



**July 6, 2026**

**Contact: Claire Crouch**  
**Dallas County District Attorney's Office**  
**214-653-3600 (Office)**  
[Claire.Crouch@DallasCounty.org](mailto:Claire.Crouch@DallasCounty.org)

**FOR IMMEDIATE RELEASE: Dallas County Secures Lengthy Prison Sentences for Three Members of Organized Credit Card Skimming Ring**

**(Dallas, Texas)** — The Dallas County Criminal District Attorney's Office has secured lengthy prison sentences against three members of an organized criminal enterprise responsible for placing credit card skimming devices at retail stores throughout the Dallas-Forth Worth area, stealing the financial information of at least 783 victims.

Gheorge-Ciprian Hilitanu, Victor Tecu, and Ionut Firan-Alexandrau each pleaded guilty to multiple felony offenses stemming from a sophisticated financial fraud scheme that targeted customers at CVS and Walgreens stores across North Texas during July 2025.

The investigation, led by the Texas Financial Crimes Intelligence Center (TX FCIC), revealed that the defendants installed hidden skimming devices on payment terminals to secretly capture debit and credit card information from unsuspecting customers.

A skimming device is a concealed electronic device placed on or inside a payment terminal that records the information stored on a payment card's magnetic strip when it is swiped. Criminals use the stolen data to create counterfeit cards or make unauthorized purchases, often before victims realize their financial information has been compromised.

Following the defendants' arrests, FCIC Special Agent's executed a search warrant at the Airbnb where the group was staying. Investigators recovered evidence of a large-scale financial fraud operation, including:

- More than 150 skimming devices
- 237 re-encoded gift cards containing stolen account information
- 25 fraudulent international identification cards and passports bearing multiple identities
- Equipment used to manufacture counterfeit payment cards and facilitate financial fraud

A forensic review of the seized devices ultimately identified 783 unique victims whose financial information had been stolen.

On June 25, 2026, Gheorge-Ciprian Hilitanu entered into an open plea before Judge Lela Mayes who sentenced him to 30 years in prison for Engaging in Organized Criminal Activity and Fraudulent Possession or Use of a Credit or Debit Card charges, along with 20 years in prison for Tampering with a Governmental Record and Unlawful Use of a Wire or Electronic Communication.

On June 29, 2026, Victor Tecu and Ionut Firan-Alexandrau each pleaded guilty and were sentenced to 20 years in prison on all cases.

"Financial crimes like these affect everyday people who are simply going about their lives," said Dallas County Criminal District Attorney John Creuzot. "The defendants in this case operated a sophisticated criminal enterprise that victimized hundreds of people across North Texas. These significant prison sentences reflect the serious harm caused by organized financial crime and demonstrate our commitment to holding those who exploit hardworking Texans fully accountable."

"This case demonstrates the TX FCIC's commitment to dismantling organized financial crime networks that target everyday Texans. We extend our sincere thanks to the Dallas County District Attorney's Office and the presiding judge for their diligence in prosecuting this case and handing down a punishment that reflects the severity of these crimes. These significant convictions send a clear message: we will pursue those who threaten the security of our financial systems and the economic well-being of our state. We remain dedicated to protecting Texas victims and our economy," said Texas FCIC Captain Jeff Roberts.

Special thank you to Assistant Criminal District Attorney Aja Reed who prosecuted the cases on behalf of the Dallas County District Attorney's Office. The Dallas County Criminal District Attorney's Office also thanks the Texas Financial Crimes Intelligence Center and its law enforcement partners for their work investigating this complex, multi-jurisdictional case.

Consumers can help protect themselves from skimming by inspecting card readers before use, covering the keypad when entering a PIN, monitoring account activity regularly, and promptly reporting suspicious transactions to their financial institution.