United States Secret Service

Cyber Investigations: 2025 Trends In Cyber Crime

NIFA Stefan Hare
Dallas Field Office

Bio

- 14 Years of Law Enforcement Experience
- Certified Digital Forensic Examiner for the Dallas Field Office United States Secret Service
- Background in criminal intelligence, investigation, and crime trend analysis
- 1,000+ hours of education in incident response, digital forensics, crime analysis, and internet crimes against children
- 2,500+ devices examined
- Investigative assistance provided from minor theft, to multimillion dollar international transitional criminal organizations
- I can type at 125 words per minute, I am told that I speak at a similar rate at times

US Secret Service - History

Worthy of Trust and Confidence

We are one of America's oldest federal law enforcement agencies, originally created in 1865 to stamp out rampant counterfeiting in order to stabilize America's young financial system. By the end of the Civil War, nearly one-third of all currency in circulation was counterfeit. As a result, the country's financial stability was in jeopardy. To address this concern, the Secret Service was established in 1865 as a bureau in the Treasury Department to suppress widespread counterfeiting.

USSS History

- Founded in 1865 as a branch of U.S. Treasury Department.
- Originally created to combat the counterfeiting of U.S. currency.
- Dual integrated mission:

Protection

Investigations

Jurisdictional History

1865 – Secret Service created to combat counterfeit currency

1901 – Assigned Presidential Protection duties

1948 – Counterfeiting & Forgery (18 U.S.C. §470-474)

1984 – Access Device Fraud, Computer Hacking (18 U.S.C §1029-1030)

1986 – Computer Hacking, Expanded (18 U.S.C. §1030)

1990 – Bank Fraud (18 U.S.C. §1344)

1996 – Fictitious Obligations (18 U.S.C. §514)

1998 – Identity Theft, Expanded (18 U.S.C. §1028)

2001 – USA PATRIOT ACT (Expanded Cyber Investigations & Created ECTFs)

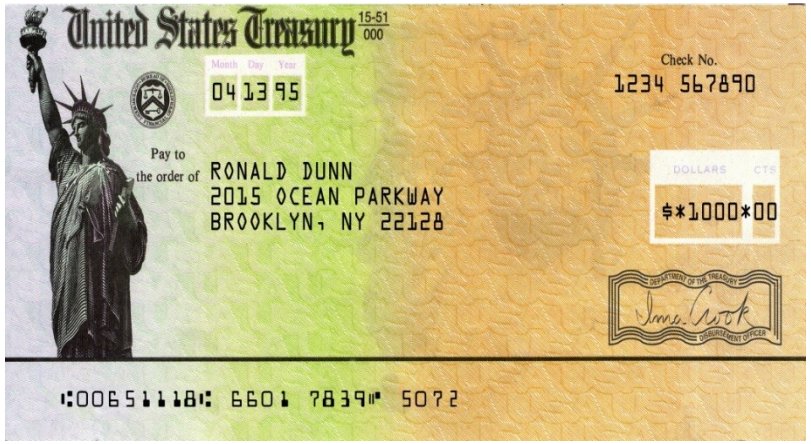
2003 – CAN-SPAM Act (18 U.S.C. §1037)

2004 – Aggravated Identity Theft (18 U.S.C. §1028A)

2020 – USSS combined ECTFs and FCTFs to create CFTFs

Investigative Mission

Protect the integrity of U.S. currency
and safeguard the nation's critical financial infrastructure



Investigations

Criminal Investigations	Financial Crimes	Cyber Fraud
• Counterfeit Currency • Counterfeit Treasury Obligations	• Identify Theft / False ID • Check Fraud / Forgery • Credit Card Abuse / Access Device Fraud • Bank Fraud • Mortgage Fraud • Money Laundering • Disaster Relief Fraud	• Network Intrusion • Business Email Compromise • Ransomware Attacks • Data Breaches • Wire Fraud • Bank Fraud • Crypto Fraud • Romance Scams

USSS Cyber Fraud Task Forces (CFTFs)

- The CFTFs are staffed with:
  - ✓ Special agents
  - ✓ Technical experts
  - ✓ Forensic analysts operating in the Digital Evidence Forensic Labs (DEFL)
  - ✓ SLTT task force officers trained through the Secret Service National Computer Forensic Institute (NCFI).

