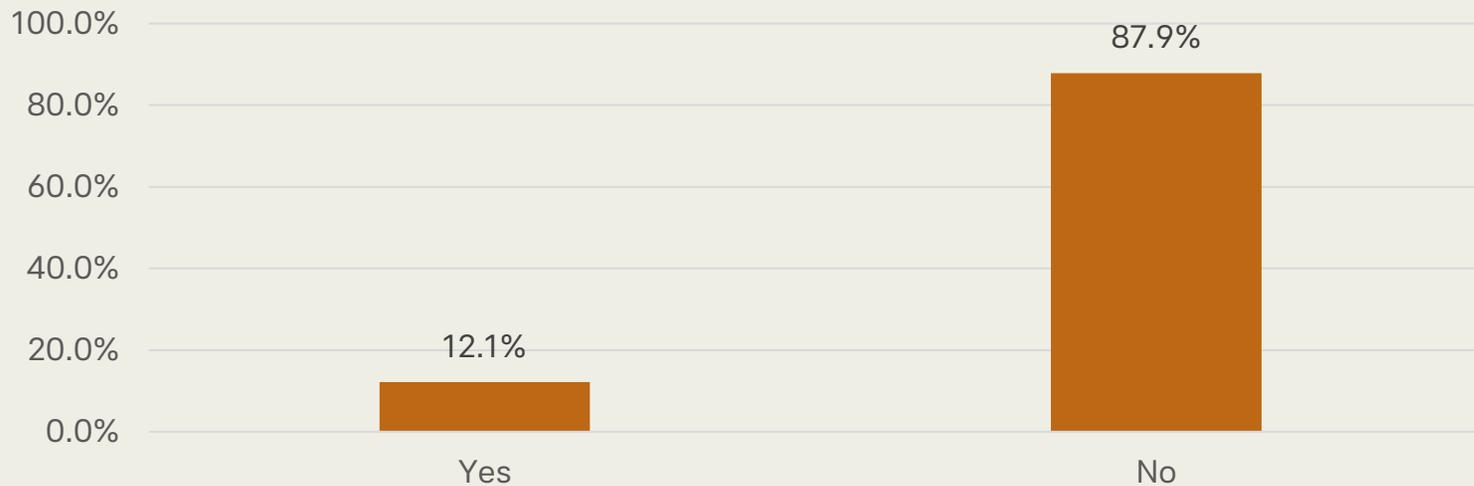
Abstract	2
I. Scams and digital fraud encounters.....	4
Percentage of scams and digital fraud encounters	4
II. Victims of scams and digital fraud	6
III. Patterns observed	7
Repeated scam vulnerability	7
Preferred methods of scammers	8
Losses caused by scams and digital fraud.....	9
IV. Reimbursement process	10
Time to reimbursement.....	12
V. Awareness and proactive measures	13
Awareness	13
Proactive measures	14
VI. Communication channels used by scammers.....	15
VII. Concluding remarks	16

I. Scams and digital fraud encounters

Percentage of scams and digital fraud encounters

The scams and digital fraud in payments survey conducted by the CBA, in collaboration with Foro di Pago Nacional (FPN) stakeholders, in 2024 measured, among others, the percentage and frequency of scams and digital fraud encounters in Aruba by residents of Aruba in the past 12 months. The findings indicate that scams and digital fraud in payments are still relatively uncommon in Aruba, with 87.9 percent of respondents reporting no such encounters in the past 12 months (chart 1).

