# Nothing Personal: Understanding the Spread and Use of Personally Identifiable Information in the Financial Ecosystem

Mehrnoosh Zaeifi
mzaeifi@asu.edu
Arizona State University
Tempe, Arizona, USA

Faezeh Kalantari
faezeh.kalantari@asu.edu
Arizona State University
Tempe, Arizona, USA

Adam Oest
Aoest@asu.edu
Arizona State University
Tempe, Arizona, USA

Zhibo Sun
zs384@drexel.edu
Drexel University
Philadelphia, Pennsylvania, USA

Gail-Joon Ahn
gahn@asu.edu
Arizona State University
Tempe, Arizona, USA

Yan Shoshitaishvili
yans@asu.edu
Arizona State University
Tempe, Arizona, USA

Tiffany Bao
tbao@asu.edu
Arizona State University
Tempe, Arizona, USA

Ruoyu Wang
fishw@asu.edu
Arizona State University
Tempe, Arizona, USA

Adam Doupé
doupe@asu.edu
Arizona State University
Tempe, Arizona, USA

## ABSTRACT

Online services leverage various authentication methods with differing usability and reliability trade-offs, such as password-based or multi-factor authentication (MFA). However, financial service providers face a unique challenge; authenticating the user's legal identity, which involves verifying Personally Identifiable Information (PII), which we call PII-based authentication (PII-BA). These methods assume that PII is private; however, identity theft victimizes millions annually and exposes their PII to criminals.

In this paper, we investigate the potential of identity fraud that breaks PII-BA with stolen PII in the financial ecosystem. First, we measure what PII is used in PII-BA across five different financial services for 17 U.S. financial institutions. We subsequently collect data where PII and associated illegal services are available for purchase by monetizers (who perform identity fraud via obtained stolen PII)–operating within the underground economy and paste sites. Finally, we analyze how monetizers can make money from stolen PII by either breaking PII-BA or directly monetizing the PII with the associated cost. Our study reveals that payment processing companies (PPCs) impose lower PII requirements for password/username recovery service PII-BA compared to commercial banks. Consequently, criminals can bypass this PII-BA service across all PPCs by paying \$3.5~\$50 as opposed to \$10.5~\$600 for banks. We also outline potential mitigations which could be an essential step in addressing identity fraud resulting from PII-BA in the financial ecosystem.

## CCS CONCEPTS

• **Security and privacy** → **Economics of security and privacy**; **Formal security models**.

## KEYWORDS

Authentication mechanisms, Security and privacy, Underground community, Web security

**ACM Reference Format:**
Mehrnoosh Zaeifi, Faezeh Kalantari, Adam Oest, Zhibo Sun, Gail-Joon Ahn, Yan Shoshitaishvili, Tiffany Bao, Ruoyu Wang, and Adam Doupé. 2024. Nothing Personal: Understanding the Spread and Use of Personally Identifiable Information in the Financial Ecosystem. In *Proceedings of the Fourteenth ACM Conference on Data and Application Security and Privacy (CODASPY '24), June 19–21, 2024, Porto, Portugal.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3626232.3653266

## 1 INTRODUCTION

With our society's increased reliance on *digital financial services*, providers of such services face the difficult task of authenticating their users who access services through web browsers and mobile applications. Similar to non-financial services, financial service providers use various authentication methods with different usability and reliability trade-offs based on the importance and risk of the service. These methods include password-based authentication (i.e., something the user *knows*) and multi-factor authentication (MFA) (i.e., adding something the user *has*).

However, financial service providers face a unique challenge: because of the financial implications to both the provider and the user, users must be authenticated not just by something they *know* or *have* but by who they *are* [6]: the user's actual, legal *identity*. This authentication of identity is accomplished by verifying users' *Personally Identifiable Information* (PII) such as name, date of birth, address, phone number, Social Security Number (SSN), or Taxpayer Identification Number (TIN).

*CODASPY '24, June 19–21, 2024, Porto, Portugal*

ACM ISBN 979-8-4007-0421-5/24/06
https://doi.org/10.1145/3626232.3653266

We call this authentication method *PII-based authentication (PII-BA)*. By using PII for authentication, PII-BA systems carry an *implicit assumption* that such PII is only available to the person it identifies. However, as one of the fastest-growing types of cybercrime, PII theft exposes millions of victims' PII every year [53]. The large amount of stolen PII available to cybercriminals makes PII-BA prone to *impersonation attacks* followed by *identity fraud*, a type of crime that has proliferated in recent years and can lead to considerable financial loss to millions of victims and companies [34].

In 2021, the FTC received 2.8 million consumer reports, totaling over $5.8 billion in losses, with 1.4 million related to fraud [10]. Goel [11] found a 9% increase in identity fraud for every 10% growth in Internet-connected households, resulting in significant financial and health consequences [34]. However, the security implications of PII disclosure for services and users relying on it remain unexplored despite its critical role in authentication (PII-BA) and its inherent vulnerability.

In this paper, we investigate the potential of identity fraud enabled by breaking PII-BA with stolen PII in 17 U.S. representative financial institutions to understand the end-to-end process from the time *monetizers* acquire a stolen identity to the time they successfully use the victim's PII to impersonate the victim to break the PII-BA of a sensitive financial service.

We then estimate a cost range for cybercriminals using the monetization methods we studied for each investigated financial institution. In this regard, we investigate two significant sources of stolen PII: (1) the underground economy (underground forums and illicit markets) and (2) paste sites (Section 4), analyzing what PII is available and how much this PII costs. We also explore *complementary* illicit services[1], which help monetizers facilitate identity fraud to discover the opportunities available to monetizers and their costs without any interaction with the providers (Section 4.3). Our investigations show that public paste sites source stolen PII is negligible in volume compared to underground forums. Finally, we explore potential improvement to the current PII-BA (Section 6).

The contributions of our work are as follows:

- We analyzed the underground ecosystem and found that similar to other areas, such as concession abuse [41], the entire ecosystem has developed around supporting different steps involved in identity fraud using stolen PII in the financial ecosystem.
- We identified viable routes of identity fraud using stolen PII: credit card fraud, creating a falsified account, hijacking accounts through breaking password/username recovery, and cashing out stolen fullz (stolen credit/debit card full information) or stolen account, and analyzed the cost of them for monetizers.
- We articulated potential mitigations based on our results, which could be an essential step to stop identity fraud through breaking PII-BA in the financial ecosystem.

## 2 BACKGROUND

Financial institutions use authentication methods for both electronic and in-person services. PII-BA is a popular financial authentication mechanism relying on user PII. As per the United States Department of Labor, PII encompasses information that directly identifies individuals or aids in their identification, either directly or indirectly, through various descriptors [30].

PII is a prime target for attackers in financial services, leading to theft and impersonation risks. These impersonation threats arise when authentication mechanisms cannot verify PII's authenticity, affecting not just PII-BA but also other authentication methods like passwords, MFA, and risk-based authentication.

**PII-Based Impersonation Attack.**

In financial ecosystem, PII-based impersonation attacks involve two key actors: "thieves" who steal and trade PII, and "monetizers" who carry out identity fraud using the stolen PII. Figure 1 illustrates the three sequential steps of a PII-based impersonation attack.

In this work, we are interested in parts of the attack where monetizers are involved: Our goal is to demonstrate the vulnerabilities of PII-BA used in the financial ecosystem, which allows monetizers to perform identity fraud using stolen PII.

### 2.1 PII Theft

*PII theft* refers to a situation in which a PII thief steals victims' PII for further unlawful activity, typically with the intent of economic gain. PII theft is accomplished using different methods: (1) *Database Compromising*, in which identity thieves exploit vulnerabilities in the websites to compromise databases [21, 33]. (2) *Malware*, a piece of code used to cause extensive damage to a target system or gain unauthorized access to steal PII [32, 44]. (3) *Social Engineering Attacks*, which is the psychological manipulation of victims into disclosing confidential information to gain unauthorized access to systems or networks for financial profit [4, 28].