- CFTFs are a partnership between the USSS and:
  - ✓ Other law enforcement agencies
  - ✓ Prosecutors
  - ✓ Private industry
  - ✓ Financial institutions
  - ✓ Healthcare industry
  - ✓ Academia

CFTFs prevent, detect, and mitigate complex cyber-enabled financial crimes. Partnering effectively leverages collective expertise to combat cybercrime.

North Texas Cyber Fraud Task Force

The USSS Dallas Field Office Electronic Crimes squad and Financial Investigations squad combined to form the North Texas Cyber Fraud Task Force (NTCFTF).

The NTCFTF has established trusted partnerships with:

- Local, state, and federal law enforcement
- Private industry/corporations
- Academic institutions
- Healthcare Industry
- Financial Institutions
- Critical Infrastructure

Together we coordinate investigations, share information and technical expertise, and training through:

- Semi-annual meetings
- **Outreach/Presentations**
- Regular advisories and informational publications
- SLTT training at NCFI
- Email: Dallas.CFTF@usss.dhs.gov

Investigative Approach

TECHNICAL INVESTIGATIONS - focus on identifying cyber actors through forensic examinations, whose intent is to remain anonymous.

FINANCIAL INVESTIGATIONS - focus on recovering lost funds and identifying illicit fund recipients, whose intent is to disguise the transactions.

INCIDENT RESPONSE – focus on assisting entities to prepare for, defend against, contain, and recover from a cyber attack or fraud loss.

Cyber Crimes

- Business Email Compromise (BEC)
- Corporate Account Takeover
- Ransomware
- Crypto Fraud
- Elder Fraud
- Mobile Malware

Socially Engineered Threat Landscape

- Since the widely accepted use of social media users have been faced with a very important decision
- To share on social media, or not to share?
- Pictures of your lunch? Ok
- Pictures of your bank account balance? Please…don’t
- Pictures of your vacation may be great, but does that open the door to an attack vector?
- What about out of office notifications on email?

IQ Test Social Media Edition

- Free IQ test seen on social media, ten questions, see if you're in the top 5% of the Country
- If you have one, you want to share it. But once you share it, you don't have one. What is it?
- Everyone in the world needs it, but they usually give it without taking it. What is it?
- What is the best football, baseball, basketball team?
- Name of your Highschool Mascot, College Mascot
- Favorite TV show?
- Favorite Movie?
- Street you grew up on?
- The sum of the last four of your social security number written as an equation? (1 2 3 4 =10)
- Date of your favorite child's birthday?
- First pet's name and type?

Common Attack Vectors and Trends

- Credential Stuffing
- Exfiltration of Encrypted data- Why?
- Social Engineering – Phishing, impersonation, AI extortion
- Physical attacks (USB disguised as cryptocurrency wallet, unsecured ethernet ports, access key theft)
- End goal is to procure PII, tradecraft, and proprietary business secrets

