Fight the fraud

Top 5 financial fraud attacks and how to prevent them

Due to the high reward associated with the financial industry, digital banking and payments will always be at risk for fraud. Criminals are smart at evolving their tactics, too. Squash one type of fraud, and another simply pops up in its place.

Unfortunately, the implications for businesses are far-reaching – from immediate financial loss to long-lasting reputational damage. Only strong fraud prevention measures can save businesses from a world of pain.

01. Phishing

The ploy:

Fraudsters obtain their victims' email and/or phone number. Posing as a legitimate entity, they convince their victims to click on a link and enter their credentials and potentially an SMS OTP. These are captured and used to log into a victim's real account and defraud them.

What to do:

Require customers to enable multi-factor authentication (MFA) on all sensitive transactions. Educate them to not click on unexpected or suspicious-looking links.

Prevalence of fraud

Linked to:

02. SIM-swap fraud

The ploy:

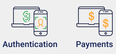
Armed with victims' personal credentials, fraudsters call a mobile network operator (MNO) and, posing as the customer, request a SIM swap. Once the new SIM card is active, all SMS OTPs are delivered to the fraudster's device, allowing them to verify transactions.

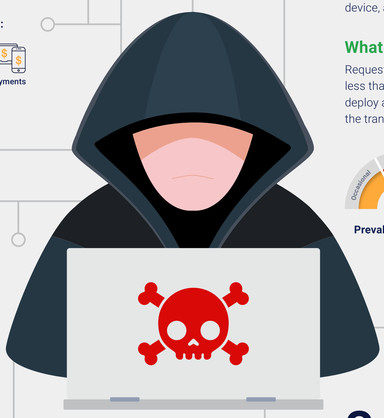
What to do:

Request a SIM info check from the MNO. If the card is less than two days old, flag the transaction and either deploy additional authentication measures or decline the transaction.

Prevalence of fraud

Linked to:





03. Social engineering

The ploy:

Posing as a bank's employee, for example, fraudsters contact their victims and convince them to participate in a security check – usually a challenge message. Once the victim has actioned the request or provided an OTP, the fraudster logs into their victim's bank account.

What to do:

Implement behavioral biometrics with more advanced risk signals. Update challenge messages to be more specific and educate customers about these tactics.

Prevalence of fraud

Linked to:

04. Chargeback fraud

The ploy:

Fraudsters buy goods online using stolen credit card details. Once goods are received, they apply for refunds. The victim's bank balance remains neutral and, if they don't check their credit card statements, the activity goes unnoticed.

What to do:

Implement a certified 3D Secure challenge flow. Improve transaction confirmation messaging, explicitly stating what was spent and where.

Prevalence of fraud

Linked to:

05. Triangulation fraud

The ploy:

Using a fake site, fraudsters advertise items at discounted prices. Victims place orders using their credit cards, and the fraudster then buys and ships the item to the customer. The customer asks no further questions, and the fraudster retains the credit card details for future use.

What to do:

Implement a certified 3D Secure challenge flow. Use more descriptive messaging during authentication challenges.

Prevalence of fraud

Linked to:

Entersekt can help you navigate this complex fraud landscape

Our proven fraud-prevention technology is relied upon by financial institutions all over the world to not only eliminate these five and all other types of fraud, but improve the overall customer experience. No more managing multiple vendors either. All you need is Entersekt, and you're in.

Book a demo today to see this technology in action.

Click here ›

entersekt and you're in.

entersekt.com