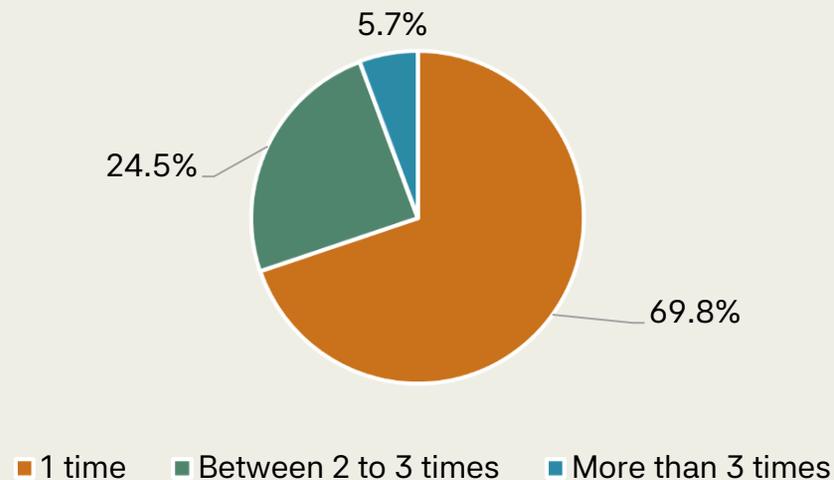
Chart. 1 Percentage of scams and digital fraud encounters



Frequency of scams and digital fraud encounters

While most victims experienced scams or fraud only once in the past 12 months (69.8 percent), a smaller group was repeatedly targeted, with 24.5 percent encountering scams two to three times and 5.7 percent more than three times (chart 2). This could imply that certain individuals are more vulnerable or that some scams are particularly persistent.

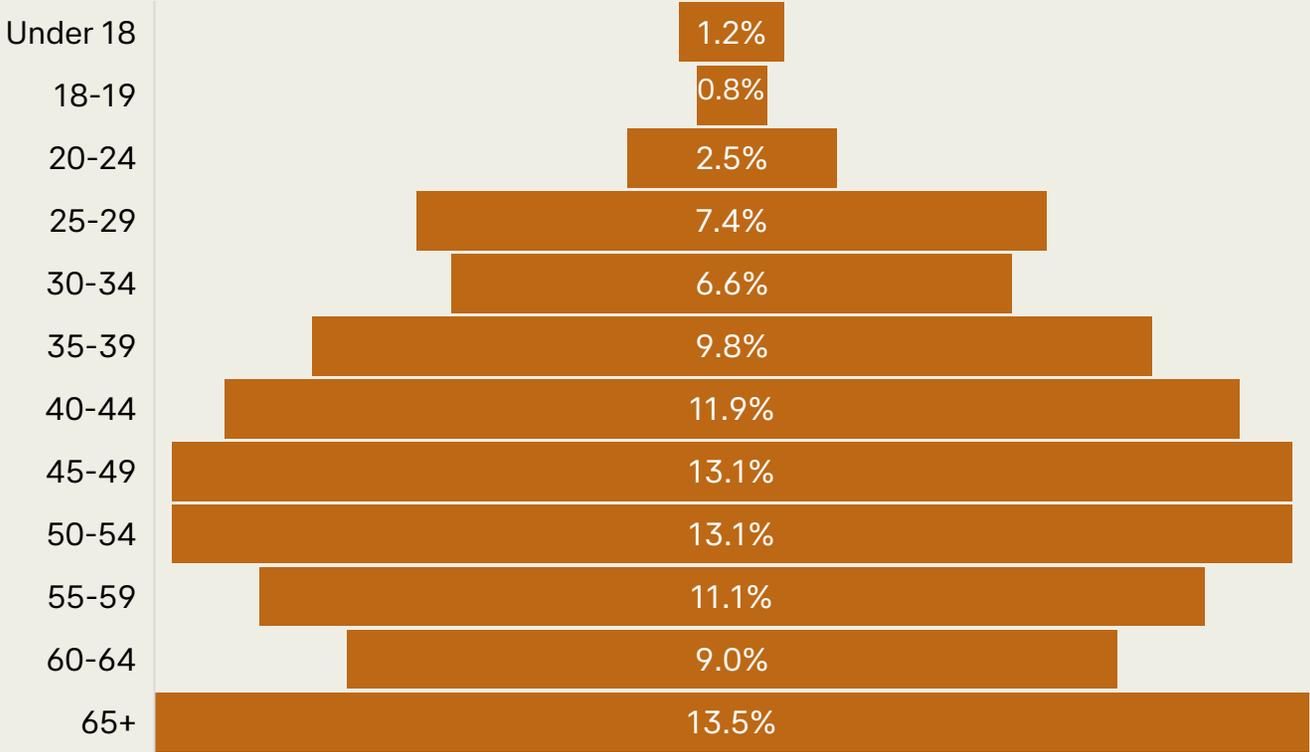
Chart 2. Frequency of scams and digital fraud encounters



II. Victims of scams and digital fraud

In addition, the survey results indicate that all age groups were affected by scams and fraud in the past 12 months. However, senior citizens (65+) as well as individuals aged 45-49 and 50-54 years were targeted more frequently by scammers (chart 3). This highlights the need for targeted awareness and support initiatives for this group to mitigate the higher risk.

