FRAUD AWARENESS FOR BUSINESSES

TRENDS, TACTICS, AND RED FLAGS

May 2026

ALERUS

AGENDA

- Welcome
- Current Fraud Trends and Red Flags to Watch For
  - Kim Lazur, Senior Manager, Fraud, Alerus
- How Fraudsters Steal and Use Your Data, and How to Protect It
  - Roger Schmitz, VP, Information Security, Alerus
- Q&A

KIM LAZUR

SENIOR MANAGER, FRAUD

- 38 years at Alerus, 20 years specializing in fraud
- Leads team of five dedicated fraud specialists, focused on detecting and preventing fraud

FRAUD MONITORING

HOW A BANK'S FRAUD TEAM MAY SUPPORT YOU

- Advanced fraud monitoring solutions help detect and prevent fraud
  - Alerts throughout the day that help prevent fraud:
    - Checks
    - Deposits
    - Wires
    - ACH
    - Suspected online account takeover

- Personal outreach
  - Fraud team may call your business to verify a transaction

Example: Certain wire and ACH transactions may require a callback to the business to verify details before releasing funds as a precautionary measure.

FRAUD MONITORING

YOUR ROLE IN IDENTIFYING FRAUD

Fraud prevention works best when businesses and banks work together.

Monitor Account Activity

Regularly review transactions to detect unusual unauthorized activity early and minimize losses.

Understanding Fraud Risks

Staying educated on common schemes like phishing and identifying theft helps you recognize red flags.

Reporting Suspicious Transactions

Prompt reporting of anomalies to your bank, ideally as soon as something feels off, helps trigger investigations and prevent further fraud.

Implementing Internal Controls

Setting approval processes, segregating duties, and using secure technologies helps protects sensitive information and business funds.

BUSINESS EMAIL COMPROMISE (BEC)

WHAT IS BEC?

- **Business email compromise** (BEC) is a type of fraud where a criminal uses or takes over email to impersonate a trusted person or business and trick a company into sending money or sensitive information.
- Targets for BEC include **companies of all sizes**, but especially those handling wire transfers, ACH payments or international payments.
- AI tools like chat generators and voice cloning make BEC attacks more convincing, producing realistic emails and phone calls that mimic executives or officials. In 2025, businesses reported over $30 million in losses from AI-driven BEC scams.

KEY STATS[1]

$3+ billion

losses attributed to BEC in the U.S. in 2025

85-90%

of BEC attacks involve impersonation of a trusted person or business — most commonly executives or vendors

$125,000+

average loss per incident

[1]Source: FBI 2025 Internet Crime Report. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

Please see last page for important disclosures.

HOW BEC UNFOLDS

Step 1: Phishing or spoofing to gain email access

- Phishing/spoofing is a form of social engineering where criminals use authentic-looking but fake emails or messages to steal log-in credentials or redirect users to fake websites.

Step 2: Monitor email threads to learn company behavior and identify when and how payments are requested.

Step 3: Send fraudulent request (e.g., fake invoice, urgent wire transfer)

- Fraudsters often masquerade as a trusted entity, such as a vendor, executive, or bank and create urgent requests for wires, ACH, gifts cards, or cryptocurrency.

Step 4: Redirect funds to scammer-controlled accounts, often overseas or unrecoverable

Any request to change payment instructions or bank details

BUSINESS EMAIL COMPROMISE

TYPES OF BUSINESS EMAIL COMPROMISE

Vendor payment fraud	Scammer poses as trusted vendor and sends email claiming payment instructions changed.
CEO/Executive impersonation fraud	Scammer impersonates an executive to request urgent payment, gift cards or sensitive data.
Account compromise	Hacked employee email addresses are used to request payments.
Data theft	Fraudsters target HR employees to gain access to tax information or employee records.

