

Identity theft
accounts for almost
half of all fraud in
the UK.¹



IDENTITY THEFT: WHAT THE FUTURE HOLDS



Making sure
it's secure.™

The largest ever
fine for a UK
data breach,
which put 11 million
citizens' data at risk,
is £980,000²



TABLE OF CONTENTS

- 3 Identity Theft Crimes
- 4 Businesses Are Targets Too
- 5 The Impact is Widespread & Risks Are Growing
- 6 Reduce Your Risks
- 7 Businesses Need to Take Precautions
- 9 Insider Threats On The Rise
- 10 What Can You Do?
- 11 Additional Best Practices
- 12 How Shred-it Can Help

Thanks to advances in technology, businesses can now reach new markets and connect with employees around the globe with the touch of a key. Customers can buy products from stores around the corner or around the world and pay for them faster and easier than ever before with mobile wallets, online payment tools and virtual currency.

But all of this convenience has opened opportunities for thieves to steal personal information, resulting in a global epidemic of identity theft crimes. Research suggests that identity theft has impacted 27% of the UK adult population at some point in time, with identity thieves making off with over £3.3 billion in stolen funds in one year alone.³ Unfortunately, every advance in technology and security to better safeguard information is being quickly met by a smarter, more innovative thief who finds new ways of accessing and using your personal data.

IDENTITY THEFT CRIMES

Identity theft crimes are more than the security breaches that you often see in headlines. They are crimes that happen in a lot of different ways, including:

- Identity thefts where documents, such as bank statements, containing personal information are stolen from home or office waste bins.
- Stolen (or cloned) payment cards.
- Social media feeds that provide criminals with the information they need (such as name, address and birthday).
- Impersonation crimes where someone calls and provides you with some information to “verify authenticity” and indicates you owe taxes or fines and need to pay right away.
- Employment fraud, whereby forged or stolen identity documents are used in order to obtain employment. False documents account for 12.9% of all successful employment application fraud.⁴
- New account fraud: Chip and pin cards make it harder for criminals to steal your credit card data but armed with your name, address, date of birth and other personal details, thieves can open up new bank accounts and credit cards in your name. It often takes a long time to identify these fraudulent accounts and the damage to a person’s credit is already done.

Fraud costs the UK economy approx. £52 billion annually⁵



BUSINESSES ARE TARGETS TOO

Individuals aren't the only target of identity theft. Criminals have started targeting businesses of all sizes putting them at increased risk of a data breach. For small businesses, this kind of a data breach can be fatal. **93% of companies that suffer data loss for more than 10 days file for bankruptcy within a year.**⁶

How does business identity theft happen?

Fraudulent orders: Thieves order products or services in a company name and use stolen cheques or credit cards for payment.

Big purchases on credit: Corporate credit cards and corporate accounts have larger limits and less scrutiny on purchases so it is much more difficult to identify abnormal purchasing behaviour.

Thieves take advantage of minimal security: Many businesses do not have the time to closely scrutinise purchases and often take more time to reconcile purchases, buying criminals time to get away with the theft.

Easily accessible information is leveraged: It's not hard to get the information needed about a company to establish fraudulent credit. Business names and addresses, incorporation details and registration numbers are readily available online.

Here are some scams you might not know about that specifically target businesses.

Fake Office Supply: Scammers use fake and urgent invoices to get paid for non-existent products, services or online advertising.

Affinity: This is the number one scam identified by the Better Business Bureau. A fraudster infiltrates a closed community, gains workers trust and steals money through an investment scheme.

Directory Listing Check: A caller verifies a listing in a (fake) business directory and then charges for it.

Malware: While this one seems obvious, it remains a significant threat that is expected to move from infiltrating computers to targeting smart phones where it can access a range of personal and corporate information. This makes the inter-connectivity of our devices both beneficial and a threat.



THE IMPACT IS WIDESPREAD & RISKS ARE GROWING

There may be a new victim of identity theft every eight seconds⁷ in the UK, but the news is not all bad. There are steps everyone can take to reduce their risks of becoming the next identity theft target. It all starts with knowing the vulnerabilities and counteracting the threats.