### 2.2 The Stolen PII Trade

After stealing PII, PII thieves will sell or share them in the underground and paste sites which are legitimate public platforms which criminals use to advertise or sell their products [3].

**The Underground Economy.** Researchers discovered that criminals actively trade information, illicit products, and services in the underground economy [41–43].

**Paste Sites.** Paste sites are legitimate public platforms that allow users to anonymously share text, source code, stories, lyrics, or written content with the world [46]. However, due to their public nature, they are prone to abuse, which turns them into places where hackers advertise, sell or share their stolen PII, illegal services, products, and information [31].

### 2.3 Identity Fraud

Monetizers obtain stolen PII from a successful *Stolen PII Trade*. Now, they can use this stolen PII to perform *Identity Fraud* [47]. To achieve this, they can either directly cash out the stolen PII, such as stolen fullz or stolen financial accounts, or break PII-BA of a financial service (Figure 1). There are some complementary illegal services that assist monetizers with identity fraud, such as stolen fullz and account, document forgery, SIM swapping, etc.

## 3 PII-BASED AUTHENTICATION

In this paper, we aim to demonstrate what identity fraud monetizers are able to do using stolen PII in the financial ecosystem. More

[1] Such services include marketplaces that sell stolen Social Security Numbers (SSNs), stolen credit/debit cards with full information (fullz), and stolen online accounts, as well as email hijacking, SIM swapping, money transfers, and document forgery.

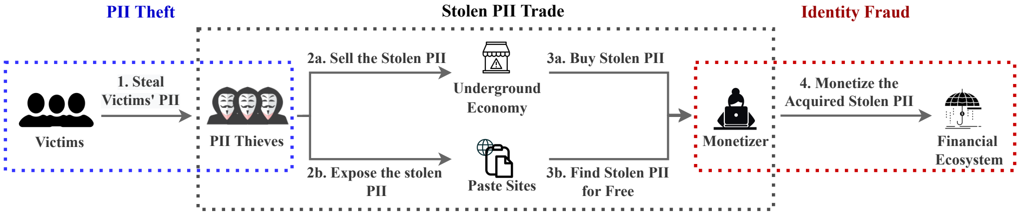


**Figure 1: PII-based impersonation attack includes PII theft, stolen PII trade, and identity fraud in the financial ecosystem.**

specifically, we target the identity fraud methods which break PII-BA using stolen PII. To do so, we analyze the types of PII current PII-BAs request from users in the financial ecosystem, which is a critical step in analyzing how these authentication mechanisms could be bypassed by stolen PII.

**Methodology:** We initiated our analysis by creating a list of ten U.S. representative banks. In this order, we compiled a comprehensive list of thirty prominent U.S. commercial banks, chosen for their significant consolidated assets as reported by the Federal Reserves [36]. This ensured representation of the broader banking landscape in the United States. To mitigate any potential bias, a subset of banks (Bank-1 to Bank-10) was then randomly chosen from this list. We determined that including ten banks from this representative sample would sufficiently demonstrate the potential for identity fraud through the illicit use of stolen Personally Identifiable Information (PII) and its associated costs for the attackers. A similar approach was taken in selecting Payment Processing Companies (PPCs) for analysis [52]. However, due to a smaller pool compared to banks, we opted to randomly select six PPCs (PPC-1 to PPC-6) from the available list. Furthermore, we added an additional PPC (PPC-7) which we collaborated for this study to the final list. Payment processing companies (PPCs) offer financial services that assist businesses in managing customer payments, acting as intermediaries between businesses and customers' banks or credit card issuers.

We focused on five sensitive financial services offered by these institutions, all utilizing PII-BA: *credit card applications*, *account openings*, *online enrollment* (for existing account access), *username retrieval*, and *password resets*. To identify the PII types requested by each institution's PII-BA mechanism for these services (Table 1), we examined their websites and used our own information for *credit card applications* and *account openings*. For *online enrollment*, *username retrieval*, and *password resets*, we utilized our own accounts to navigate the authentication processes. If necessary, we contacted customer service to ensure we had identified all requested PII types.

**Result:** The result of investigating the types of PII that current PII-BAs request from users in the financial ecosystem is shown in Table 1. This table also shows that all selected banks offer the selected services; however, the selected PPCs provide their customers with a subset of the services. Although we disclosed our findings to all the investigated institutions, many have not yet responded. Therefore, we decided to anonymize the investigated financial institutions' names.

## 4 STOLEN IDENTITY RESOURCES

This paper's main goal is to uncover identity fraud opportunities for monetizers in the financial ecosystem by bypassing PII-BA. We also aim to assess the associated costs of impersonation methods.

In Section 3, we analyzed the PII requirements for passing PII-BA in five services offered by 17 financial institutions. In this section, we investigate online resources for stolen PII and illicit services, addressing key questions: (1) Available stolen/leaked PII. (2) The cost of stolen PII. (3) Illicit services aiding identity fraud. (4) Service costs. Then, in Section 5, we use this data to analyze PII-BA vulnerabilities that monetizers can exploit with stolen information and illicit services.

**Investigation Results:** To comprehend the economics of stolen PII trade, we studied U.S. data breaches and illicit services within the underground economy. We also explored paste sites, a common source for monetizers to obtain stolen PII. Figure 2 displays the stolen PII and the illicit services, along with their respective cost ranges for monetizers, as per our research findings.

### 4.1 PII From Data Breaches

Discovering the major available U.S. based data breaches is critical to identifying the volume, type, and price of exposed PII.

**Methodology:** First, we identified recent data breaches that occurred from 2016 to 2021 in U.S. using an API from haveibeenpwned.com (HIBP) [7]. HIBP is a free resource to assess if an email or a phone number has been compromised and appeared in any data breach or paste site. Additionally, this website provides a comprehensive list of recent data breaches, making it a valuable tool for compiling and staying updated on recent data breach incidents. Next, we identified four forums with a significant focus on topics related to PII theft, stolen PII trade, and identity fraud: (1) By interviewing two security experts in a financial institution (interviews were confidential), we collected an initial candidate list of nine underground forums. (2) We refined our list by keeping forums with at least 200 threads on identity fraud-related topics. Our refined list included five underground forums, which were still online and satisfied our condition. (3) To compile our final candidate list, we exhaustively crawled the remaining forums' public content to discover new candidate forum URLs and recursively applied the same refining process to the new candidates. We reached the final list of seven candidate forums through this process. (4) Through a manual analysis of the final candidate forums and considering the status of the forums, the number of threads, and the activity of users, we decided to study

**Table 1: U.S. representative financial institutions that use PII-based authentication along with the required PII and MFA for each service they offer. Gray sections mean that the institution does not offer that specific service.**