REAL-WORLD EXAMPLE

BEC: LOOK-ALIKE EMAIL

Scenario: Machinery vendor negotiation

What happened

- Criminals hijacked an existing email thread with a legitimate vendor using a look-alike address
- Fraudulent wiring instructions were provided for a down payment
- Business sent a $105,000 international wire

How it was detected

- After the initial payment, the “vendor” requested additional funds, raising concerns
- Client reviewed the email chain and discovered subtle email mismatch

Response and outcome

- Bank initiated a wire recall and hold-harmless request
- Law enforcement and IC3 reports were filed
- No funds recovered — $105,000 loss

REAL EXAMPLE

BEC: EMAIL ACCOUNT TAKEOVER

Scenario: Account takeover at vendor

What happened

- Criminals compromised a legitimate vendor's email account
- Payment change request sent from the trusted vendor contact
- Business initiated three ACH payments over several weeks

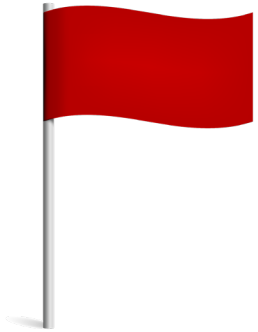
How it was detected

- Client learned the vendor's email had been compromised
- Upon review, confirmed the payment change request was fraudulent
- Fraud was reported to the bank after the final ACH transaction posted

Response and outcome

- The bank immediately issued hold-harmless requests to the receiving bank
- Client was advised to file reports with law enforcement and ic3.gov
- No funds recovered — $151,000 loss

RED FLAGS TO WATCH FOR



- Urgent or time-sensitive requests involving payments or financial transactions
- Requests to bypass standard payment procedures or change banking information
- Unusual timing, tone, or wording that doesn't match how the sender normally writes
  - Overly formal or unusual language (for example, repeated use of "kindly")
- Slight changes to email address or domains
  - Look-alike or misspelled domains (m1crosoft.com vs microsoft.com)

PREVENTION STRATEGIES

- Set up payment verification procedures for all payment instruction changes (callbacks, dual approval)
  - Always verify using a known, trusted phone number
- Treat email-only payment change requests as high-risk
- Separate duties so no single employee can create and release payments
- Require multi-factor authentication (MFA) on all email accounts
- Train employees to recognize phishing and report suspicious messages immediately
  - Short, interactive training is most effective
- Have IT monitor for unusual email rule changes and suspicious log-ins
- Use email filtering to detect spoofed or look-alike domains
- Use bank tools such as positive pay, ACH filters, and transaction alerts

INCIDENT RESPONSE PLAN

IF YOU SUSPECT BEC

Identify	Identify suspicious payments, emails, or account activity immediately
Isolate	Secure compromised email and banking accounts Reset credentials and suspend further transactions
Alert	Contact your bank immediately — time is critical Alert internal IT/security teams
Report	File a report to the FBI's IC3 (ic3.gov) Contact local law enforcement as advised
Recover	Work with your bank to attempt fund recovery Act quickly — recovery chances decrease significantly over time

BANK IMPERSONATION SCAMS

Please see last page for important disclosures.

BANK IMPERSONATION SCAMS

What it is.	Fraudsters pretend to be from your bank, often spoofing a valid bank phone number.
The goal.	Trick you into sharing sensitive information or to authorize fraudulent transactions.
Tactic.	• The scammer claims there is a suspicious ACH or wire transaction • Asks for your confirmation code (MFA), company ID, username, or password to “stop” the transaction
Red flags.	▪ Urgent language: “Your account has been compromised!” ▪ Pressure to act quickly to avoid “losses” or “account suspension.” ▪ Calls appear to come from your bank’s real phone number ▪ Links to fake websites mimicking your bank’s login page ▪ **Your bank will never ask for your one-time passcode or password**