48% of loyal consumers avoid retailers after a security breach⁸



REDUCE YOUR RISKS

Here are some common tactics thieves use to steal personal information and tips on how you can reduce your risks.

- **Threats on the go:** 58% of adults use their phones to go online¹⁰, and more than 1 in 4¹¹ mobile phones are lost/stolen every year in the UK. Protect your phone's data with a passcode, keep operating software up to date, log out of software that's not in use and turn off Wi-Fi and Bluetooth when you don't need them.
- **Secure your sharing:** With the positive marketing benefits of social media come real threats to security. Social media can be targeted to steal corporate information or trade secrets, or even employee or customer information. Make sure social media strategies are part of your security plan, provide guidelines for acceptable posting and give employee training detailing what can and can't be discussed online. A simple "like" online, coupled with birthday wishes might seem innocuous but can provide fraudsters with a lot of information.
- **Keep up to date:** Software companies regularly update their solutions as vulnerabilities are identified. Don't make it easy for thieves. Keep your software patches up to date to minimise software risks.
- **Don't "remember" passwords:** It might seem simple but not having your computer remember your passwords can help prevent theft in the event a device is stolen. Make your password hard to crack using unique or complex combinations of letters and numbers, and never use the same passwords for multiple sites.
- **Sophisticated 'phishing':** We might all know not to click on an email claiming that we've won the lottery we didn't enter in a country we've barely heard of but fraudsters are getting more sophisticated posing as your bank or favourite online store. Assume any email that you didn't initiate is fraud. If you are not sure, call the company or visit their website. Never click on the link provided or enter information without verifying the source.
- **Watch downloads:** Apps and software can be the opening thieves are looking for. Ensure all software and apps are downloaded from reputable sources and have been scanned for worms, key loggers and Trojan horses.
- **Lock down devices:** It might seem obvious but all mobile technology needs to have secure passwords and should have software to wipe the drives if the device is lost or stolen. This goes for laptops, smartphones and any wearable device including new smartwatch technology.



BUSINESSES NEED TO TAKE PRECAUTIONS

While all of the previous tips might seem to focus on the consumer, all businesses should include these strategies in their security policies. To further safeguard your company from identity theft and fraud, it's important to recognise the role employees play. To ensure your security processes aren't breached by an activity an employee initiated, they need to understand the risks and be trained on your policies.

Office equipment, laptops, and smartphones might seem like obvious places for criminals to target for identity theft and fraud, but there are some less obvious and often overlooked areas of an office that could leave you vulnerable to a privacy breach.

Five vulnerable (and often ignored) areas in an office include:

Office Area	Why It's Vulnerable	How to Negate Risks
<p>1. Printers</p>	<p>Papers left on printers can be picked up by anyone.</p>	<p>Implement access codes that have to be entered on the printer to complete the print job. This ensures that the employee is there to pick up the document as soon as it's printed.</p>
<p>2. Recycling Bins</p>	<p>Confidential papers can be thrown into recycling bins as employees try to be environmentally conscious.</p>	<p>A Shred-All Policy eliminates document handling mistakes; and, when using a reputable document destruction company, paper can be recycled after shredding – making sure your green initiatives are upheld.</p>
<p>3. Messy Desks</p>	<p>Files piled on a desk or in trays can be easily picked up or read by anyone walking by.</p>	<p>A Clean Desk Policy ensures all files are put away under lock and key, forcing employees to be better organised and boosting security.</p>
<p>4. Electronic Storage Devices</p>	<p>External hard drives, USB keys and even cloud services make it easy to bring files with us, but they could also increase risks of fraud. Small drives can be stolen and used by outsiders and not all cloud services are as secure as we think.</p>	<p>Encrypt any and all data being taken outside the office.</p> <p>When electronic devices are outdated or will be retired, don't rely on software to wipe the contents; ensure they are permanently destroyed so the data can never be recovered.</p> <p>Verify the security protocols of your cloud service providers and limit what can and can't be uploaded or accessed remotely.</p>
<p>5. Offsite Locations (hotels, cars, aeroplanes, taxis and cafés)</p>	<p>With more and more employees working remotely, corporate data is being opened digitally from anywhere and files are leaving the office more often than ever before. They could be left in hotels or airports or accessed over unsecure Wi-Fi.</p>	<p>Document a strict policy about what files can and can't leave the office – physically or digitally.</p> <p>Instruct staff on proper secure access and disposal of information when offsite.</p> <p>Train staff on safe offsite practices to reduce risks from laptops and other portable devices.</p> <p>Ensure all devices have remote wipe capabilities in the event of theft or loss.</p>

INSIDER THREATS ON THE RISE

Not all fraud and identity theft crimes are perpetrated by faceless outsiders or hackers who take advantage of system vulnerabilities. Some threats come from the inside and by that we mean your employees.