Chart 3. Victims of scams and digital fraud by age

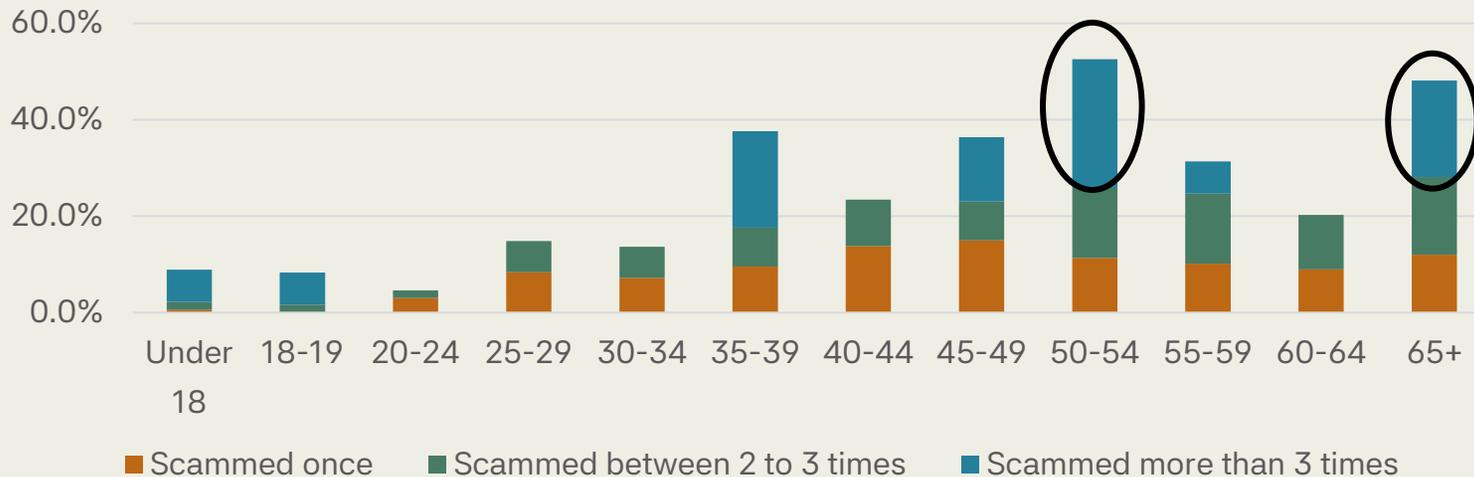


III. Patterns observed

Repeated scam vulnerability

The survey results uncover distinct patterns in how scams and digital fraud are emerging in Aruba. Chart 4 presents the patterns observed with respect to scams and fraud by age category. The data shows that older citizens are more vulnerable to repeated scams than younger age groups, with e.g., respondents aged 50 to 54 and 65+ reporting the highest rates of being scammed more than three times. This finding reiterates the need for targeted awareness, education and support initiatives by commercial banks, the CBA, payment service providers (PSP), and other key stakeholders to help older citizens recognize scams and fraud and hopefully prevent them from being victimized by scammers.