| | | Bank-1 | Bank-2 | Bank-3 | Bank-4 | Bank-5 | Bank-6 | Bank-7 | Bank-8 | Bank-9 | Bank-10 | PPC-1 | PPC-2 | PPC-3 | PPC-4<br>PPC-5<br>PPC-6<br>PPC-7 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Credit Card Application | DoB | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ▨ |
| | name | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ▨ |
| | address | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ▨ |
| | SSN/TIN | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ▨ |
| | MMN | | | | | | | ✓ | | ✓ | | | | | ▨ |
| New Account | DoB | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | |
| | name | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | email | | | | | | | | | | | ✓ | ✓ | ✓ | ✓ |
| | address | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | |
| | SSN/TIN | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | |
| | ID card info | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | | | |
| | phone number | | | | | | | | | | | ✓ | | ✓ | |
| | former address | | | | | | ✓ | | | ✓ | | | | | |
| | MMN | | | | | | | | | ✓ | | | | | |
| Online Enrollment | DoB | | | | | | | ✓ | ✓ | ✓ | ✓ | ▨ | ▨ | ▨ | ▨ |
| | name | | | | | | ✓ | ✓ | ✓ | ✓ | | ▨ | ▨ | ▨ | ▨ |
| | email | | | | | | | | | | ✓ | ▨ | ▨ | ▨ | ▨ |
| | SSN/TIN | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ▨ | ▨ | ▨ | ▨ |
| | account/card info | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ▨ | ▨ | ▨ | ▨ |
| | (MFA) phone or email | ✓ | ✓ | ✓ | | | | | | | | ▨ | ▨ | ▨ | ▨ |
| Username Retrieval | PIN | | ✓ | ✓ | | | | ✓ | | | ✓ | | ▨ | ▨ | ▨ |
| | DoB | ✓ | | | | | | | ✓ | | | | ▨ | ▨ | ▨ |
| | email | | | | | | | | | | | ✓ | ▨ | ▨ | ▨ |
| | password | | | | | | | ✓ | | | | | ▨ | ▨ | ▨ |
| | SSN/TIN | ✓ | ✓ | | | ✓ | ✓ | ✓ | ✓ | | ✓ | | ▨ | ▨ | ▨ |
| | (MFA) phone | | ✓ | ✓ | | ✓ | | | | | ✓ | | ▨ | ▨ | ▨ |
| | (MFA) call the branch | | | | ✓ | | | | | ✓ | | | ▨ | ▨ | ▨ |
| | account/card info | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ▨ | ▨ | ▨ |
| | MMN | | | | | | | | ✓ | | | | ▨ | ▨ | ▨ |
| Password Reset | PIN | | ✓ | | ✓ | | | ✓ | | | | | | | |
| | DoB | ✓ | | ✓ | | | | | ✓ | | | | | | |
| | username | | | | | ✓ | ✓ | ✓ | | ✓ | | ✓ | ✓ | ✓ | ✓ |
| | SSN/TIN | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | |
| | (MFA) email | | | | | | | | | ✓ | | ✓ | ✓ | ✓ | ✓ |
| | (MFA) phone | | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | | ✓ | ✓ | ✓ | |
| | (MFA) security word | | | ✓ | | | | | | | | | | | |
| | (MFA) security device | | | | | | | | | | ✓ | | | | |
| | account/card info | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | | | | | | |

✓ Indicates that the selected financial institution request that specific PII in the authentication process of the corresponding service.

Gray Service is not offered by the institution.

four underground forums[2]. We summarize the relative popularity of these forums at the time of our data collection in mid-2021 in Table 2.

Then, to access the selected forums discreetly, we created multiple accounts and engaged in realistic activities to avoid account closures. Additionally, we automated the crawling of the four chosen forums, targeting threads with offers related to significant data breaches. This effort yielded a total of 11,580 posts.

Reputation holds paramount importance in the underground economy, signifying trustworthiness. To ensure credibility, we filtered threads to include only unique posts from high-reputation criminal actors. In three forums (forums #1, #2, and #4), reputation is gauged by the number of satisfied users. We focused on sellers with a minimum of 50 satisfied customers. In the fourth forum (forum #3), seller reputation is rated from zero to five based on user satisfaction, with a focus on those with ratings equal to or greater than three. We analyzed the resulting 978 posts to comprehend the selling options of the selected data breaches.

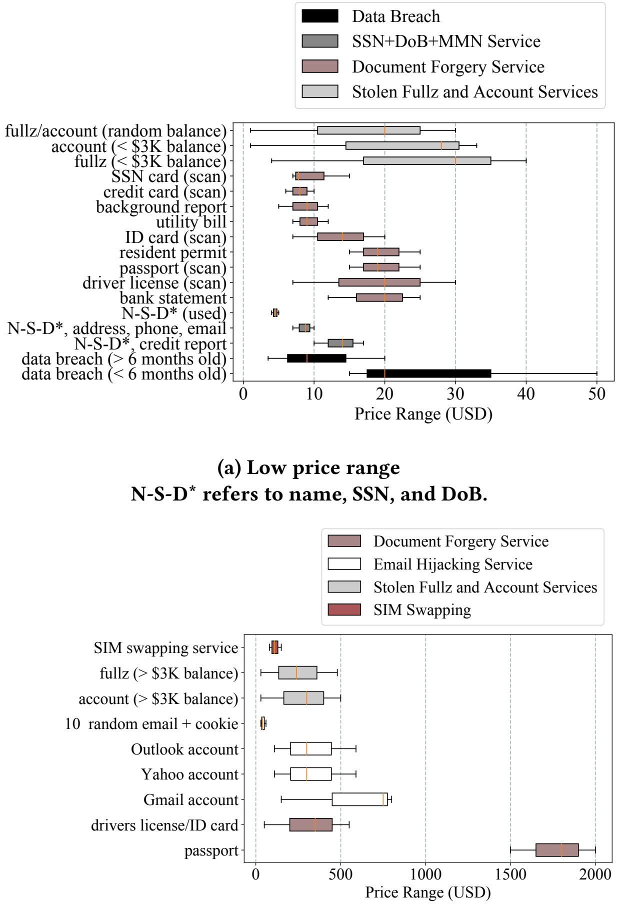
**Table 2: Popularity statistics for the forums we analyzed.**

| Forum | # Threads | # Posts | # Users |
|---|---|---|---|
| Forum #1 | 164,444 | 1,683,720 | 213,458 |
| Forum #2 | 103,117 | 3,188,497 | 642,357 |
| Forum #3 | 69,314 | 352,113 | 187,807 |
| Forum #4 | 11,730 | 71,377 | 213,458 |

**Results:** By analyzing the four selected underground forums, we found 67 highly reputable sellers and four marketplaces offering 382 data breaches. These breaches exposed a massive 7.582 billion records, including 6.056 billion email credentials, 2.317 billion names, 1.257 billion birth dates, 217 million phone numbers, 153 million addresses, 2.3 million mother's maiden names, and 0.2 million Social Security Numbers. These breaches also contained additional data like former addresses and purchase history.

Prices for these breaches depended on freshness, compromised PII types, and the number of records. Prices varied between $3.5 and $20 for a data breach (the entire exposed records by a data breach) more than six months old and $15 to $50 for newer ones (shown as black bars in Figure 2).

[2] Upon our final manual analysis, it was evident that these four underground forums had the highest number of threads and posts concerning identity fraud-related topics within our compiled list.



**(a) Low price range**
**N-S-D* refers to name, SSN, and DoB.**

**(b) High price range**

**Figure 2: Price ranges of stolen PII and complementary illegal services found in the underground economy.**

## 4.2 PII From Paste Sites

To determine available stolen PII, costs, and prevalence, we identify and analyze popular paste sites which help monetizers collect stolen PII.

**Methodology:** We started by identifying popular paste sites known for hosting compromised data. We gathered insights from financial institution security experts, resulting in a list of fifteen monitored paste sites. We complemented this list with paste sites monitored by HIBP, forming a final list of twenty paste sites. Subsequently, we selected ten PII keywords: *SSN*, *tax identification number*, *ID card*, *phone number*, *date of birth*, *address*, *dump*, *identity*, *PII*, and *fullz*. Then, we aimed to locate posts containing these keywords on the selected paste sites. As most paste sites lacked internal search engines, we employed Google Dorking (Google Hacking) [23] and Google Programmable Search Engine (GPSE) [39] to facilitate this search.

We limited the results to the first 200 result pages for each dork searches due to the limitation of the GPSE. Ultimately, we automatically filtered the results to posts with at least ten exposed PII records, analyzed the results.

**Results:** We found 2.021 million exposed records (0.003% of exposed records by the investigated data breaches), including 1,757,984 unique credentials, 8,452 unique names, 6,981 dates of birth, 6,123 phone numbers, 2,266 addresses, and 2,857 SSNs. Our results show that paste sites source PII is negligible in volume compared to underground forums, so we focus on the underground forums in the rest of our analysis.