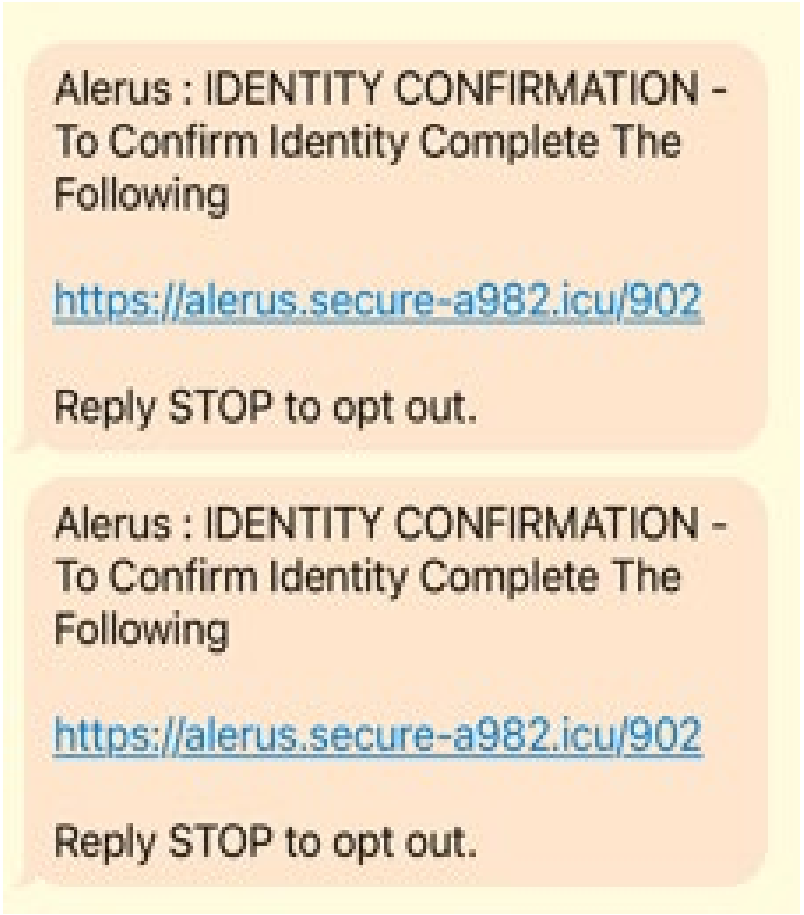
REAL EXAMPLE

PHISHING TEXTS

Alerus®: Keeping your information secure is our top priority, we're always on the lookout for new ways to protect you, and your account. One of our security measures is the client credential termination. Please follow

https://
securealerus.ir72-369.icu/
914

Reply STOP to opt out.



REAL EXAMPLE

BANK IMPERSONATION

Scenario: Fraudster impersonates bank fraud department

What happened

- Fraudster posed as bank's fraud department using a spoofed phone number
- Caller claimed there were suspicious transactions and texted a link to fake bank website

How the scam succeeded

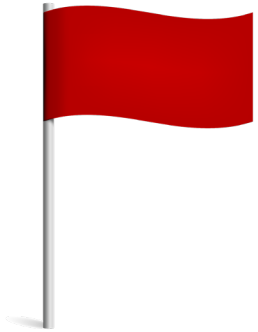
- The client entered online banking credentials and shared a one-time passcode
- Fraudster accessed online banking, posed as an authorized signer, and increased wire limit

Response and outcome

- Fraudster initiated 12 outgoing wires in one day totaling $310,000
- Some wires stopped by alerts, others processed
- Recalls and hold-harmless notices sent; recovery ongoing
- Potential client loss — $48,000

RED FLAGS AND PREVENTION STRATEGIES

BEST PRACTICES FOR BUSINESSES



- Your bank will never request your online credentials or one-time passcode.
- Caller ID can be spoofed and should not be relied upon as proof of authenticity.
- Avoid clicking on links received via text or email purporting to be from your bank.
- If you receive a suspicious call, remain cautious and verify the caller's identity by contacting your bank directly using a trusted phone number before taking any action.
- Enforce multi-factor authentication (MFA) for all online banking users.
- Develop internal procedures to verify payment and account change requests.
- Utilize fraud prevention measures such as payment alerts, positive pay, and ACH controls.
  - Educate employees to identify common scam methods.
  - Reference: banksneveraskthat.com (American Bankers Association)
- If you suspect fraudulent activity, cease all interactions immediately and contact your bank at once.


SERVE WITH PASSION
DO THE RIGHT THING
RESPECT EVERYONE
TO EMPOWER AND GUIDE LASTING FINANCIAL WELL-BEING
SUCCESS IS NEVER FINAL
EMBRACE CHANGE
CHERISH PEOPLE
COLLABORATIVE

CHECK FRAUD

CHECK FRAUD

Check fraud is the illegal use of checks to acquire funds that do not belong to the fraudster.