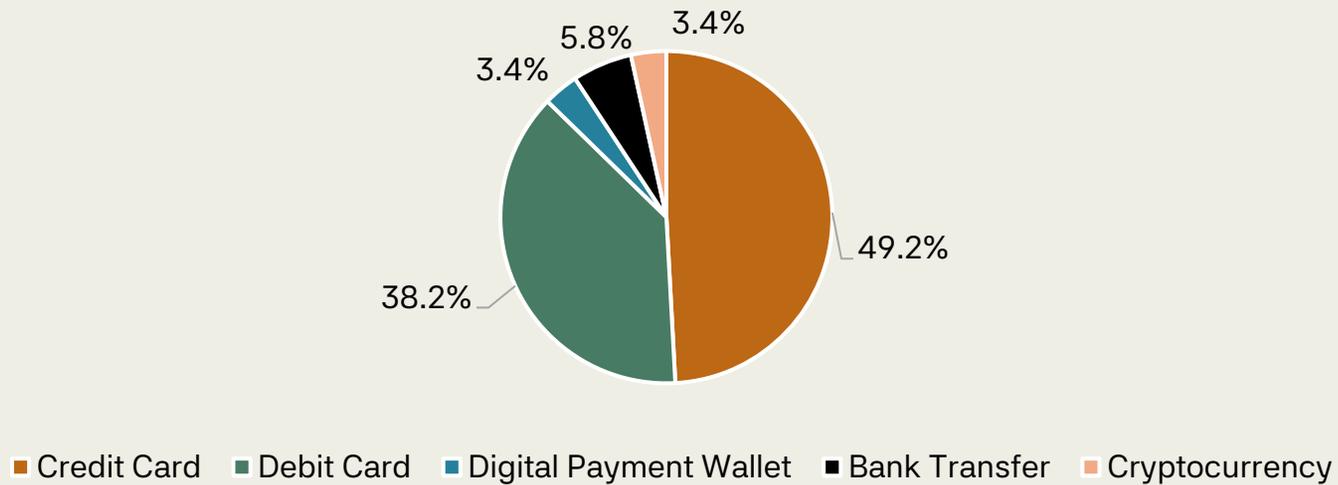
Chart 4. The patterns and risks of multiple scam and fraud incidents across age groups



Preferred methods of scammers

When diving into the payments methods used by scammers, the survey results indicate that credit cards (49.2 percent) and debit cards (38.2 percent) are the most commonly used methods in scams and digital fraud in Aruba (chart 5). While digital wallets (3.4 percent), bank transfers (5.8 percent), and cryptocurrencies (3.4 percent) are less frequently targeted by scammers, they still pose a risk. These findings underscore the need for robust security measures and vigilance across all payment methods to protect against scams and fraud.

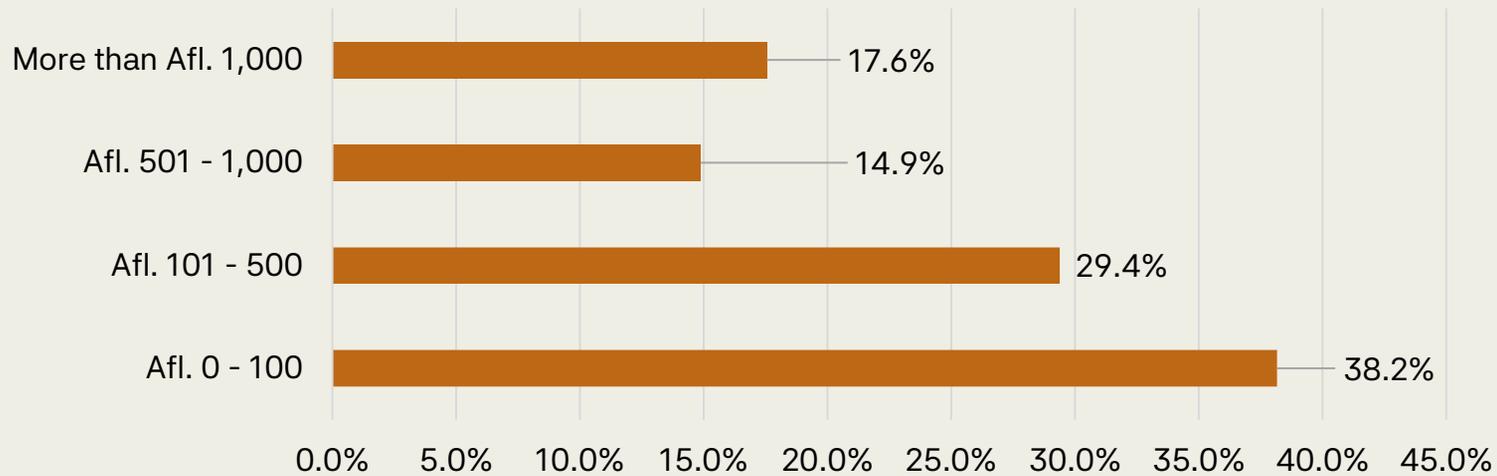
Chart 5. Payment methods involved in scams and digital fraud