## 4.3 Complementary Illegal Services

To determine monetizers' abilities, costs, and prevalence, we identify and analyze *illicit services* which help facilitate identity fraud.

**Methodology:** We investigated the same underground forums as in Section 4.1 to uncover illicit complementary services provided by criminals. Initially, we selected twenty keywords closely related to identity fraud.

We automatically collected and stored all threads from May 2020 to May 2021 that contained at least one of these keywords: *Social Security Number*, *tax identification number*, *ID card*, *phone number*, *date of birth (DoB*, *address*, *dump*, *identity*, *PII*, *CVV*, *fullz*, *account hijacking*, *SIM swapping*, *money transfer*, *document forgery*, *CC*, *cash-out*, *carding*, *fraud*, and *bank*. This resulted in 37,580 posts.

Subsequently, we filtered the data to retain unique posts from high-reputation criminals, using the same reputation thresholds as in Section 4.1. This filtering yielded 1,286 posts, which we analyzed to identify illegal services, including monetization services, and the individuals and illicit marketplaces offering them. To access these services, we created accounts on the identified marketplaces that did not require invitations and activated our accounts.

**Results:** By following this methodology, we found five types of illegal services that significantly help monetizers find stolen PII and exploit financial services to make money:

(1) **SSN+DoB+MMN Service.** We identified five illegal marketplaces and 38 individual criminals who sell "bundles" of victims' SSNs together with other PII such as name, address, DoB, mother maiden name (MMN), or phone number. The cost of this service varies between $4 and $17 depending on two main attributes: age (younger victims' PII is in high demand) and the amount of available information about the victim (price ranges shown by dark gray bars in Figure 2).

(2) **Email Hijacking Service.** Email hijacking is a popular service that hackers provide in the underground community [27]. This service is an appropriate solution to bypass email-based 2FA. We identify 12 criminals and one illicit marketplace offering this service. They offer hacking emails from various email providers, such as *Gmail*, *Yahoo*, or *Outlook* using phishing or malware. The cost range of the service offered is $110–$590 for an Outlook or a Yahoo account and $150–$800 for a Gmail account, and the price depends on whether an MFA option is enabled or disabled.

(3) **SIM Swapping Service.** SMS/call MFA is a prevalent MFA method, although it is prone to multiple attacks [40]. One of these attacks is SIM swapping, in which attackers trick a mobile carrier into switching the victim's phone number to a SIM card that they

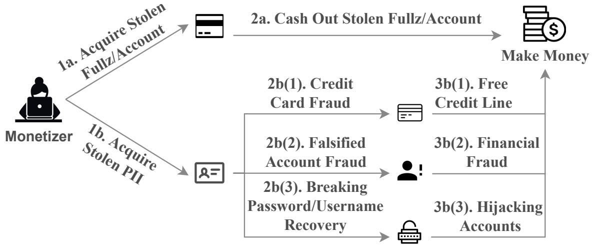

1a. Acquire Stolen Fullz/Account
2a. Cash Out Stolen Fullz/Account
Make Money
Monetizer
1b. Acquire Stolen PII
2b(1). Credit Card Fraud
3b(1). Free Credit Line
2b(2). Falsified Account Fraud
3b(2). Financial Fraud
2b(3). Breaking Password/Username Recovery
3b(3). Hijacking Accounts

**Figure 3: Different methods that monetizers make money from stolen PII in the financial ecosystem.**

own and gain access to SMSs sent to the victim's mobile phone [25]. This attack could be achieved by social engineering or through a rogue employee at a mobile carrier. This illegal service has grown in recent years, and the FBI Internet Crime Complaint Center received 1,611 SIM swapping complaints in 2021, which is five times higher than in 2020 [29]. We identified eight criminals who offer this illegal service to monetizers in the underground economy for various prices from $80 to $150 (red bar in Figure 2) depending on the victim's address and mobile phone carrier.

(4) **Document Forgery Service.** Document forgery is an essential component of a successful identity fraud because identity documents are essential attributes of PII-BA in the financial ecosystem. We identified two dedicated illicit marketplaces and eighteen individual criminals in the underground economy that offer different types of forged documents, such as state ID cards, driver's licenses, passports and credit/debit cards. The prices of these products depend on the type and the quality of the requested document, and it could be as cheap as a couple of dollars, such as $5 for a background report, or thousands of dollars, such as $2,000, for a high-quality passport (prices showed by pink bars in Figure 2).

(5) **Stolen Fullz and Account Services.** *Fullz* here refers to the full information of a credit/debit card with the holder's information, and *account* denotes online banking or PPC account's credential, log, and browser fingerprints. We identified 28 active sellers in the underground forum and six marketplaces that sell stolen fullz and accounts issued by different financial companies. We found that these criminals sell these fullz and accounts mainly based on the card or account issuer institution and the amount of the seller's promised profit. Sellers also use other attributes, such as the country of the issuer institution of the stolen credit/debit card or account and the date of the attack (how fresh the information is). Based on these attributes, our findings show that this service costs $30–$480 for a stolen fullz with more than $3,000 balance and $4–$40 for a stolen fullz with less than $3,000. Likewise, the cost range for a stolen account with more than $3,000 or less than $3,000 balance is $30–$500 and $1–$33, respectively. Moreover, all of the discovered criminals and marketplaces are selling fullz and accounts with unverified random balances for $1–$30, which is essentially gambling for monetizers (all price ranges shown by light gray bars in Figure 2).

# 5 HOW MONETIZERS MAKE MONEY

In this section, we explore how monetizers use stolen PII to make money by targeting the services (described in Section 3) using the resources discussed in Section 4. We consider two ways that monetizers make money from stolen PII: (1) breaking PII-BA of financial institutions' services and (2) directly monetizing stolen PII. An overview of this process is shown in Figure 3. In the case of breaking PII-BA, we consider credit card fraud, creating falsified accounts, and breaking the password/username recovery process. Likewise, in the case of directly monetizing stolen PII, we consider cashing out stolen fullz and accounts. For each monetizing opportunity, we identify vulnerable institutions and estimate the cost to the monetizer to acquire the necessary PII and illegal services (based on Figure 2).

**Monetizers Capabilities.** To procure stolen PII by purchasing *datasets from data breaches* or accessing illicit services such as *SSN+DoB+MMN Service*. Additionally, they can utilize a range of illicit services including *Email Hijacking Service*, *SIM Swapping Service*, *Document Forgery Service*, and *Stolen Fullz and Account Services*. With these resources available, attackers can carefully plan and carry out different types of attacks, adjusting how they use illegal services to fit their harmful goals. Having access to stolen personal information and illegal services gives attackers the ability to get around security measures and take advantage of weaknesses, making their attacks more harmful.

## 5.1 Breaking PII-BA

Figure 4 shows the required PII and illegal services and monetizers' cost for each method of breaking PII-BA using stolen PII in the investigated financial institutions.

### 5.1.1 *Credit Card Fraud.*

Applying for a new credit card allows monetizers to access a line of credit but can leave the victim liable for the debt. However, the monetizer must successfully pass the PII-BA checks of the new credit card application. Table 1 shows that from 13 institutions providing this service (10 banks and 3 PPC), 11 institutions ask for the same PII set. Only two (Bank-7 and Bank-9) require an additional MMN.

In all the data breaches we analyzed, we found 243,000 sets of names, addresses, dates of birth, MMNs, and SSNs, which allow a monetizer to apply for credit cards in all 13 institutions offering this service. We use the price range of data breaches we observed in the underground economy, $3.5 to $50 (per breach), to estimate the cost to the monetizer because our data collection is not comprehensive.

Moreover, a monetizer has access to SSN+DoB+MMN services in the underground economy, which sell specific sets of PII, including all five required PII for $4 to $17.