Forged signatures


Stolen blank checks


Altered checks


Counterfeit checks


Mail theft

High risk — Check fraud can result in significant financial losses for businesses and disrupt operations.

Prevalent and Increasing

- Check fraud remains a significant and growing threat, despite the shift towards digital payments.
- The fraud is becoming more sophisticated, with tactics including mail theft, digital counterfeiting, and AI-powered forgeries.
- For businesses, checks remain the payment method most often targeted by fraudsters.
- 58% of organizations experienced attempted or actual check fraud in 2025.

Source: 2026 Association for Financial Professions (AFP) Payments Fraud and Control Survey

CHECK FRAUD

Warning Signs

- Unexpected check transactions
- Discrepancies in check amounts or payees
- Unusual delays in check clearing or returned items
- Notifications from your bank about suspicious activity
- Notification from your vendor that payment was not received

Prevention Strategies

- Mail checks directly from the post office and avoid unsecured mailboxes
- Use Uni-ball® 207 gel pens
- Monitor accounts daily and reconcile promptly
- Secure check stock and limit access
- Use payee positive pay services to validate payees and amounts
- Train employees to recognize check fraud

Source: practicesafechecks.com, American Bankers Association

Please see last page for important disclosures.

CHECK FRAUD

HOW TO REPORT AN INCIDENT

Report check fraud IMMEDIATELY

- Contact your bank to complete an affidavit of forgery
- File local police report
- For mail theft cases: report to U.S. Postal Inspection Service at **uspis.gov/report** or 877.876.2455

FRAUD PREVENTION TOOLS

Check Fraud Controls

Positive Pay

- Bank compares checks presented for payment to a list of checks you issued
- Mismatches are flagged for review before payment

Payee Positive Pay

- Adds payee name matching to detect altered or washed checks
- Stops checks with changed payees from clearing

Reverse Positive Pay

- Daily review of checks presented
- Client decides what is paid or returned

ACH Fraud Controls

ACH Positive Pay

- Blocks unauthorized ACH debits
- Only approved vendors or transactions are allowed
- Exceptions require client approval

Block Services

Check Block

- Automatically returns all checks
- Best for accounts that never issue checks

ACH Block

- Automatically returns all ACH activity
- Best of accounts with no ACH usage

REAL EXAMPLE

HOW POSITIVE PAY PREVENTED CHECK FRAUD AND ACH LOSS

Scenario: Check and ACH fraud attempt

What happened

- Account and routing numbers were compromised
- Fraudsters created counterfeit checks and attempted six ACH debits
- Total attempted fraud exceeded $189,000

What was detected

- Four counterfeit checks were identified and returned within 24 hours of posting
- All fraudulent ACH debits were detected and returned

Why loss was prevented

- Client reviewed items daily and acted quickly
- Positive pay flagged unauthorized checks and ACH for review
- Suspicious transactions were returned within required timeframes

Outcome

- No financial loss to the client or the bank

ROGER SCHMITZ

VICE PRESIDENT OF INFORMATION SECURITY, ALERUS

- 30 years at Alerus, specializing in information technology
- Leads team of four focused on information security
  - Cybersecurity management
  - Strategic security oversight
  - Threat detection and response
  - Incident management
  - Security policy and training
  - Internal controls and risk management

Please see last page for important disclosures.

HOW FRAUDSTERS STEAL AND USE YOUR DATA, AND HOW TO PROTECT IT

Please see last page for important disclosures.

THE WORLD WE LIVE IN TODAY

CYBERCRIME LANDSCAPE AND STATISTICS

- **Cybercrime is industrialized and accelerating.** Threat actors now operate with automation, AI, and commoditized tools.
- **AI is both a defense tool and a weapon.** Deepfake-enabled fraud, voice cloning, and synthetic impersonations are being readily used.
- **Fraud is increasingly precise and psychological.** Criminals exploit trust through impersonation, phishing, and social engineering.
- **Regulatory pressure is intensifying.** New laws on AI, privacy, and breach notification are raising compliance costs and operational complexity.
- **Cybersecurity teams are understaffed and undertrained.** Many teams lack sufficient personnel, and few companies train non-security staff for cyber roles.
- **Cybercrime-as-a-service is thriving.** Dark web marketplaces offer plug-and-play fraud kits, phishing sites, and voice cloning tools to anyone with money.
- **Threats are everywhere.** From mobile apps to supply chains, every digital touchpoint is a potential vulnerability.