Losses caused by scams and digital fraud

Chart 6 reveals that the majority of losses due to scam or digital fraud in payments in Aruba are relatively small, with 38.2 percent of incidents involving losses between Afl. 0 – 100. However, losses involving higher amounts are still prevalent, with 32.5 percent of cases involving amounts over Afl. 500. This highlights the importance of being vigilant and taking preventive measures to protect against fraud, regardless of the amount at risk.

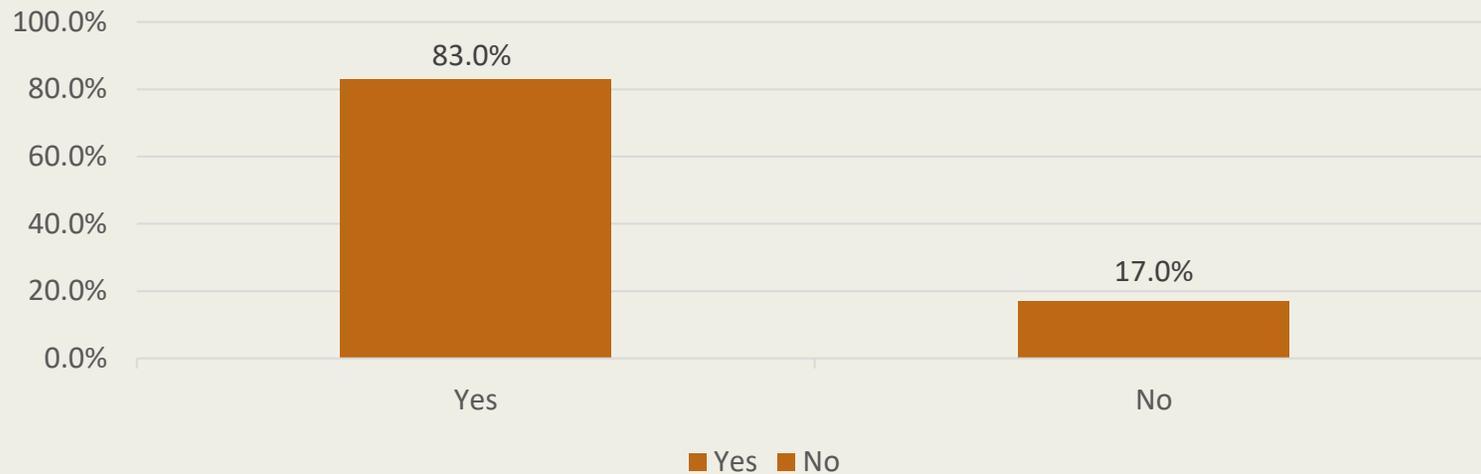
Chart 6. Total amount of money lost



IV. Reimbursement process

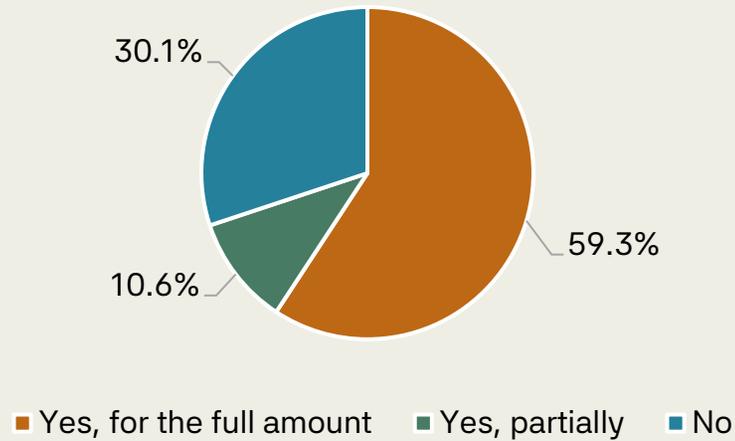
Fortunately, banks and payment service providers have established reimbursement procedures to support victims of scams and digital fraud, offering a crucial safety net in times of financial distress. The survey results indicate that a great majority of respondents (83.0 percent) have contacted their bank or payment service provider to request a reimbursement after experiencing fraud (chart 7). However, 17.0 percent of respondents have not reported their fraud encounters, highlighting a need for greater awareness about the benefits of reporting scams and digital fraud, both to recover lost funds and to help prevent future incidents.

