Credit-Push Fraud Schemes

Credit-push fraud schemes manipulate victims into willingly transferring funds to fraudulent accounts. Fraudsters use tactics such as email spoofing, impersonation, and social engineering to convince individuals or businesses to process payments. Below are common types of credit-push fraud and ways to prevent them.

Business Email Compromise (BEC)

How It Works:

- Fraudsters impersonate a trusted executive, supplier, or business partner via email spoofing or compromised email accounts.
- They instruct employees to send a payment for an urgent invoice or wire transfer.
- The funds are sent to an account controlled by the fraudster.

Prevention Tips:

- Verify all payment requests through a separate communication channel (phone, in-person).
- Implement dual-approval processes for high-value transactions.
- Educate employees to spot phishing tactics and unusual payment requests.

Vendor or Supplier Invoice Fraud

How It Works:

- Fraudsters pose as legitimate vendors and send fake invoices.
- They may compromise email accounts or use lookalike domains to convince a business to update payment details.
- Payments are sent to the fraudster's bank account instead of the real vendor.

Prevention Tips:

- Verify any changes to payment details with vendors directly.
- Use trusted vendor portals for invoice management instead of email-based instructions.
- Train employees to look for subtle changes in email addresses (e.g., 'supplier@xyzcompany.com' vs. 'supplier@xyzc0mpany.com').

Payroll Diversion Fraud

How It Works:

- Fraudsters spoof HR or payroll departments and request that an employee's direct deposit details be updated.
- The employee's paycheck is redirected to a fraudulent account.

Prevention Tips:

- Require in-person or two-factor authentication (2FA) before making payroll changes
- Notify employees when their direct deposit details are updated.
- Monitor sudden multiple payroll updates from the same IP address.

Real Estate Wire Fraud

How It Works:

- Fraudsters hack or spoof emails from real estate agents, title companies, or attorneys.
- Homebuyers receive fake closing instructions directing them to wire funds to fraudulent accounts.
- The buyer unknowingly sends their down payment to a criminal.

Prevention Tips:

- Verify wire instructions over the phone before transferring funds.
- Use secure document portals instead of email for sensitive communications.
- Train real estate professionals to warn buyers about fraud risks.

Double-Sided Spoofing Fraud

How It Works:

- Fraudsters simultaneously target both a business customer and their financial institution using spoofed phone calls and emails.
- They impersonate bank representatives or law enforcement to trick the business into revealing login credentials and security information.
- Using the stolen information, they then impersonate the business when contacting the financial institution, requesting a token reset or security override.
- Once the token is reset, they take over the business’s account and initiate fraudulent ACH and wire transfers to accounts under their control.