THE HUNT

HOW FRAUDSTERS GAIN INFORMATION

Fraudsters don’t attack blindly. They meticulously gather intelligence from multiple sources to build a detailed profile of their target, making their attacks highly effective and difficult to detect.

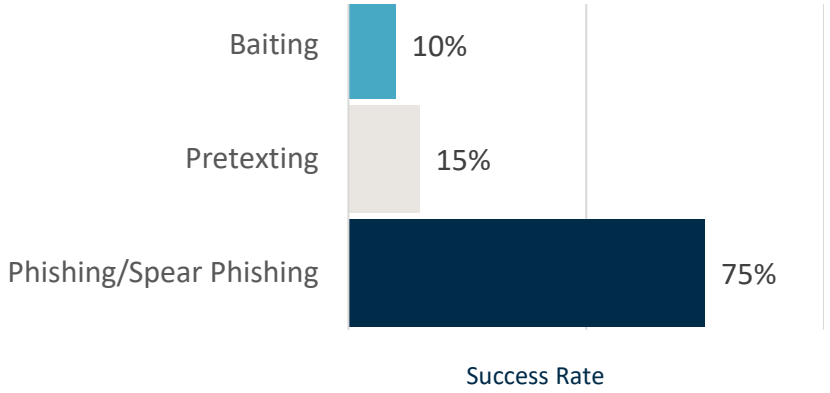
Open-Source Intelligence (OSINT)

Attackers start by collecting publicly available information. This passive data gathering forms the foundation of their attack plan, revealing your organization’s structure, technology, and key personnel.

- Social media – job roles, connections, and personal details
- Company websites – staff directories and organizational structure
- Public records – business registrations and legal filings

Social Engineering Tactics

Once they have a profile, attackers manipulate human psychology. Phishing remains the most dominant and successful tactic, preying on trust and urgency.