Chart.7 Rate of victims that requested a reimbursement



Furthermore, chart 8 provides insight into the effectiveness of the reimbursement process. While 59.3 percent of victims received full compensation and 10.6 percent received partial reimbursement, a concerning 30.1 percent did not recover any funds (chart 8). This highlights a significant gap in financial recovery support, underscoring the need for more consistent reimbursement mechanisms.

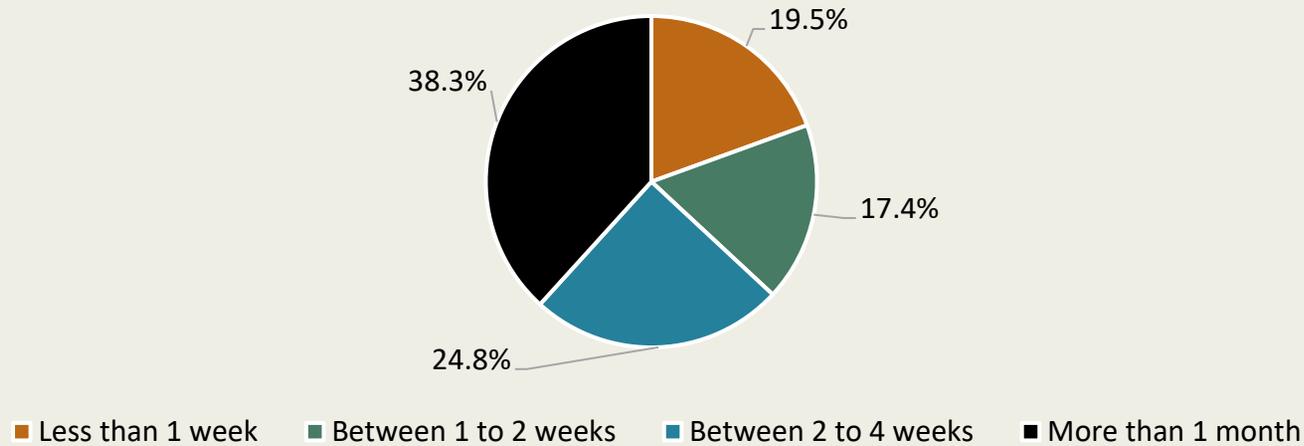
Chart.8 Reimbursement rates



Time to reimbursement

In addition to examining the effectiveness of the reimbursement process, the survey also delved into how efficiently victims are reimbursed, an area that directly impacts trust in financial institutions. Chart 9 breaks down the time it takes to get a reimbursement, revealing significant variation in the process. While 19.5 percent of victims were reimbursed in less than a week, with 93.1 percent of them receiving the full amount, a much larger share, 38.3 percent, had to wait more than a month. Additionally, 24.8 received their funds back within 2 to 4 weeks, and 17.4 percent within 1 to 2 weeks. These findings suggest that while some victims benefit from swift resolution, the process can be lengthy for many, pointing to an area for improvement in fraud response and support systems.

