Card Testing/Payment Fraud

Card testing, also known as carding or payment fraud, is a fraudulent activity where cybercriminals use stolen credit card information to make small purchases or transactions to verify if the card is still active and valid. The bad actors know they can use the card for larger fraudulent purchases if successful transactions happen.

How Card Testing Works:

Obtaining Card Information: Fraudsters acquire stolen credit card information from data breaches, phishing attacks, or the dark web.

Testing the Card: They make small, low-value transactions online or in person to see if the card is valid and active.

Analyzing the Results: If the transactions are successful, the fraudsters proceed to make larger purchases or sell the verified card information.

Performing Card Testing in a Small Restaurant Setting:

Employee Involvement: An insider, such as an unscrupulous employee, might be involved in processing unauthorized small transactions using stolen card details.

Small Purchases: The fraudster may order inexpensive items or services, testing multiple cards to avoid detection.

Automated Systems: In some cases, fraudsters might use automated scripts or bots to quickly test a large number of cards.

Example Scenario:

1. **Insider Threat:** A waiter or cashier has access to the restaurant's Point of Sale (POS) system. They can manually enter stolen card details for small transactions (e.g., a coffee or dessert) to test the cards.
2. **Suspicious Patterns:** The fraudster might make multiple small transactions in a short period, which can be a red flag for card testing activity.

Preventive Measures:

Employee Background Checks: Conduct thorough background checks on employees to reduce the risk of insider threats.

Monitor Transactions: Implement real-time monitoring and alert systems to detect unusual transaction patterns, such as multiple small transactions in a short time frame.

Limit Manual Entry: Restrict manual entry of credit card information to minimize the risk of unauthorized transactions.

Educate Staff: Train employees to recognize and report suspicious behavior or transactions.

Use Advanced Security: Employ advanced security measures like EMV (chip) technology and tokenization to protect card data.

Regular Audits: Conduct regular audits of transactions to identify and address any suspicious activity promptly.

According to kount.com, although card testing transactions may involve small amounts, these minor losses can accumulate rapidly. If a cardholder notices an unauthorized charge, it could result in a chargeback. Even if the transaction is declined, you still incur processing fees. Either way, you're losing money, which could be avoided by preventing card testing in the first place.

By understanding the mechanisms of card testing and implementing preventive measures, small restaurants can protect themselves and their customers from payment fraud.

References

Ackley, M. (2023, April 11). Card testing fraud: What you need to know. Kount. Retrieved August 10, 2024, from https://kount.com/blog/card-testing-fraud