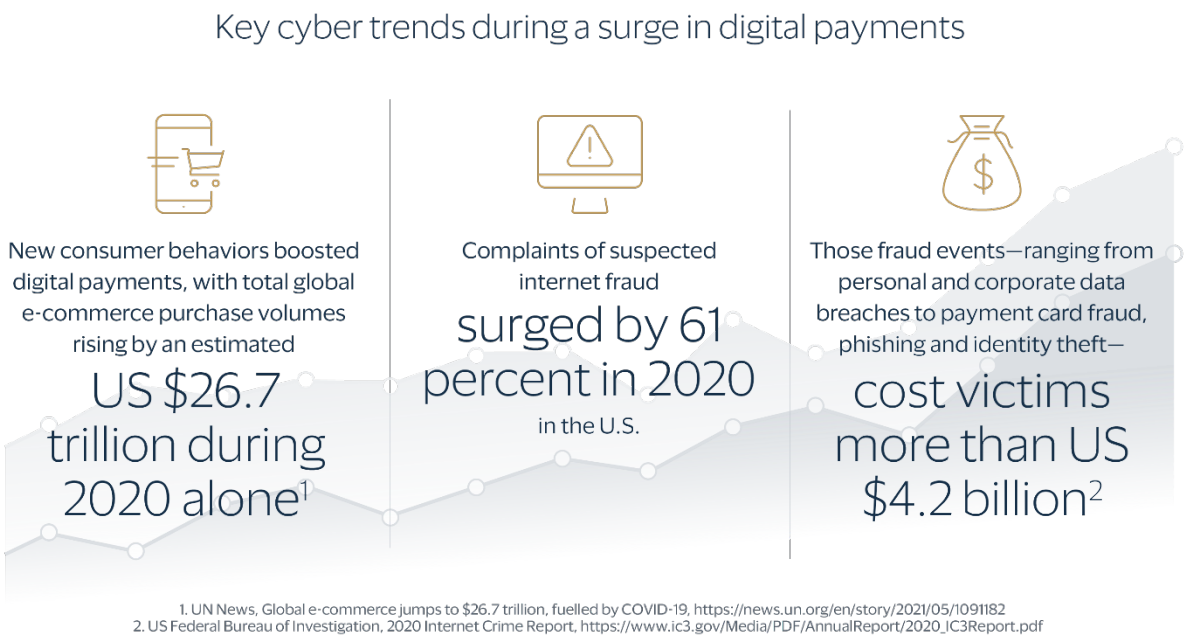
Countering emerging cyber threats

Visa Consulting & Analytics

Ecommerce has grown exponentially in the past few months, but with the rise of digital payments comes a rise in threats from bad actors. As you think about cybersecurity, keep an eye out for these five key cyber trends.



Five leading payment cybercrime trends

1. Enumeration attacks

These types of attacks use trial-and-error to guess payment credentials. Cybercriminals have been using the global surge in ecommerce volumes as cover for their automated testing of common payment fields including the full payment account number, CVV2, and/or expiration date. Where they have been successful in guessing legitimate account details, an emerging trend has been to use them to purchase cryptocurrencies. Here are some solutions for issuers take:

> Cybercrime in the payments space is any fraudulent activity targeting digitally enabled payment systems and companies that operate in the payments ecosystem. Examples include theft of stored payment credentials, the use of compromised payment credentials, or the use of digital payment systems to monetize other forms of fraud.

- Set up account monitoring activities (including monitoring API functionality and behavior for bot or scripting attacks)
- Look out for unusually high growth in transaction counts
- Pay attention to declines for invalid account numbers

- Identify flurries of regular authorization requests from the same source (e.g., one every few seconds)
- Implement security safeguards such as IP Allow list, which indicates what IP addresses can access your account, CAPTCHA, which enables web hosts to distinguish between human and automated access to websites and device fingerprinting, a process used to identify a device based on its unique configuration

It also pays to look out for authorization requests using sequential account numbers and provide extra protection to any similar numbers, perhaps by applying highly targeted transaction-level blocks.

2. **Rapid emergence of buy online, pickup in store**

   The buy online, pickup in store service meets the needs of merchants and consumers but can open up new ways for criminals to commit payment fraud. Typically, cybercriminals use compromised account credentials to conduct fraudulent online purchases or intercept details of legitimate purchases. They then go to the store to pick up the goods, pretending to be customers.

   The best solution is for merchants to make process improvements – for example, by applying some additional checks at the time of pickup, such as order number verification and ID verification.

3. **Payment-related ransomware**

   Ransomware is malware designed to stop a user or organization from accessing their own files. Through ransomware, criminals encrypt files and demand a ransom payment for the decryption key. While ransomware is a risk faced by any business, cybercriminals are increasingly directing their attacks at the payments ecosystem. For example, in addition to or instead of disabling core systems, the perpetrator may also steal payment account data.

   To prevent such attacks, organizations should apply a rigorous approach to cybersecurity. For financial institutions and merchants, it is important to segment networks, specifically, segmenting information systems that process and/or store cardholder information or payments information.

4. **Targeting government disbursements**

   Over the past couple of years, many governments introduced financial assistance programs for both employers and citizens and have been supporting recovery with stimulus payments. The rapid rise of these programs created high risk of fraud. In the U.S., for example, cybercriminals have used stolen identity credentials to apply for unemployment insurance and then loaded the funds onto prepaid or virtual payment accounts. These are then monetized through the purchase of gift cards, cryptocurrency, or electronics or by making peer-to-peer funds transfers.

Partnerships between government, law enforcement, and the payment industry are the best defense. In addition, issuers can apply additional checks and controls to minimize the risks – such as enhanced identity verification at the account opening/account loading phase and monitoring for suspicious monetization techniques once funds have been disbursed.

5. **POS malware and e-skimming**

Payment account data is constantly being targeted by cybercriminals and a continuing threat is the rise of e-skimming or digital skimming. Attacks involve injecting malicious code into a merchant's e-commerce system to harvest payment card details as they are being entered into checkout pages. If these attacks are successful, cybercriminals can maintain access to the compromised servers and move around within the merchant's wider network.

Through secure acceptance technologies, such as EMV, tokenization is increasingly used to desensitize and protect account data. In addition to this, merchants and their vendors must effectively deploy the latest cyber controls. For example, you should ensure that all payments software is regularly updated and patched, robust firewalls are in place, access to administrative portals is effectively controlled, and systems are regularly scanned for vulnerabilities or malware. The enablement or deployment of secure acceptance technologies, such as chip and tokenization, significantly reduce the risk of cardholder data compromises as a result of POS and e-skimming malware.