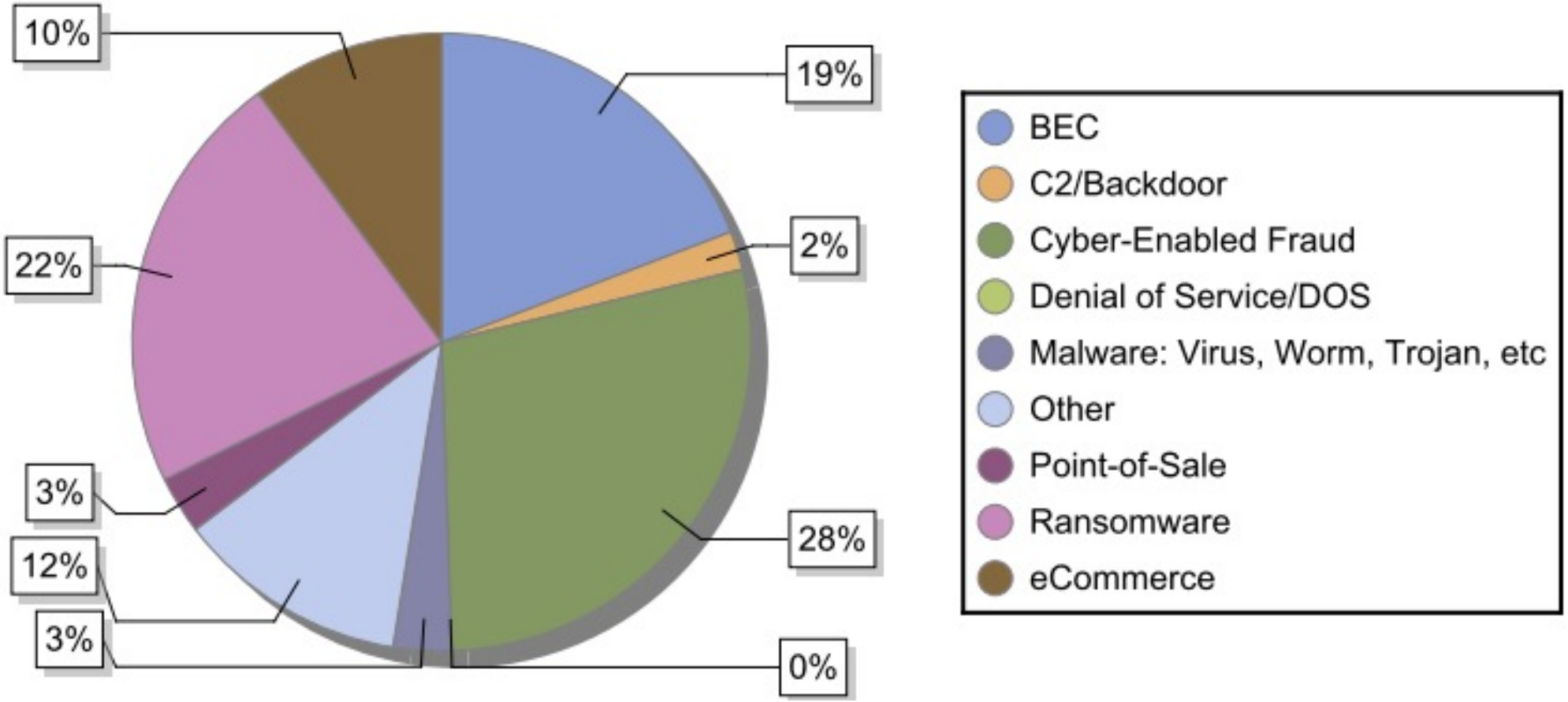
Hypothetical Case Example

- Large data breach occurs containing users emails, passwords, and corporate proprietary information
- Information is posted on dark web forums for sale
- Transnational Criminal Organization purchases data
- Organization refused to pay ransom/extortion demands
- Rather than release customer information TCO creates synthetic identities for current and future vendors, as well as ALL current employees of the victim corporation
- TCO utilizes social engineering and synthetic identities to file unemployment and SBA loans for THOUSANDS of employees (C Suite targeted first)
- TCO creates synthetic identity documents, drivers license, bank accounts, social media, email addresses for the victim corporation employees
- TCO leverages street level groups to open in person lines of credits, refinance of homes, second mortgages, new vehicle purchase