Chart.9 Time to reimbursement

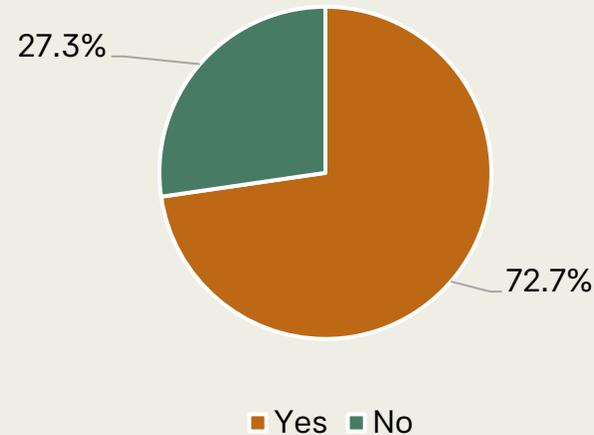


V. Awareness and proactive measures

Awareness

The survey results reveal that a significant majority (72.7 percent) of respondents are aware of the risks associated with scams and digital fraud in payments (chart 10). The fact that a significant number of respondents are aware of the risks linked to scams and digital fraud indicates a strong level of public vigilance. This awareness creates a solid foundation for encouraging safer payment behaviors and timely reporting. However, the remaining 27.3 percent still represent a vulnerable group that should be reached by commercial banks, the CBA, PSP's, and other key stakeholders through targeted communication and support.

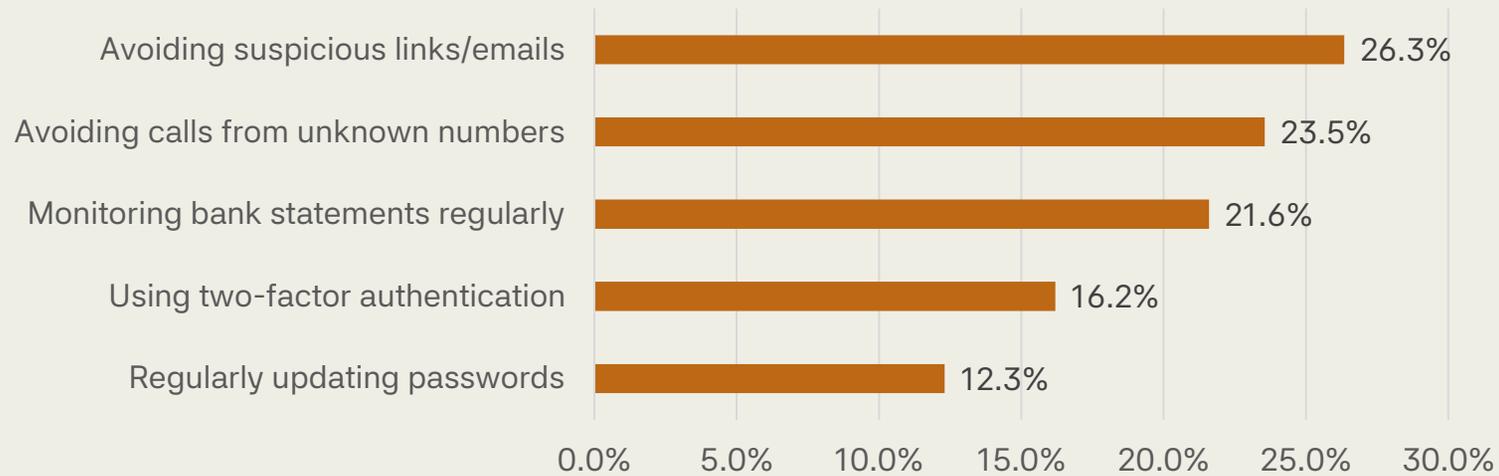
Chart.10 Percentage of respondents aware of the risks



Proactive measures

Among those taking proactive steps to protect themselves from scams and digital fraud in payments, 26.3 percent do so by avoiding suspicious emails and links, 23.5 percent by avoiding calls from unknown numbers, and 21.6 percent by monitoring bank statements regularly. In contrast, regularly updating passwords is the least adopted measure (12.3 percent), suggesting that some basic security habits are still overlooked. Using two-factor authentication is the second least adopted measure to prevent scams and digital fraud in payments. These findings highlight the need for continued education and awareness campaigns by commercial banks, the CBA, PSP's, and other key stakeholders to ensure everyone understands the importance of digital security in payments. This is essential for the continued growth and adoption of digital payment technologies.