### 5.1.2 *Creating Falsified Accounts.*

Monetizers start abusing this process by creating a new account using a stolen identity, which we call a *falsified account*. In this regard, when they do not have all the PII needed for bypassing PII-BA of this service, they fabricate the missing PII. After monetizers create a falsified account, although the newly created account has no deposits, they use it in nefarious ways, such as money laundering and anonymous money transferring to make a profit. This emerging financial fraud is becoming more prevalent in recent years.

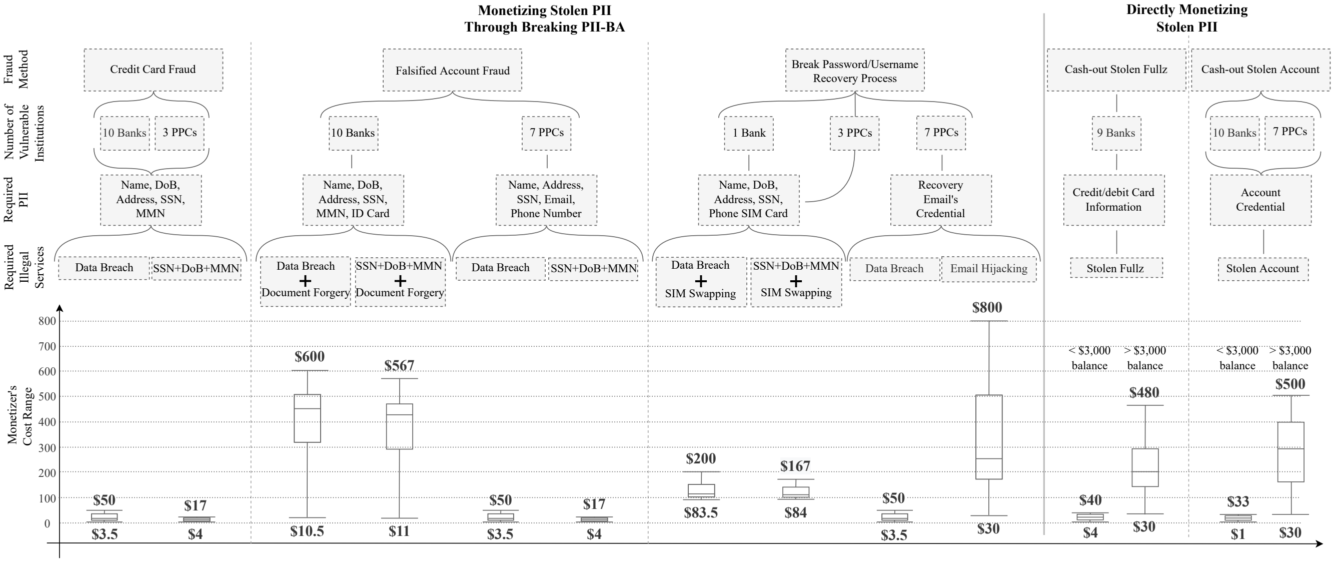


**Figure 4: We consider two ways monetizers make money from stolen PII: breaking PII-BA, on the left side of the diagram (credit card fraud, creating falsified accounts, and breaking password/username recovery processes) and directly monetizing stolen PII, on the right side of the diagram (cashing out stolen fullz and accounts). For each monetizing opportunity, we identify vulnerable institutions and estimate the cost to the monetizer to acquire the necessary PII and illegal services.**

Table 1 illustrates the PII required for creating a new account in the respective financial companies. These pieces of information go through different checks, and if they pass all checks, the account will be created successfully. Therefore, using valid stolen information to create accounts helps monetizers pass these checks successfully.

Figure 4 shows that creating a falsified bank account costs more than a falsified PPC account for monetizers because banks require users to provide a copy of an Identity card (ID card) besides providing multiple PII types. The required PII set to create an account in eight banks includes name, address, date of birth, SSN/TIN, email, a copy of an ID card, and phone number. The other two banks (Bank-6 and Bank-9) require a former address too. Therefore, a monetizer needs to use either a data breach that includes all these required PII types or SSN+Dob+MMN service along with document forgery service, which costs $10.5–$600 and $11–$567 in total, respectively. Moreover, after a successful falsified account creation fraud, monetizers can break PII-BA of the online enrollment process because they have the required PII. Therefore, monetizers can create falsified accounts with online accessibility (e.g., online transaction and activity monitoring) in all investigated banks.

Among the PPCs, two institutions (PPC-1 and PPC-3) require new customers to provide a name, address, email, and phone number, and the other five companies only require name and email. Both of these required PII sets are accessible to monetizers through data breaches or SSN+Dob+MMN service. Therefore, monetizers are able to create falsified accounts in all PPCs by purchasing a data breach ($3.5–$50) or SSN+DoB+MMN service ($4–$17).

### *5.1.3 Breaking Password/Username Recovery.*

As shown in Figure 3, monetizers must obtain the victims' PII required by the target financial institution for password/username recovery to break the PII-BA of the password/username recovery service, hijack the victims' accounts and earn money.

Table 1 shows that banks provide more secure processes for password and username recovery services than online payment institutions by requiring more PII. Nine out of the ten banks require card or account information, security device, security word, or PIN in addition to other PII types (DoB, SSN/TIN, or phone number) for username/password recovery. This additional information makes it difficult for monetizers to break these processes. We could not find these combinations of PII (these nine banks require them for their password/username recovery) in the investigated resources. However, Bank-5 only requires its customers to provide SSN and phone number (SMS MFA) to reset their passwords or retrieve their usernames. Therefore, monetizers can break this bank's password and username recovery processes using either data breaches or SSN+Dob+MMN services in a company with SIM hijacking service for $83.5–$200 and $84–$167, respectively. For a successful attack, the monetizer must use the victim's SSN and a SIM-swapping service to recover the victim's username. Then, the monetizer must use the recovered username, SSN, and SIM swapping service (which usually requires name, date of birth, and address) to recover the password and successfully hijack the accounts.

Among the PPC group, three institutions (PPC-1, PPC-2, and PPC-3) require recovery email credentials or SMS MFA, and the other four only require recovery email credentials, making them an easier target for monetizers. As shown in Figure 4, they can (1) use data breaches and SIM swapping services to break SMS MFA (similar to Bank-5), (2) use data breach to break email MFA ($3.5–$50), or (3) use email hijacking service to break email MFA ($30–$800). Note that the benefit of taking over an online payment account for a monetizer depends on the account balance and other stolen account abuse methods, such as money laundering.

## 5.2 Directly Monetizing Stolen PII

Here, we focus on cashing-out stolen fullz and stolen accounts.

*5.2.1 Cash-out Stolen Fullz.* In this scenario, monetizers first purchase stolen fullz from individual criminals or illicit marketplaces and attempt to cash it out by buying goods, such as gift cards, online services, and luxury items or money transferring via money mules [48]. Based on our investigation results, this attack scenario is the most prevalent due to the high number (34) of sellers and marketplaces who offer stolen fullz. We identified fullz for sale for nine out of 10 banks. From our data, a fullz costs $4–$40 for a stolen fullz with a balance less than $3,000 and $30–$480 for a fullz with a balance more than $3,000 (Figure 4).

*5.2.2 Cash-out Stolen Accounts.* Selling stolen accounts is one of the popular services available in the underground economy—that is, selling full information such as credentials, web browser fingerprints, and cookies (to attempt to bypass risk-based authentication by mimicking the browsing patterns of the victim). Monetizers use the purchased stolen account to perform an account takeover [31, 51] and gain money. In our investigation in Section 4, we identified stolen accounts available for purchase for all 17 financial institutions. We discovered the cost range of acquiring a stolen bank/PPC account is $1–$33 for accounts with less than $3,000 and $30–$500 for accounts with more than $3,000 balance.

# 6 POTENTIAL MITIGATION APPROACHES

In this section, we discuss potential PII-BA mechanism improvements in the financial ecosystem.