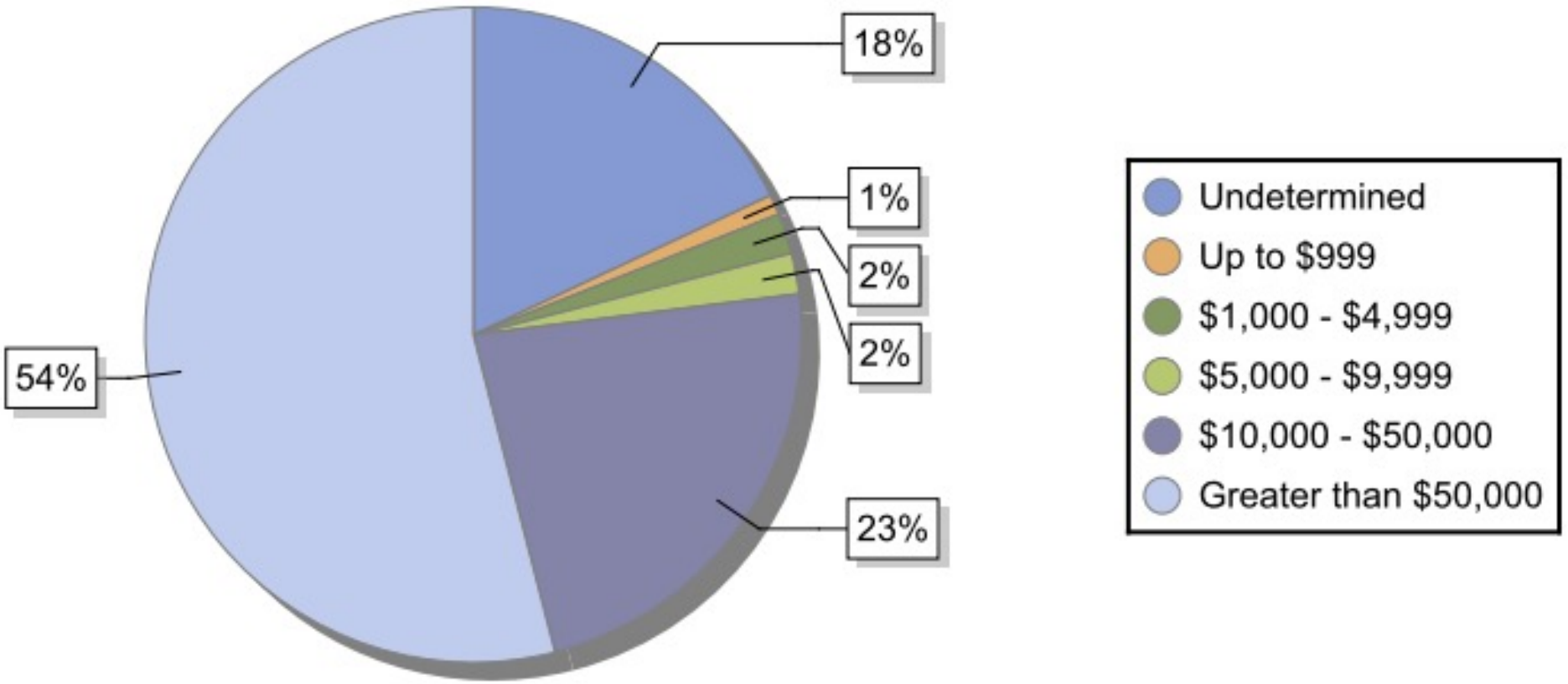
2025 The Year of the Synthetic Identity

- Synthetic Identity- The process of procuring a false identity through illicit and fraudulent means
- Identity theft has been an attack vector for decades
- Services range from $5-$500 USD to purchase a passable identity card
- Drivers license, insurance cards, passports, tax documents
- Fraudsters are becoming more aggressive, looking for larger accounts to steal funds
- This is a large change from targeting more people for smaller gains i.e $25 cashapp scam vs. $2,000,000 crypto enabled fraud