Employees can, either maliciously or accidentally, do things that put a company and its data at risk. A U.S. study of mega data breaches flagged that in one third of data breach cases, it took companies two or more years to discover a breach, and in 55% of cases the cause of the breach was never identified.⁹

When corporate data is being threatened from the inside, businesses require more stringent processes, as well as control over who can and can't access the data. Companies have to take a firmer approach to securing information. File servers, cloud services and databases should have strict access controls and all activity levels should be monitored. This includes the external and internal downloading of information that could point to potential theft.

Increased monitoring and control can help reduce the time it takes to identify breaches.

27% of UK companies are concerned about information theft from their own employees¹²



WHAT CAN YOU DO?

The problem of identity theft is global but there are a lot of everyday things that consumers and businesses can do to protect themselves:

- Implement a Shred-All Policy
- Ensure employees follow a Clean Desk Policy
- Outline crisis plans to specify document management processes
- Develop document lifecycle management protocols for storing and disposing of confidential information. All confidential documents must be identified, labeled and securely stored until no longer needed, with a plan for secure destruction at the end of life.

Integrate these best practices into your security protocols and make sure your staff are regularly trained and audited to verify compliance with the policies.

In addition, businesses need to make sure that their staff aren't taking undue risks with office technology that could compromise internal security. Make sure to provide clear policies and regular, ongoing training that covers:

- Remote access to information
- Downloading of software and apps
- Safe surfing and online access
- Digital security including passwords



ADDITIONAL BEST PRACTICES

Here are some additional best practices that can help to reduce risks from inside and outside security threats.

1. **Hotlines:** Although not new, hotlines that let employees share information about suspicious behaviour are effective and have been associated with a 54.5% reduction in fraud losses.¹³
2. **Data Monitoring:** Proactive monitoring of access to information and online activity can help reduce fraud by up to 60%.¹³
3. **Employee Training:** Training is often overlooked and few companies adequately train staff on security. Include fraud and security training at every meeting.
4. **Surprise Audits:** Internal audits are an important step for workplaces to practice continued security. Businesses should perform an internal audit on a regular basis to ensure on-going protection from illegal activity.¹³

HOW SHRED-IT CAN HELP

Shred-it is the global leader in information security, providing information destruction services to over 400,000 customers worldwide.

Secure Document and Hard Drive Destruction

- Secure end-to-end chain of custody
- Certificate of Destruction after every service
- Tailored solutions to fit your specific needs

Advice and Expertise

- All associates are Certified Information Security Professionals
- We conduct a free Data Security Survey to assess security risks in your organisation
- Helpful resources available at shredit.co.uk/resource-centre

Contact Shred-it today at **0800 028 1164** or visit us at **shredit.co.uk**

Sources

1. CIFAS, 2014 Fraudscape Report
2. Tech World, The UK's 10 Most Infamous Data Breaches
3. NFA, 2012 Annual Fraud Indicator
4. CIFAS, 2014 Employee Fraudscape
5. National Fraud Authority (NFA), 2013 Annual Fraud Indicator
6. British Chamber of Commerce, ICT Report
7. Equifax, Identity Fraud Facts & Statistics
8. Interactions Marketing, Interactions Finds 45% of Shoppers Don't Trust Retailers to Keep Information Safe
9. Ponemon Institute, 2014: A Year of Mega Breaches
10. Office of National Statistics, 2014 Internet Access – Households and Individuals
11. 2012 Norton Cybercrime Report
12. Ipsos Mori, 2015 Shred-it Information Security Tracker
13. Association of Certified Fraud Examiners, 2014, Report to the Nations on Occupational Fraud and Abuse