## 6.1 Cross-account Authentication

Nine out of ten investigated banks request card/account information, security word, security device, or PIN along with other PII and MFAs in their password/username recovery PII-BA. In our investigation we found the chance of purchasing all these pieces of information together very low. Consequently, requesting the same PII can be used by the other banks and PPCs. Moreover, PPCs can enhance password/username recovery PII-BA by adding cross-account authentication using credit/debit card associated with the account or account information. This approach can also be extended to other PII-BA methods for potential improvements. Similarly, mobile carriers can employ this method to prevent SIM swapping.

On the other hand, increasing PII requirements in PII-BA methods may lead to unintended consequences, such as the need to store more PII in databases, which, if compromised, could enable more sophisticated identity fraud.

## 6.2 Increase Monetization Cost and Effort

**Breaking Password/Username Recovery Process.** Figure 4 reveals that all PPCs and one bank are vulnerable to this attack scenario, emphasizing the risks. Moreover, data breaches commonly expose email credentials, available for $3.5 to $50 per breach. Therefore, relying solely on email MFA, as all investigated PPCs do, is risky. Introducing phone SMS/call MFA increases costs by $80 and reduces success rates (due to SIM swapping challenges), making it a potential substitute for email MFA. Similarly, phone authentication applications and security device MFA offer alternatives, but they come with trade-offs between security and usability, ultimately raising monetization costs.

**Credit Card Fraud.** Current PII-BA techniques used for applying credit card services are prone to impersonation because they rely on requesting sets of PII that are available to monetizers through data breaches or SSN+DoB+MMN. A potential improvement is requesting PII types that are more expensive for monetizers to purchase, such as providing a high-quality ID card scan to increase cost while maintaining the possibility of online application.

**Falsified Account Fraud.** Detecting and mitigating account fraud is crucial in finance. Figure 4 highlights vulnerability across all financial institutions. Banks raise the cost for attackers by requesting ID card scans (Figure 4). Therefore, PPCs can enhance their account creation PII-BA by incorporating high-quality ID card scans.

## 6.3 Digital Identity Authentication

Digital Identity Authentication allows people to prove their legal identity online. Companies that provide this service use multiple methods to verify their clients' identities confidently. A potential improvement for authentication mechanisms in the financial ecosystem (based on our informal interview with our collaborator PPC) is adopting the identity verification methods that this service is using or partnering with companies, such as *ID.me* [16]. The mentioned identity verification methods are (1) Remote Document Verification, in which service providers parse the document images a client uploads, extract content from it, and apply a proprietary database of rules and Artificial Intelligence methods to verify the document's authenticity. (2) Face Matching requires clients to provide a selfie to compare it with the picture on the uploaded ID document. In the case of an unsatisfactory result, service providers ask users for a virtual video call to verify the face matching.

# 7 ETHICAL CONSIDERATIONS

In this study, we explored two primary resources of stolen PII and related illegal services: *underground community* and *paste sites*. We secured approval from our Institutional Review Board (IRB) for an ethical protocol that balances research objectives with potential risks.

**Underground Economy.** Engaging in a study involving interactions with criminal entities presents ethical challenges, which we will discuss, along with the steps we took to address them.

1. **Understanding PII from Data Breaches.** We inspected the volume, price, exposure year, and type of exposed PII of 382 U.S.-based data breaches without purchasing PII or interacting with criminals.
2. **Understanding Illicit Services.** We discovered illicit marketplaces and individual service providers of illegal complementary services and investigated their types and prices. We did not contact criminals or purchase any of the identified services.

**Paste Sites Investigation.** In the paste sites investigation, we automatically downloaded publicly available posts, ran automated experiments, and securely deleted the data. To validate the process, we manually viewed a small sample of the data which was immediately discarded.

**Dual-Use Risks.** While there is a risk that our findings could be used by cybercriminals to enhance their operations, we believe it's vital to openly study and share knowledge of their activities to develop effective countermeasures. To mitigate this risk, we redacted the names of financial institutions studied in the paper and made efforts to contact and disclose identified flaws, detailed in Section 8.

## 8 DISCUSSION

**Responsible Disclosure.** The importance of our findings necessitates the responsible disclosure of the results of our paper to the affected financial institutions. In this regard, we disclosed our findings and offered remediations to every vulnerable company through bug bounty programs or contact points dedicated to security issues reporting. During the writing period, two companies (PPC-3 and PPC-1) responded and requested a detailed report. After providing the reports, we set up an offline interview with one of them to get more insight into their countermeasure, which is discussed in detail in Section 6. The other companies did not respond to us; however, due to the importance of our findings, we reached out to their security team members over either the LinkedIn platform or email. Therefore, we decided to anonymize the investigated financial institutions' names throughout the paper.

**Identity Theft Protection Services.** Consumers can use identity protection services like IdentityGuard [15] to help mitigate identity theft. These services continuously monitor for exposed identities, notify clients in case of theft, and assist in minimizing potential consequences. While they aid in protecting accounts, they may not have access to all stolen PII and cannot mitigate all consequences [26].

**Future Work.** In future research endeavors, researchers can explore the testing of the quality of identified stolen PII and illicit services discovered in criminal resources. This collaborative effort will involve providing access to the datasets and methodologies utilized in the study to enable comprehensive evaluations by other researchers. Additionally, further exploration into simulating scenarios using stolen PII, with the requisite consent from victims, can expand the understanding of identity fraud risks. Furthermore, the assessment of mitigation strategies mentioned in the findings will be open to scrutiny and analysis by the research community, fostering a collective effort towards enhancing security measures against identity fraud.

## 9 LIMITATIONS

Our analysis is based on a dataset we collected by investigating data breaches, stolen PII, and illegal services found in four underground forums and twenty paste sites, which leads to incomplete coverage. Moreover, we did not consider other sources of PII, such as public social media platforms (Facebook, Instagram, LinkedIn, etc.). However, our data set allows us to analyze the cost of various monetizing methods of stolen identities in the ecosystem. Consequently, our perspective of the stolen PII trade and fraud scale should be considered a lower bound. Moreover, because we built our monetizer cost analysis on our dataset, which covers some resources and capabilities, our cost analyses could be off in both directions.

Moreover, to validate the stolen PII and illicit services within the underground economy, explore potential avenues for identity fraud, and develop effective mitigations, collaboration with a financial company is essential.

## 10 RELATED WORK

*Password-based authentication* relies on usernames and passwords for user account verification [1]. Research has already delved into the security and privacy issues associated with this method [1, 17, 45]. *MFA* aims to create another level of security for user accounts, and prior research has also explored its security and usability across different platforms [5, 12, 35]. *Risk-based authentication* creates user profiles based on various factors like browser features and behavior to evaluate the risk of account compromise during login. It complements other authentication methods when login attempts seem suspicious. However, bypassing this scheme is possible through techniques like browser fingerprinting [20], device fingerprinting [8], and tracking mechanisms [9].

*PII theft* threatens all three authentication schemes, password-based, MFA, and risk-based authentication, which would lead to *identity frauds* such as account take-over and credential stuffing [45, 51]. To the best of our knowledge, authentication-related research has not explored the impact of PII theft on *PII-BA*. Our focus is on PII-BA within the financial sector and the consequences of PII theft on its security. We utilize underground forums and paste sites as sources of stolen PII and related illegal services for identity fraud in the financial ecosystem.

Researchers have quantified cybercrime's commoditization by scrutinizing transactions in the underground economy and illicit marketplaces, revealing the prevalence and quality of illegal services [43, 48]. Haslebacher et al. [13] presented evidence of financial product trade on online forums, detailing the stolen financial data and the reputation of criminals. However, they did not investigate the ramifications of these illegal data trades on PII-BA and omitted an analysis of illicit services facilitating identity fraud within the financial ecosystem.