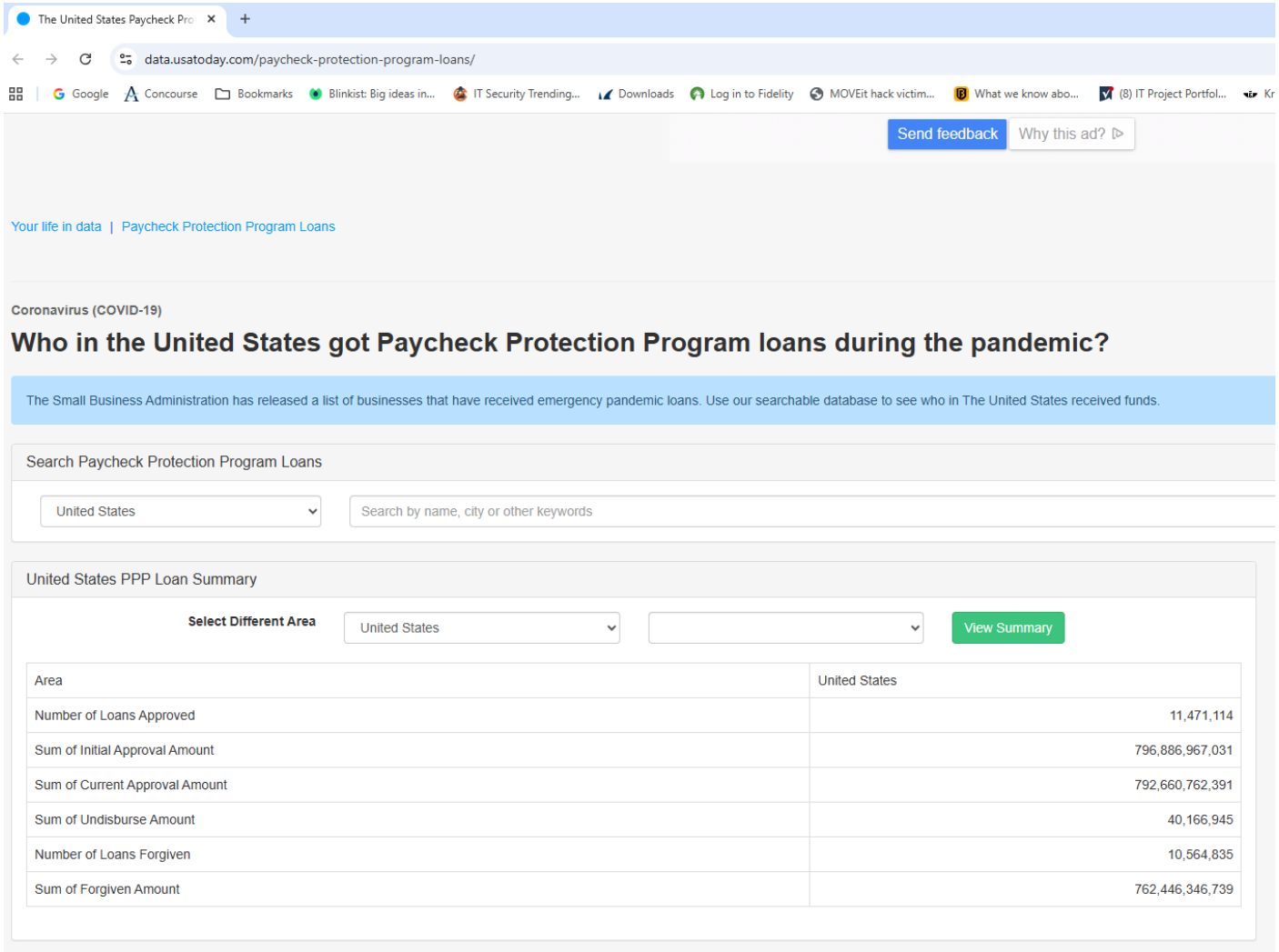


PROFILING

HOW FRAUDSTERS GAIN INFORMATION

- Open-Source Intelligence (OSINT)
  - Social media
  - Company websites
  - Public records
  - News articles and publications
- Social engineering
  - Phishing/spear phishing – trick victims into revealing sensitive information
  - Pretexting – gain trust to make a fraudulent request seem legitimate
  - Baiting – enticing offers to lure victims into traps
- Technical exploits and data breaches
  - Vulnerability scanning – shodan.io, criminalip.io, etc.
  - Malware and spyware – malware for sale, exploit database
  - Data breaches – Pastebin websites, TOR (darkweb)

PPP LOAN INFORMATION



Area	United States
Number of Loans Approved	11,471,114
Sum of Initial Approval Amount	796,886,967,031
Sum of Current Approval Amount	792,660,762,391
Sum of Undisburse Amount	40,166,945
Number of Loans Forgiven	10,564,835
Sum of Forgiven Amount	762,446,346,739

Please see last page for important disclosures.