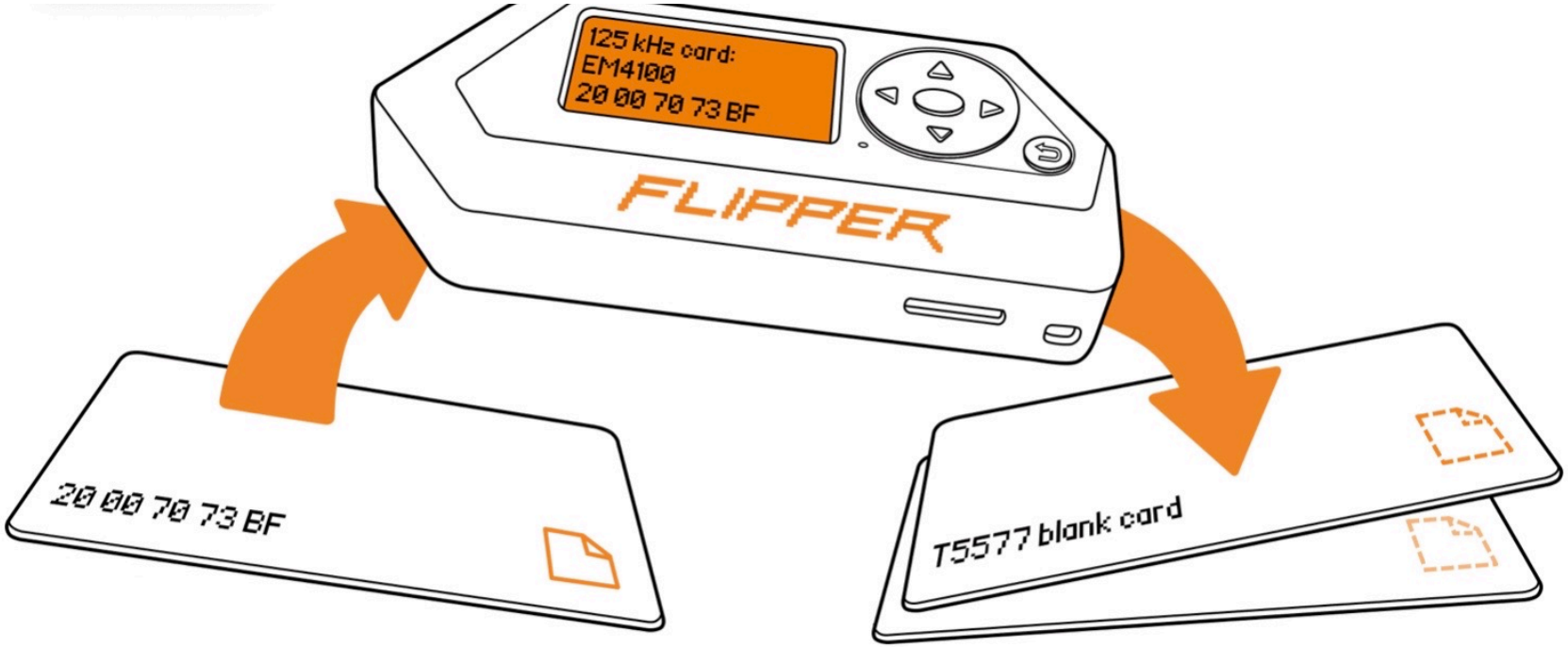
Intrusion by Type 2025



Intrusion by Cost as of June



Flipper Considerations



You can write saved and manually added 125 kHz cards to a T5577 rewritable blank card, which can be programmed to emulate cards with various low-frequency RFID protocols. The T5577 blanks may come in different forms and shapes, such as cards, keyfobs, stickers, and animal microchips. Flipper Zero is capable of writing data with all the supported low-frequency RFID protocols.

ATM Physical Vulnerability Scenario

[redacted] ATM Machine Bezel and cassette Keys set of 2 keys

Brand New

$14.00

Buy It Now

Free delivery

[redacted] (57) 100%

ATM Physical Attack Hypothetical Case

- There are estimated to be over 500,000 physical ATMs in the USA
- The vast majority are readily updated, and secured with modern attack prevention
- What happens when attackers clone the internal operating system drive after a physical attack and deploy malware?
- Any built in system commands that could force the machine to empty its contents completely?
- How much cash currency is stored in a typical ATM?

United States Secret Service

North Texas Cyber Fraud Task Force
Dallas Field Office
972-868-3200
dallas.cftf@usss.dhs.gov

Thank you for this opportunity

PCI Security Standards Council®

2025 NORTH AMERICA COMMUNITY MEETING