In the area of PII theft, there have also been several quantitative and qualitative studies. For instance, the relation between users' online activities and PII theft victimization was investigated [2, 49]. Salvin and Nimkit [38] analyzed age as a significant risk factor for PII theft and fraud victimization showing that older people and their dependents are victimized more. Researchers have also studied the effects of fear of PII theft victimization on online purchase intention [18, 19].

Due to the prevalence of PII theft, other researchers investigated PII theft protection and detection methods [14, 22, 24, 50]. Selection of a proper detection method is crucial; therefore, prior work provided a quantitative analysis of various identity fraud detection services [26, 37]. Current identity fraud detection services limit the amount of identity fraud in the financial ecosystem, but they can not stop the occurrence of PII theft. Therefore, users may decide to partially adopt or abandon identity fraud detection services [54].

## 11 CONCLUSION

The ability for criminals to easily purchase PII and monetize it fuels the cybercrime engine. This paper demonstrates that relying on PII to remain *private* for PII-BA is simply not viable. Therefore, we must rethink identity verification and consider PII as Public Identifiable Information. The next step in the battle against cybercrime must be for financial organizations to improve their PII-BA by asking for difficult and expensive to acquire PII. This method will increase the effort and cost of successfully breaking PII-BA using stolen PII for criminals. Moreover, financial companies can adopt authentication methods introduced by digital identity authentication or partner with companies that provide to improve their PII-BA mechanisms.

## REFERENCES

[1] Marina Sanusi Bohuk, Mazharul Islam, Suleman Ahmad, Michael Swift, Thomas Ristenpart, and Rahul Chatterjee. 2022. Gossamer: Securely measuring password-based logins. In *31st USENIX Security Symposium (USENIX Security 22)*. 1867–1884.

[2] David Burnes, Marguerite DeLiema, and Lynn Langton. 2020. Risk and protective factors of identity theft victimization in the United States. *Preventive Medicine Reports* 17 (2020), 101058.

[3] Blake Butler, Brad Wardman, and Nate Pratt. 2016. REAPER: an automated, scalable solution for mass credential harvesting and OSINT. In *2016 APWG symposium on electronic crime research (eCrime)*. IEEE, 1–10.

[4] Mark Button and Cassandra Cross. 2017. *Cyber frauds, scams and their victims*. Taylor & Francis.

[5] Stéphane Ciolino, Simon Parkin, and Paul Dunphy. 2019. Of Two Minds about Two-Factor: Understanding Everyday FIDO U2F Usability through Device Comparison and Experience Sampling. In *SOUPS*.

[6] Federal Financial Institutions Examination Council. 2005. Authentication in an internet banking environment. *FFIEC gencies (August 2001 Guidance)* (2005).

[7] Lyle Daly. 2020. have i been pwned? https://haveibeenpwned.com/.

[8] Peter Eckersley. 2010. How unique is your web browser?. In *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 1–18.

[9] Steven Englehardt and Arvind Narayanan. 2016. Online tracking: A 1-million-site measurement and analysis. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 1388–1401.

[10] Federal Trade Commission. 2022. New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021. https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0.

[11] Rajeev K Goel. 2019. Identity theft in the internet age: Evidence from the US states. *Managerial and Decision Economics* 40, 2 (2019), 169–175.

[12] Maximilian Golla, Grant Ho, Marika Lohmus, Monica Pulluri, and Elissa M Redmiles. 2021. Driving 2FA Adoption at Scale: Optimizing Two-Factor Authentication Notification Design Patterns. In *USENIX Security*.

[13] Andreas Haslebacher, Jeremiah Onaolapo, and Gianluca Stringhini. 2017. All your cards are belong to us: Understanding online carding forums. In *2017 APWG symposium on electronic crime research (eCrime)*. IEEE, 41–51.

[14] Bing-Zhe He, Chien-Ming Chen, Yi-Ping Su, and Hung-Min Sun. 2014. A defence scheme against identity theft attack based on multiple social networks. *Expert Systems with Applications* 41, 5 (2014), 2345–2352.

[15] Identity Guard. 2020. Identity Guard. https://www.identityguard.com.

[16] ID.me. 2022. The Digital Wallet that Puts You in Control. https://www.id.mei.

[17] Gokul Chettoor Jayakrishnan, Gangadhara Reddy Sirigireddy, Sukanya Vaddepalli, Vijayanand Banahatti, Sachin Premsukh Lodha, and Sankalp Suneel Pandit. 2020. Passworld: A serious game to promote password awareness and diversity in an enterprise. In *SOUPS*.

[18] Gašper Jordan, Robert Leskovar, and Miha Marič. 2018. Impact of fear of identity theft and perceived risk on online purchase intention. *Organizacija* 51, 2 (2018), 146–155.

[19] Charles M Kahn and José M Liñares-Zegarra. 2016. Identity theft and consumer payment choice: Does security really matter? *Journal of Financial Services Research* 50, 1 (2016), 121–159.

[20] Soroush Karami, Faezeh Kalantari, Mehrnoosh Zaeifi, Xavier J Maso, Erik Trickel, Panagiotis Ilia, Yan Shoshitaishvili, Adam Doupé, and Jason Polakis. 2022. Unleash the Simulacrum: Shifting Browser Realities for Robust Extension-Fingerprinting Prevention. In *31st USENIX Security Symposium (USENIX Security 22)*. 735–752.

[21] Sowmya Karunakaran, Kurt Thomas, Elie Bursztein, and Oxana Comanescu. 2018. Data breaches: User comprehension, expectations, and concerns with handling exposed data. In *SOUPS*.

[22] Hana Kim, Byung Il Kwak, and Huy Kang Kim. 2015. A study on the identity theft detection model in MMORPGs. *Journal of The Korea Institute of Information Security & Cryptology* 25, 3 (2015), 627–637.

[23] Alekya Sai Laxmi Kowta, Karan Bhowmick, Jeev Ratan Kaur, and N Jeyanthi. 2021. Analysis and overview of information gathering & tools for pentesting. In *2021 International Conference on Computer Communication and Informatics (ICCCI)*. IEEE, 1–13.

[24] James R LaPiedra et al. 2016. *Identity Lockdown: Your Step-By-Step Guide to Identity Theft Protection*. Lulu. com.

[25] Kevin Lee, Benjamin Kaiser, Jonathan Mayer, and Arvind Narayanan. 2020. An Empirical Study of Wireless Carrier Authentication for SIM Swaps. In *Sixteenth Symposium on Usable Privacy and Security SOUPS 2020)*. 61–79.

[26] David Liau, Razieh Nokhbeh Zaeem, and K Suzanne Barber. 2020. A Survival Game Analysis to Common Personal Identity Protection Strategies. (2020).

[27] Ariana Mirian, Joe DeBlasio, Stefan Savage, Geoffrey M Voelker, and Kurt Thomas. 2019. Hack for hire: Exploring the emerging market for account hijacking. In *The World Wide Web Conference*. 1279–1289.

[28] Adam Oest, Penghui Zhang, Brad Wardman, Eric Nunes, Jakub Burgis, Ali Zand, Kurt Thomas, Adam Doupé, and Gail-Joon Ahn. 2020. Sunrise to Sunset: Analyzing the End-to-end Life Cycle and Effectiveness of Phishing Attacks at Scale. In *29th USENIX Security Symposium (USENIX Security 20)*.

[29] Federal Bureau of Investigation. 2022. Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public. https://www.ic3.gov/Media/Y2022/PSA220208.

[30] U.S. Department of Labor. 2020. Guidance on the Protection of Personal Identifiable Information. https://www.dol.gov/general/ppii.

[31] Jeremiah Onaolapo, Enrico Mariconti, and Gianluca Stringhini. 2016. What happens after you are pwnd: Understanding the use of leaked webmail credentials in the wild. In *Proceedings of the 2016 Internet Measurement Conference*. 65–79.