PPP LOAN INFORMATION

Business	Current Approval Amount (*Undisburse Amount*)	Forgiveness Amount	Jobs Retained	Business Type	Lender	Date Approved
[redacted] Yazoo City, MS	20,159.00 *(0.00)*		1	Drinking Places (Alcoholic Beverages) (Sole Proprietorship)	BSD Capital, LLC dba Lendistry	May 29, 2021
[redacted] Gate City, VA	1,448.12 *(0.00)*	1,450.77 (Aug. 18, 2021)	1	Women's Clothing Stores (Sole Proprietorship)	The Enterprise Center Capital Corporation	May 28, 2021
[redacted] Union City, GA	20,832.00 *(0.00)*	20,963.94 (Jan. 21, 2022)	1	Beauty Salons (Sole Proprietorship)	Prestamos CDFI, LLC	May 26, 2021
[redacted] Kansas City, MO	15,963.00 *(0.00)*	16,034.39 (Dec. 2, 2021)	1	Offices of All Other Miscellaneous Health Practitioners (Sole Proprietorship)	Texas National Bank	May 26, 2021
[redacted], Greensboro, NC	6,528.00 *(0.00)*	6,643.00 (March 22, 2023)	1	Cosmetology and Barber Schools (Sole Proprietorship)	BSD Capital, LLC dba Lendistry	May 25, 2021
[redacted], Forrest City, AR	2,235.00 *(0.00)*	2,247.91 (Dec. 28, 2021)	1	All Other Transit and Ground Passenger Transportation (Sole Proprietorship)	Capital Plus Financial, LLC	May 22, 2021
[redacted] Greensboro, NC	2,916.00 *(0.00)*	2,956.50 (Nov. 1, 2022)	1	Child Day Care Services (Self-Employed Individuals)	Capital Plus Financial, LLC	May 21, 2021
[redacted], Mclean, VA	1,740.00 *(0.00)*	1,749.96 (Dec. 28, 2021)	1	Medicinal and Botanical Manufacturing (Sole Proprietorship)	Metro City Bank	May 20, 2021
[redacted], Rugby, ND	20,833.32 *(0.00)*	20,937.49 (Nov. 17, 2021)	1	Soybean Farming (Sole Proprietorship)	Gate City Bank	May 18, 2021
[redacted] Sabin, MN	20,833.32 *(0.00)*	20,901.03 (Sept. 15, 2021)	1	General Freight Trucking, Long-Distance, Truckload (Sole Proprietorship)	Gate City Bank	May 18, 2021

Please see last page for important disclosures.

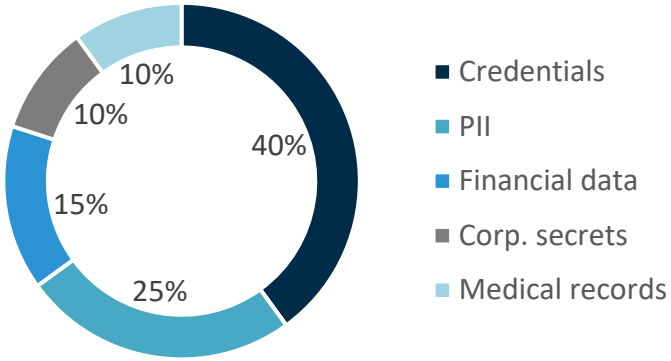
THE BLACK MARKET

WHERE YOUR DATA GOES

Stolen information isn't just used once; it's packaged, sold, and traded in a thriving underground economy. A single breach can fuel countless future attacks against your business and employees.

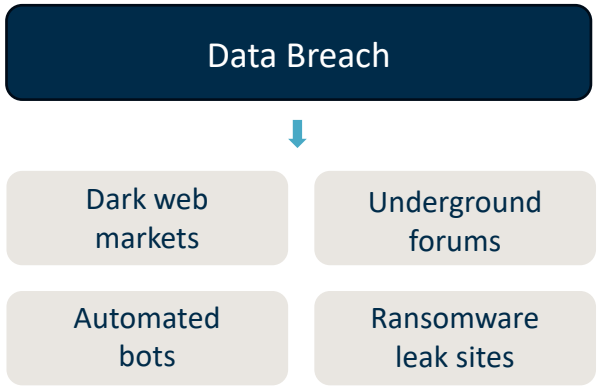
Most Traded Data Types

On dark web marketplaces, credentials and personal identity information are the hottest commodities, as they provide direct access to accounts and enable large-scale fraud.



The Data Laundering Flow

Data from a breach is quickly distributed through various channels, making it nearly impossible to contain once it's been compromised.



