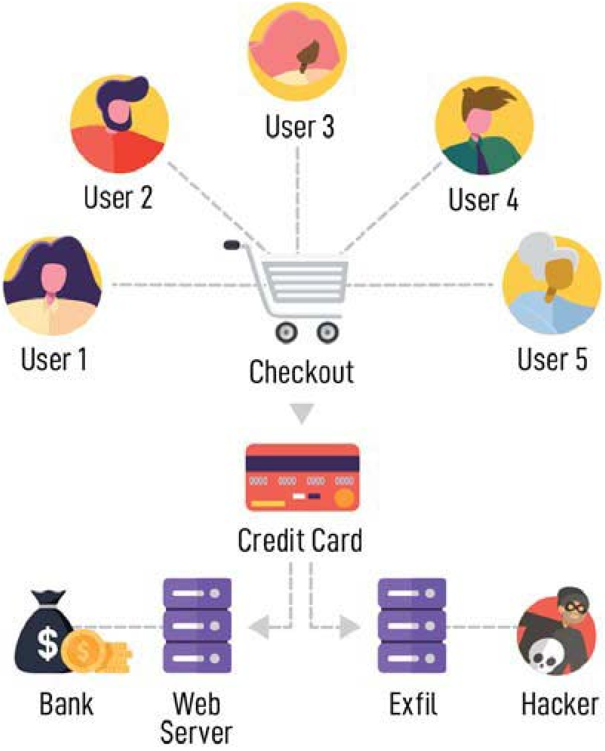
Protecting You and Your Family

FCCB
FIRST CITIZENS COMMUNITY BANK

E-SKIMMING

E-skimming is when online consumer payment data is stolen from website checkout forms. Cyber criminals introduce skimming code on payment card processing web pages to capture credit card and personally identifiable information and send the stolen data to a domain under their control.
Skimming code is introduced to payment card processing websites by:

- ✓ Exploiting a vulnerability in the website's e-commerce platform
- ✓ Gaining access to the victim's network through a phishing email or brute force of administrative credentials
- ✓ Compromising third-party entities and supply chains by hiding skimming code in the JavaScript loaded by the third-party service onto the victim website
- ✓ Cross-site scripting which redirects customers to a malicious domain where malicious JavaScript code captures their information from the checkout page



The malicious code captures credit card data as the user enters it in real time. The information is then sent to an Internet-connected server using a domain name controlled by the actor. Subsequently, the collected credit card information is either sold or used to make fraudulent purchases. Any business accepting online payments on their website is at risk of an e-Skimming attack.

WHAT ARE THE WARNING SIGNS?

- ✓ Complaints of fraudulent activity on several customers' accounts after making a purchase.
- ✓ Identifying a new domain not known to be registered.
- ✓ JavaScript code has been edited.

HOW CAN YOU MINIMIZE RISK?

- ✓ Perform regular updates to payment software.
- ✓ Install patches from payment platform vendors.
- ✓ Keep anti-virus software updated.
- ✓ Monitor and analyze web logs.