

BANK OF ISRAEL

Office of the Spokesperson and Economic Information

November 19, 2023

Boosting **data security, cyber protections, and business continuity**

in the Payment Cards Transaction Chain, Especially During the Gaza War

Payment by card no longer means swiping your card at the Point of Sale (POS), or even dipping or tapping it at the POS. The established well-accepted strategic advantage of the card industry, a huge deployment of POS terminals that enable card acceptance at most businesses, has become outdated. In Israel and across the world, the market share of transactions deemed "Card Present (CP)" has decreased tremendously. Card Present (CP) transactions occur when the physical device – a plastic card, smart phone or smart watch – touches or almost touches the POS terminal. In contrast, the market share and volume of transactions that are deemed "Card Not Present (CNP)" has grown tremendously. Card Not Present (CNP) transactions occur when the card number and other identifying information, known as credentials, are saved somewhere securely in the cloud, and there is no need for physical proximity to a POS terminal when making a payment. In Israel and elsewhere, for years now, we have more Card Not Present (CNP) volumes than Card Present (CP) volumes. In other words, the volume of truly digital card payments now exceeds physical card payments, and the gap grows every year.

For clarity, in our new digital environment, Card Not Present (CNP) does not necessarily mean the customer does not physically visit the business where she is making a payment. For example, in Israel, fuel chains have launched mobile applications that enable customers to securely save their card credentials in the app, and pay by card using their phone's geolocation technology, e.g., GPS coordinates. One user experience I love goes like this: I pull my car in to the gas station, next to a fuel pump, open the fuel chain's mobile app in my phone, based on the phone's GPS coordinates it detects my location and identifies the specific gas station where I arrived, generates a one-time code on my app, I enter that code in the fuel pump, and then fill my gas. The fuel chain charges my card, whose credentials I saved in the app, but I do no not need to touch or tap a POS terminal with my card or mobile phone. It's all done securely in the cloud, with various technology systems communicating in the back end. Similar examples abound in other verticals, such as parking, dining, food delivery, entertainment and more.

In other words, even in physical verticals that require the customer's physical presence to receive a product, service, or experience, the payment flow has migrated to a digital environment and from a payments perspective, it takes place virtually.

In order for the digital environment to function seamlessly, though, multiple technology providers are required. They have all kinds of roles – payment gateways, payment aggregators, software providers, wallet providers, shopping cart vendors, reconciliation providers, token issuers, closed loop payment processors, technology integrators, Internet Service Providers (ISPs), and more. Each of these players provides a unique and important service, without which, in most cases, a digital card transaction would not work well. Notably, though, many of these technology providers are not regulated or supervised. That comes in contrast to legacy players in the cards eco system that are regulated or supervised, such as payment card issuers, mostly banks; merchant acquirers, many of which were formerly subsidiaries of banks; and payment systems, also known as card switches, in the payment card space. Over the years the regulated or supervised legacy players have become more technologically savvy and capable, but still often find themselves reliant on the new unregulated technology vendors in the payment card eco system.

The consumer who seeks to make a payment, and the business that seeks to receive a payment, don't know or really care about all the players in the middle. They just want the payment to work, they want the payment processing service they receive to cost as little as possible, they want the payment flow to move as quickly and conveniently as possible, and they want to be assured that the transaction and all its data are kept secure. But the end-to-end transaction chain, from the moment the consumer initiates a payment on a mobile app, a website, a POS terminal, or otherwise, to the moment the business receives payment in its bank account, contains multiple players, some of which are regulated and some of which are not. Those that are not regulated create exposure and risk that bad actors may seek to exploit, by capturing sensitive transaction data and using it to achieve financial gain or other geopolitical goals. While unregulated players in the payment chain often implement cybersecurity measures as a good business practice, uniform regulatory or supervisory requirements will likely increase levels of security in the eco system.

In May earlier this year, I spoke on a Cyber Security Panel titled “Operational reliability, the challenge of cyber,” at Global Payments Week ([https://www.worldbank.org/global-payments-week-2023](https://www.worldbank.org/en/events/2023/05/15/global-payments-week-2023)) , a week-long gathering hosted by @The World Bank, for central bankers who fill the roles of payments regulators, supervisors, and/or operators. Well before the deadly October 7th attack by Hamas on Israel, and well before the war that ensued, I shared a perspective that locally is intuitive to all of us: in Israel, cybersecurity is not only a matter of independent bad actors seeking financial gain, but also a matter of immoral nation states, terror organizations, and in some cases governments or government entities, seeking to achieve geopolitical or security goals. In some cases a bad actor may seek simply to disrupt the ordinary course of life in enemy territory, creating damage and confusion where possible. In such scenarios, bad actors stealing individuals' transaction histories and personal details, or diverting businesses' incoming payments to other payees, might benefit from financial gain, but they are much more highly motivated by adversarial ideology whose limits go far beyond financially motivated hackers. Central bank representatives from other countries, especially where geopolitical conflicts have flared up, shared that they see similar phenomena in their jurisdictions.

It was in this context last week that we announced that participants in the Payment Cards Committee that we lead, agreed on a set of standards in the areas of cybersecurity, information security, and business continuity, which will apply to players in the Israeli payment card eco system. The standards include simple things like completing assessment questionnaires and appointing internal officers responsible for relevant areas, as well as more challenging tasks like implementing business processes and criterion for preventing and managing things like denial of service (DDOS) attacks, collaboration with the @National Cyber Directorate, performing development with scanning and code standardization from a security perspective, engaging in annual penetration testing, and much more.

We published our formal announcement on this initiative in Hebrew and English.  Here is a link to the English version: [https://www.boi.org.il](https://www.boi.org.il/en/communication-and-publications/regular-publications/overview-of-the-payment-and-settlement-systems-red-book/e19-11-23/)

And the standards we announced appear in English here: <https://www.boi.org.il/media/21zn0zc0/information-security-and-cyber-protection-standards-document1.docx>

Especially for small unregulated entities, implementing these new standards can require significant time and resources. For this reason, the standards will become binding one year from publication. Still, cognizant of the potential for increased cybersecurity threats to the Israel economy during the current ongoing Swords of Iron War in the Gaza Strip, as the Bank of Israel, we called on all players in the payments in the eco system to review the standards and implement whichever of them are possible, with all due speed. Sometimes "quick wins" in this regard are achievable with minimal effort, through increased awareness and implementation of initial simple steps. Through this two-pronged approach, prompting all members of the card payment eco system along the transaction chain to pursue immediate implementation where possible, and requiring them to launch the process for full implementation within a year, we aim to achieve increased resilience for the Israel market during our period of national emergency.

An important note about the Israel Payment Cards Committee that we lead: on the same Cyber Security Panel where I spoke at Global Payments Week ([https://www.worldbank.org/global-payments-week-2023](https://www.worldbank.org/en/events/2023/05/15/global-payments-week-2023)), I noted that far more important than rules and procedures is the need to cultivate a culture of cooperation, collaboration and urgency in the event of cyberattacks, including among competitors and regulators. In the background of the geopolitical environment in which we operate, in this sense, we are pleased and proud of the Israeli payment cards eco system, duly represented in the Payment Cards Committee. While at times they hold conflicting interests, when it comes to cybersecurity and business continuity, we are lucky to have the culture of cooperation that we expect – yet another benefit of the robust Israel market.