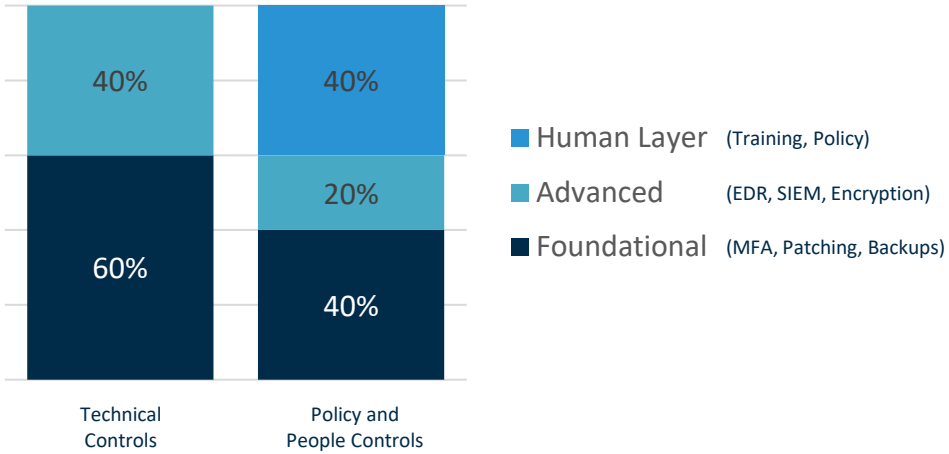
THE SHIELD

BUILDING YOUR DEFENSES

Protecting your business requires a multi-layered defense, combining robust technology with well-defined policies, and most importantly, an educated and vigilant workforce.

Balancing Technology and People

While technology provides the essential tools, your employees are the first line of defense. A successful security strategy invests heavily on both areas to create a resilient security culture.



Please see last page for important disclosures.

BE PROACTIVE TO PROTECT YOUR BUSINESS

TECHNICAL CONTROLS

- Strong password policies and multi-factor authentication
- Regular software updates and patch management
- Endpoint security
- Network security
- Data encryption – at rest and in transit
- Regular backups (test restores) – **Immutable** (tamper proof) and **air gapped** (isolated from the network)
- Access control and least privilege
- Security information and event management (SIEMs)/Logging

BE PROACTIVE TO PROTECT YOUR BUSINESS

POLICY AND PEOPLE CONTROLS

- Employee security awareness training — phishing campaigns, fake links
- Incident response plan — strategy and procedures for preparing for and recovering from a cybersecurity incident
- Vendor security management
- Data minimization — What do you need to keep available?
- Physical security
- Cybersecurity insurance

BE PROACTIVE TO PROTECT YOURSELF

1. Strong authentication

- Use strong passwords or passphrases
- Enable multi-factor authentication (MFA) for email, banking, and critical accounts
- Never reuse passwords across accounts
- Do not use business credentials on personal sites

2. Keep systems updated

- Apply regular software updates on workstations and mobile devices
- Automate updates where possible

3. Watch for phishing

- Verify identities before acting on requests involving money or sensitive data
- Be cautious with unexpected links or attachments

BE PROACTIVE TO PROTECT YOURSELF

(CONTINUED)

4. Secure your devices

- Install reputable antivirus and anti-malware software
- Enable firewalls on all devices

5. Protect your network

- Avoid public Wi-Fi for sensitive transactions
- Use strong passwords for home Wi-Fi
- Consider a VPN for financial or confidential access

6. Backup regularly

- Use cloud storage or external drives for backups

BE PROACTIVE TO PROTECT YOURSELF

(CONTINUED)

7. Enable alerts

- Set up notifications on banking, email, and other systems to detect suspicious activity

8. Practice cyber hygiene

- Log out when finished
- Avoid public computers for sensitive information
- Don’t overshare on social media

9. Check your exposure

- Visit HaveIBeenPwned.com to see if your accounts were compromised

RANSOMWARE

CONSIDERATIONS AND PREPARATION

Considerations

- Determine if and what you will pay for your data
  - What is your data worth?
  - Do you trust fraudsters will provide decryption key or not use your data?
  - If you decide to pay, do you have a crypto account?
- Do you report it to legal authorities?

Preparation

- Tabletop ransomware exercises
  - Logistics — response team, communication (employees, clients, media, fraudster negotiation)
  - Playbook/procedures documented
- Risk assessment and business impact analysis
- Backup and recovery strategy – immutable and air gapped
- Cyber insurance coverages

Q&A

THANK YOU FOR ATTENDING!

Kim Lazur

Senior Manager, Fraud

kim.lazur@alerus.com

Roger Schmitz

Vice President, Information Security

roger.schmitz@alerus.com

EQUAL HOUSING LENDER