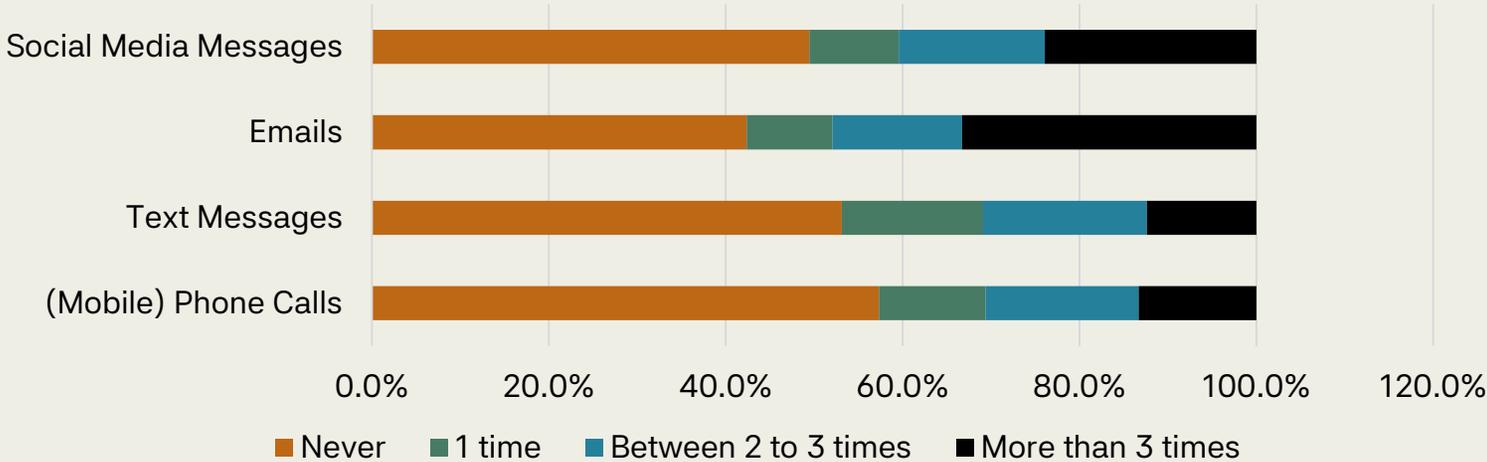
Chart.11 Proactive measures by respondents



VI. Communication channels used by scammers

The results of the survey indicate that although most respondents never received scam communications through any channel, those who were repeatedly targeted were primarily contacted via email and social media messages (chart 12). This pattern underscores the need for heightened vigilance across digital communication platforms to better protect users from persistent scam attempts.

Chart.12 Type and frequency of communication of scams and fraud



VII. Concluding remarks

While scams and digital fraud in payments are not yet common in Aruba, a small but significant group continues to face repeated threats, particularly older citizens, who remain the most vulnerable across all age groups. The preference of scammers for credit and debit cards highlights the need for vigilance in everyday financial activities. Although most losses tend to be small, the presence of larger financial impacts cannot be overlooked. Encouragingly, victims are taking action, but delays and gaps in reimbursement processes remain a concern. The growing awareness and proactive behavior among users are positive signs, yet the persistent threats via social media and email platforms underscore the importance of continued education and robust protective measures to safeguard all citizens, especially the elderly. Therefore, there is a clear call to action for commercial banks, the CBA, PSP's, and other key stakeholders to make meaningful contributions toward ensuring safe and secure payments for all. All three parties must work together to share data, track emerging threats, and maintain vigilance, because while scams can never be completely eliminated, proactive measures and collaboration are essential to keeping payment systems safe and trustworthy.

Some examples of possible initiatives are among others:

- Commercial banks should educate their customers, especially older citizens who are most vulnerable, on how to recognize and avoid scams, while also offering support services such as financial literacy programs, help lines, and assistance with recovering losses.
- Payment service providers should ensure strong security by using tools like multi-factor authentication and continuous monitoring of transactions, as well as providing easy-to-access fraud support for users.
- The CBA could coordinate nationwide awareness campaigns to promote safe digital payments.

CENTRALE BANK VAN ARUBA

J.E. Irausquin Blvd. 8

P.O. Box 18

Oranjestad, Aruba

Phone: (+297) 525 100

© Centrale Bank van Aruba 2025

All rights reserved.