[32] Ori Or-Meir, Nir Nissim, Yuval Elovici, and Lior Rokach. 2019. Dynamic malware analysis in the modern era—A state of the art survey. *ACM Computing Surveys (CSUR)* 52, 5 (2019), 1–48.

[33] I Ponemon. 2018. cost of a data breach study: Global overview. *Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC* (2018).

[34] Ryan Randa and Bradford W Reyns. 2020. The physical and emotional toll of identity theft victimization: A situational and demographic analysis of the National Crime Victimization Survey. *Deviant Behavior* 41, 10 (2020), 1290–1304.

[35] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. 2019. A Usability Study of Five Two-Factor Authentication Methods. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 357–370.

[36] Federal Reserve. 2022. Federal Reserve Statistical Release. www.federalreserve.gov/releases/lbr/current/.

[37] I Sadgali, N Sael, and F Benabbou. 2019. Performance of machine learning techniques in the detection of financial frauds. *Procedia computer science* 148 (2019), 45–54.

[38] Paul Salvin and Nimkit Lepcha. 2019. Financial Frauds and Scams. *Encyclopedia of Gerontology and Population Aging* (2019), 1–7.

[39] Irina Shamaeva and David Galley. 2021. *Custom Search–Discover more:: A Complete Guide to Google Programmable Search Engines*. Chapman and Hall/CRC.

[40] Hossein Siadati, Toan Nguyen, Payas Gupta, Markus Jakobsson, and Nasir Memon. 2017. Mind your SMSes: Mitigating social engineering in second factor authentication. *Computers & Security* 65 (2017), 14–28.

[41] Zhibo Sun, Adam Oest, Penghui Zhang, Carlos Rubio-Medrano, Tiffany Bao, Ruoyu Wang, Ziming Zhao, Yan Shoshitaishvili, Adam Doupé, Gail-Joon Ahn, et al. 2021. Having Your Cake and Eating It: An Analysis of Concession-Abuse-as-a-Service. In *30th USENIX Security Symposium (USENIX Security 21)*. 4169–4186.

[42] Zhibo Sun, Carlos E Rubio-Medrano, Ziming Zhao, Tiffany Bao, Adam Doupé, and Gail-Joon Ahn. 2019. Understanding and predicting private interactions in underground forums. In *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy*. 303–314.

[43] Kurt Thomas, Danny Huang, David Wang, Elie Bursztein, Chris Grier, Thomas J Holt, Christopher Kruegel, Damon McCoy, Stefan Savage, and Giovanni Vigna. 2015. Framing dependencies introduced by underground commoditization. (2015).

[44] Kurt Thomas, Frank Li, Ali Zand, Jacob Barrett, Juri Ranieri, Luca Invernizzi, Yarik Markov, Oxana Comanescu, Vijay Eranti, Angelika Moscicki, et al. 2017. Data breaches, phishing, or malware? Understanding the risks of stolen credentials. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*. 1421–1434.

[45] Kurt Thomas, Jennifer Pullman, Kevin Yeo, Ananth Raghunathan, Patrick Gage Kelley, Luca Invernizzi, Borbala Benko, Tadek Pietraszek, Sarvar Patel, Dan Boneh, et al. 2019. Protecting accounts from credential stuffing with password breach alerting. In *USENIX Security*.

[46] Tala Vahedi, Benjamin Ampel, Sagar Samtani, and Hsinchun Chen. 2021. Identifying and Categorizing Malicious Content on Paste Sites: A Neural Topic Modeling

Approach. In *2021 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE, 1–6.

[47] Steve GA van de Weijer, Rutger Leukfeldt, and Wim Bernasco. 2019. Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology* 16, 4 (2019), 486–508.

[48] Rolf Van Wegberg, Samaneh Tajalizadehkhoob, Kyle Soska, Ugur Akyazi, Carlos Hernandez Ganan, Bram Klievink, Nicolas Christin, and Michel Van Eeten. 2018. Plug and prey? measuring the commoditization of cybercrime via online anonymous markets. In *27th USENIX security symposium (USENIX security 18)*. 1009–1026.

[49] Zoran Vučković, Dragan Vukmirović, Marina Jovanović Milenković, Slobodan Ristić, and Katarina Prljić. 2018. Analyzing of e-commerce user behavior to detect identity theft. *Physica A: Statistical Mechanics and its Applications* 511 (2018), 331–335.

[50] Cheng Wang, Bo Yang, and Jing Luo. 2017. Identity theft detection in mobile social networks using behavioral semantics. In *2017 IEEE International Conference on Smart Computing (SMARTCOMP)*. IEEE, 1–3.

[51] Ke Coby Wang and Michael K Reiter. 2020. Detecting Stuffing of a User's Credentials at Her Own Accounts. In *USENIX Security*.

[52] Wikipedia contributors. 2022. List of online payment service providers — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=List_of_online_payment_service_providers&oldid=1123747838 [Online; accessed 6-December-2022].

[53] Jim Zaiss, Razieh Nokhbeh Zaeem, and K Suzanne Barber. 2019. Identity threat assessment and prediction. *Journal of Consumer Affairs* 53, 1 (2019), 58–70.

[54] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. 2020. Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–15.

## 12 APPENDIX

As mentioned in Section 4.2, we investigated 20 popular pastes sites (Table 3) to identify the approximate number of leaked PII in this type of stolen PII resource.

Moreover, as we mentioned in Section 3, we disclosed our findings to all the investigated institutions; however, many did not respond. Therefore, we decided to anonymize the investigated financial institutions' names throughout the paper. Tables 4 and 5 show some statistics about the selected financial companies.

**Table 3: Selected paste sites for stolen PII investigation.**

| | Paste Site | Availability Status |
|---|---|---|
| 1 | pastebin.com | active |
| 2 | pastie.com | active |
| 3 | slexy.org | active |
| 4 | ghostbin.com | active |
| 5 | justpaste.com | active |
| 6 | pastefs.com | active |
| 7 | codepad.org | active |
| 8 | controlc.com | active |
| 9 | paste4btc.com | active |
| 10 | paste.ee | active |
| 11 | bitbin.it | active |
| 12 | paste.rohitab.com | active |
| 13 | jsitor.com | active |
| 14 | pastebin.osuosl.org | active |
| 15 | plnkr.co | active |
| 16 | rentry.co | active |
| 17 | paste.scratchbook.ch | active |
| 18 | pastebin.ulvis.net | active |
| 19 | pastebin.pl | active |
| 20 | pastelink.net | active |
| 21 | quickleak.se | inactive |
| 22 | adhocurl.com | inactive |
| 23 | permanentoptout.com | inactive |
| 24 | optout.com | inactive |

**Table 4: Consolidated and domestic assets of the selected U.S. commercial banks, as of September 2022.**

| Financial Institution | Consolidated Assets (in million dollars) | Domestic Assets (in million dollars) |
|---|---|---|
| Bank-1 | 3,308,575 | 2,521,739 |
| Bank-2 | 2,407,902 | 2,286,214 |
| Bank-3 | 1,714,474 | 1,038,239 |
| Bank-4 | 553,395 | 551,701 |
| Bank-5 | 591,211 | 582,319 |
| Bank-6 | 394,332 | 394,332 |
| Bank-7 | 1,712,442 | 1,689,553 |
| Bank-8 | 120,288 | 120,288 |
| Bank-9 | 178,715 | 178,715 |
| Bank-10 | 124,556 | 124,556 |

**Table 5: Number of active users of the selected Online Payment Companies(PPCs), as of mid-2022.**

| Financial Institution | Number of Users in 2022 (in millions) |
|---|---|
| PPC-1 | 432 |
| PPC-2 | 600 |
| PPC-3 | 83 |
| PPC-4 | 0.03 |
| PPC-5 | 3.1 |
| PPC-6 | 3 |
| PPC-7 | 1,300 |